МИНОБРНАУКИ РОССИИ
Глазовский инженерно-экономический институт (филиал)
федерального государственного бюджетного образовательного
учреждения высшего образования
«Ижевский государственный технический университет имени М.Т.Калашникова»
(ГИЭИ (филиал) ФГБОУ ВО «ИжГТУ имени М.Т. Калашникова»)

УТВЕРЖДАЮ
И.о. директора
_____ А.В. Золотов
11 марта 20 26 г.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 3DA273AA38C240BA869FA062FFFB332C
Владелец: Золотов Алексей Васильевич
Действителен: с 29.07.2026 до 22.10.2027

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине

МДК.02.06 «Безопасность программного обеспечения»

09.02.11 Разработка и управление программным обеспечением

Глазов 2026

Фонд оценочных средств разработан на основе Федерального государственного образовательного стандарта по специальности среднего профессионального образования 09.02.11 "Разработка и управление программным обеспечением", утвержденного приказом Министерства просвещения Российской Федерации 24 февраля 2025 г. № 138 (зарегистрирован 31.03.2025 № 81696).

Организация разработчик: ГИЭИ (филиал) ФГБОУ ВО «ИжГТУ имени М.Т. Калашникова»

Разработчик: Горбушин Денис Шарибзянович, преподаватель СПО

Утверждено: Протокол Ученого совета филиала № 7, от 11 марта 2026 г.

Руководитель образовательной программы

_____ Т.А. Савельева

13 марта 2026 г.

Согласовано: Начальник отдела по учебно-методической работе

_____ И.Ф. Яковлева

13 марта 2026 г.

ПАСПОРТ
ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ
по дисциплине «Безопасность программного обеспечения»

Результаты освоения дисциплины соотносятся с планируемыми результатами освоения образовательной программы, представленными в матрице компетенций выпускника.

В результате освоения дисциплины обучающийся должен:

Код ОК, ПК	**Уметь**	**Знать**	**Владеть навыками**
ОК.01	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам	актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности	-
ОК.02	Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности	номенклатура информационных источников, применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации, современные средства и устройства информатизации; порядок их применения и программное обеспечение в профессиональной деятельности в том числе с использованием цифровых средств	-
ОК.03	Планировать и	содержание актуальной	-

	реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях	нормативно-правовой документации; современная научная и профессиональная терминология; возможные траектории профессионального развития и самообразования; основы предпринимательской деятельности; основы финансовой грамотности; правила разработки бизнес-планов; порядок выстраивания презентации; кредитные банковские продукты	
ОК.04	Эффективно взаимодействовать и работать в коллективе и команде	психологические основы деятельности коллектива, психологические особенности личности; основы проектной деятельности	-
ОК.05	Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста	особенности социального и культурного контекста; правила оформления документов и построения устных сообщений	-
ОК.06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения	сущность гражданско-патриотической позиции, общечеловеческих ценностей; значимость профессиональной деятельности по специальности; стандарты антикоррупционного поведения и последствия его нарушения	-
ОК.07	Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата,	правила экологической безопасности при ведении профессиональной деятельности; основные ресурсы,	-

	принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях	задействованные в профессиональной деятельности; пути обеспечения ресурсосбережения; принципы бережливого производства; основные направления изменения климатических условий региона	
ОК.08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности	роль физической культуры в общекультурном, профессиональном и социальном развитии человека; основы здорового образа жизни; условия профессиональной деятельности и зоны риска физического здоровья для специальности; средства профилактики перенапряжения	-
ОК.09	Пользоваться профессиональной документацией на государственном и иностранном языках	правила построения простых и сложных предложений на профессиональные темы; основные общеупотребительные глаголы (бытовая и профессиональная лексика); лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; особенности произношения; правила чтения текстов профессиональной направленности	-
ПК 2.1	− проектировать модули, соответствующие бизнес-задачам; − создавать архитектурные диаграммы и документацию; − определять структуру и интерфейсы модулей; − анализировать требования к модулю и	− основные принципы проектирования модулей программного обеспечения; − языки программирования и технологии для реализации модулей; − паттерны проектирования и структуры данных для создания эффективных и	− проектирования модулей ПО с учетом требований заказчика; − создания архитектурных диаграмм и спецификаций модулей; определения интерфейсов и взаимодействия модулей в системе.

	определять его функциональность; − проектировать архитектуру модуля, включая выбор подходящих паттернов проектирования и структуры данных; − создавать диаграммы классов, последовательностей и прочих диаграмм для визуализации проектируемого модуля; − выбирать подходящие языки программирования и технологии для реализации модуля; − проектировать интерфейсы программного обеспечения для взаимодействия с другими модулями и системами; − учитывать требования к масштабируемости, производительности и безопасности при проектировании модуля; проводить анализ и оптимизацию проектируемого модуля для повышения его эффективности и качества	масштабируемых модулей; − методы анализа требований и способов определения функциональности модуля; − принципы создания интерфейсов для взаимодействия с другими модулями и системами; − принципы обеспечения безопасности, производительности и масштабируемости при проектировании модулей; методы анализа и оптимизации проектируемых модулей для повышения их эффективности и качества.	
ПК 2.2	− разрабатывать модули программного обеспечения с использованием различных языков программирования и технологий; − применять паттерны проектирования и структуры данных для создания эффективных и масштабируемых модулей; − анализировать требования и определять функциональность модуля; − создавать интерфейсы для взаимодействия с	− язык программирования, основные конструкции, синтаксис; − паттерны проектирования; − структуры данных; − принципы создания интерфейсов для взаимодействия с другими модулями и системами, таких как REST API, SOAP; − работу с инструментальным программным обеспечением; − методы оптимизации кода и алгоритмов;	− создания модулей программного обеспечения на различных языках программирования; − отладки и тестирования разработанных модулей; − применения структурного и объектно-ориентированного программирования; − оптимизации кода и алгоритмов программных модулей для увеличения производительности; мониторинга и анализа

	другими модулями и системами; − обеспечивать безопасность, производительность и масштабируемость при разработке модулей; − оптимизировать проектируемые модули для повышения их эффективности и качества; − работать с системой контроля версий; − улучшать производительность модулей, выявляя и устраняя узкие места; − проводить анализ и мониторинг производительности приложений; применять инструменты для рефакторинга и оптимизации программного кода.	− эффективные алгоритмы и структуры данных для повышения производительности; − многопоточность в программных модулях; − методы оптимизации сетевых протоколов для ускорения обмена данными; − кэширование данных; − управление памятью; техники повышения производительности программного обеспечения	производительности приложений.
ПК 2.3	− интегрировать модули и компоненты, обеспечивая их взаимодействие; − работать с API и устанавливать соединения между компонентами; − отслеживать и устранять конфликты и ошибки интеграции; − анализировать и определять зависимости между модулями и компонентами; работать с различными форматами данных и протоколами передачи данных	− общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой информационно-коммуникационной системы; − международные стандарты локальных вычислительных сетей; − методы и подходы к интеграции модулей и компонентов; − принципы версионирования и управления изменениями при интеграции; принципы безопасности при интеграции модулей и компонентов	− интеграции программных модулей и компонентов в единое программное решение; − работы с API и веб-сервисами для взаимодействия между модулями; − работы с интеграционными платформами и инструментами; обеспечения совместимости и стабильности системы
ПК 2.4	− анализировать требования к программному обеспечению и составлять планы тестирования; − создавать тестовые	− принципы и методы тестирования программного обеспечения; − основы программирования и архитектуры	− отладки программного обеспечения на уровне программных модулей; − тестирования программного обеспечения; − формирования

	сценарии и тест-кейсы для проверки функциональности и соответствия требованиям; − выполнять тестирование программного обеспечения вручную и автоматизировать процесс тестирования; − анализировать результаты тестирования и документировать найденные ошибки; − разрабатывать стратегии отладки и исправлять ошибки в программном обеспечении; − выполнять модульные тесты с использованием инструментов тестирования, в том числе автоматизированного тестирования; − использовать системы контроля дефектов ПО; составлять отчет о выполнении тестирования ПО	программного обеспечения; − основы баз данных и SQL-запросов; − инструменты для автоматизации тестирования; − основы разработки и отладки программного обеспечения на разных языках программирования; − понятие дефекта программного обеспечения; − критерии качества ПО; − виды и типы тестирования ПО; − техники ручного тестирования; − техники автоматизированного тестирования; − жизненный цикл дефекта ПО; − принципы работы в системе контроля дефектов; основные понятия о качестве ПО	тестовых сценариев; − подготовки тестовых платформ (установка операционной системы, дополнительного ПО и другого по необходимости); − оценки объема тестирования ПО с целью определения необходимых ресурсов для его выполнения; − настройки тестовой среды и аппаратных средств для выполнения тестирования ПО в соответствии с заданием на тестирование в пределах своей компетенции; − формирования и представления отчетности о подготовке к выполнению задания на тестирование ПО в соответствии с установленными регламентами; выполнения тестовых процедур на тестовых данных
ПК 2.5	− описывать функциональность модулей в документации; − создавать диаграммы для иллюстрации работы модулей; − программировать с использованием комментариев для документирования кода; − использовать специальные метки/теги для отметки важных частей кода в документации; − вести журнал изменений и фиксировать обновления программных модулей; − разбивать модули на логические блоки и описывать каждый блок отдельн;	− стандарты технической документации; − принципы документирования программного обеспечения; инструменты для создания технической документации и комментирования кода	− создания технической документации для модулей; − документирования кода, API и интерфейсов; работы со специализированным ПО по документированию программного кода

	− включать в документацию особенности модулей, такие как ограничения, уязвимости или оптимальные настройки; проводить регулярное обновление документации при изменении модулей или добавлении нового функционала.		

Раздел 1. Зачетно – экзаменационные материалы

Вопросы к зачету

1. Что такое безопасность ПО? Какие триаде CIA (конфиденциальность, целостность, доступность) она охватывает и почему это важно на практике?
2. Объясните принципы безопасного проектирования: минимальные привилегии, по умолчанию безопасно, дефензивная инерция (defense in depth), принцип наименьших полномочий.
3. Различия между аутентификацией и авторизацией. Какие типы аутентификации существуют (многофакторная, одноразовые коды, биометрия) и какие угрозы им характерны?
4. Что такое SDLC и Security-by-Design? Назовите этапы безопасной разработки и методы встроенной безопасности (Static/Dynamic Analysis, Threat Modeling, Security Testing).
5. OWASP Top 10: перечислите и кратко объясните наиболее распространенные уязвимости (например, Injection, Broken Authentication, Sensitive Data Exposure, XML External Entities, Broken Access Control, Security Misconfiguration, XSS, Insecure Deserialization, Using Components with Known Vulnerabilities, Logging & Monitoring).
6. Что такое SQL-инъекция и XSS? Каковы базовые принципы защиты от них (параметризация запросов, валидация входов, безопасное кодирование вывода, политики контента)?
7. Что такое CSRF и как защититься от него (Token CSRF, SameSite cookies, проверка реферера)?
8. В чем различие между статической и динамической верификацией безопасности? Какие задачи решают каждое тестирование?
9. Что такое безопасная обработка ошибок и логирования? Какие риски связаны с обогащением логов чувствительной информацией?
10. Что такое управление уязвимостями и why it matters: сканеры уязвимостей, SBOM, патч-менеджмент, процессы реагирования на инциденты.
11. Опишите понятия аутентификационных протоколов (OAuth2, OpenID Connect) и их базовую архитектуру безопасного обмена токенами.
12. Что такое криптография в контексте ПО: основные схемы шифрования (симметричное, асимметричное), хеширование, соль, адам-процедуры (KDF), протоколы TLS.
13. Что такое безопасность поставок ПО (Supply Chain Security)? В чем состоит роль SBOM и управление зависимостями.
14. Объясните разницу между защитой данных “во время передачи” и “на хранении” (TLS/HTTPS vs encryption at rest).
15. Что такое тестирование на устойчивость к ошибкам (термостабильность), устойчивость к нагрузке и стресс-тестирование в контексте безопасности?
16. Что такое инцидент-менеджмент: основные фазы (подготовка, обнаружение, реагирование, восстановление, учеты) и роль учёта и уроков после инцидента.

17. Что такое безопасная настройка серверов и конфигураций (Security Misconfiguration)? Какие общие примеры ошибок конфигураций и как их предотвращать?
18. Каковы принципы безопасной обработки персональных данных (GDPR/локальные аналоги) и роль принципа приватности по умолчанию?
19. Что такое тестирование гипотез в безопасности ПО: например, A/B тестирование новых механизмов защиты, ограничение ложных срабатываний).
20. Как организовать безопасную разработку API: авторизация, аутентификация, управление ключами, JWT, rate limiting, защита от повторных запросов.

Задания к лабораторным работам

ЛР 1. Моделирование угроз и STRIDE для простого веб-приложения
Цель: выявить угрозы и сформулировать контрмеры по методологии STRIDE.
Задачи: описать архитектуру приложения, распознать угрозы по каждому классу STRIDE, предложить меры предотвращения и тестовые сценарии.
Deliverables: отчет с таблицей STRIDE, карту рисков и план мероприятий.

ЛР 2. Практика безопасной обработки ввода и защита от инъекций
Цель: реализовать безопасную обработку входных данных и SQL-инъекции в тестовой среде.
Задачи: сделать параметры запросов и подготовленные выражения, реализовать валидацию входов, протестировать защиту на тестовых данных.
Deliverables: код с примерами безопасных запросов, краткий отчёт об итогах тестирования.

ЛР 3. Аутентификация и хранение паролей
Цель: реализовать безопасную аутентификацию и хранение паролей.
Задачи: реализовать хеширование паролей с солью (bcrypt/argon2), политику паролей, безопасное хранение и проверку; продемонстрировать может ли система выдержать атаки на угадывание паролей.
Deliverables: исходники реализации, инструкции по развёртыванию, тестовые сценарии.

ЛР 4. Защита от XSS и CSRF; политика безопасности контента
Цель: предотвратить межсайтовые скрипты и поддельные запросы.
Задачи: реализовать кодирование вывода, применить Content Security Policy (CSP), продемонстрировать защиту от CSRF токенами.
Deliverables: код и отчёт по тестированию уязвимостей.

ЛР 5. Безопасность API: аутентификация, авторизация, токены
Цель: построить безопасный API с использованием токенов доступа.
Задачи: реализовать OAuth/OpenID Connect flow или JWT-валидацию, настроить проверку подписи токенов, защитить конечные точки.

Deliverables: работающий API, примеры запросов, тесты в Postman/Insomnia.

ЛР 6. Управление зависимостями и SBOM
Цель: исследовать безопасность зависимостей.
Задачи: собрать список зависимостей проекта, запустить анализ уязвимостей, составить SBOM, предложить меры по обновлению/замене опасных зависимостей.
Deliverables: отчет по зависимостям, список уязвимостей и план ремедиации.

ЛР 7. Логирование, мониторинг и ответ на инциденты
Цель: организовать безопасное логирование и обработку инцидентов.
Задачи: реализовать безопасное логирование (без утечки паролей), настроить базовые правила мониторинга, смоделировать инцидент и реакцию на него.
Deliverables: конфигурации логирования/инструментов, сценарий инцидента и шаги реагирования.

ЛР 8. Безопасная настройка сред разработки и CI/CD
Цель: внедрить контрмеры в CI/CD для предотвращения внедрений и уязвон.
Задачи: добавить статический анализ кода, сканеры зависимостей, тесты на безопасность в пайплайне, политику секретов.
Deliverables: конфигурации CI/CD, примеры отчётов и результаты тестирования.

ЛР 9. Контроль доступа и RBAC
Цель: смоделировать и реализовать контроль доступа в приложении.
Задачи: определить роли, реализовать ограничение доступа к ресурсам в зависимости от ролей, проверить устойчивость к атакам на восприятие прав.
Deliverables: код роли и тесты на контроль доступа.

ЛР 10. Тестирование безопасности веб-приложения (практика)
Цель: провести ручное и автоматизированное тестирование безопасности маленького веб-приложения.
Задачи: провести тестирование на уязвимости OWASP Top 10 в тестовой среде, задокументировать найденные проблемы и предложить исправления.
Deliverables: тестовый протокол, список найденных уязвимостей и меры ремедиации.

Вопросы к самостоятельным работам

Задание 1. Разработайте архитектуру безопасной веб-службы: выберите стек технологий, опишите архитектуру, роли пользователей и виды атак, предложите контрмеры и процедуры тестирования.

Задание 2. Напишите обзор литературы по одной из тем: безопасная обработка данных в облаке, безопасность контейнеров, управление секретами, безопасный CI/CD. Включите сравнение подходов и выводы.

Задание 3. Разработайте политику безопасности (policies): политика паролей, политика управления секретами, политика обновления зависимостей, план реагирования на инциденты.

Задание 4. Проведите threat-modeling для выбранной системы (STRIDE или PASTA): выявите угрозы, оцените риск и предложите меры снижения риска.

Задание 5. Реализуйте небольшой безопасный модуль (например, аутентификацию или API-защиту) и проведите код-ревью на предмет уязвимостей.

Задание 6. Сравните два метода тестирования безопасности: статический анализ кода против динамического тестирования. Опишите преимущества и ограничения каждого.

Задание 7. Напишите план внедрения безопасного SDLC в небольшом проекте: роли, этапы, артефакты, критерии готовности.

Задание 8. Выполните обзор подходов к управлению секретами и конфиденциальной информацией в разработке (скрытие секретов, окружения, хранилища секретов).

Вопросы к тесту

Часть А.

Множественный выбор (MCQ) — один правильный ответ

Что обозначает аббревиатура CIA в контексте информационной безопасности? A) Confidenciality, Integrity, Availability B) Compliance, Integrity, Accessibility C) Concealment, Independence, Assurance D) None of the above

Какой из подходов лучше подходит для защиты секретов в коде? A) хранение секретов в репозитории B) использование переменных окружения и секретов управляющих систем C) кодирование секретов простым Base64 D) хранение секретов в конфигурационных файлах

Что такое XSS и как предотвратить его? A) межсайтовый скриптинг; кодирование вывода, CSP B) межсайтовная атака через CSRF C) использование криптографических протоколов D) атака на базу данных через инъекции

Что такое CSRF и как предотвратить его? A) атака на аутентификацию через подмену запросов; защита токенами CSRF, SameSite B) атака через инъекции SQL C) атака на файловую систему D) атака на сеть

Какой протокол обычно используется для защиты передачи данных в

интернете? A) HTTP B) TLS/SSL C) FTP D) UDP

Что лучше всего отражает концепцию «меньше привилегий» при проектировании системы? A) каждому пользователю и компоненту дать наименьшие необходимые привилегии B) всем членам команды давать полный доступ к серверу C) использовать только локальные учетные записи D) отключать все полномочия на продакшн-среде

Что такое SBOM и зачем он нужен? A) Security Bill of Materials; документ о составе ПО для оценки рисков поставок B) Secure Binary Object Metadata C) Software Base Object Manifest D) Systemic Budget of Operability

Что означает понятие "Supply Chain Security" в контексте разработки ПО? A) безопасность цепочки поставок программного обеспечения и зависимостей B) безопасность физической цепи поставок оборудования C) безопасность сетевых протоколов D) безопасность баз данных

Часть B. Краткие задачи

Опишите минимально необходимую стратегию защиты входящих данных в веб-форме (валидаторы, ограничение форматов, обработка ошибок).

Приведите пример безопасного хранения паролей и объясните, почему соль и адаптивная трудность важны.

Опишите ключевые шаги при анализе зависимостей проекта на наличие известных уязвимостей.

Приведите краткую схему реагирования на инцидент_SECURITY-incident: обнаружение, анализ, устранение, уведомления.

Часть C. Открытые вопросы

Объясните разницу между threat modeling и risk assessment. Как связаны эти подходы в процессе разработки?

Опишите принципы безопасной разработки веб-API и почему важна аутентификация, авторизация, валидация входов и аудит.

Каковы основные различия между статическим и динамическим анализом кода, и как они дополняют друг друга?

Обсудите преимущества и недостатки использования стандартов безопасности (OWASP, ISO/IEC 27001) в рамках академического курса.