МИНОБРНАУКИ РОССИИ
ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
Колледж информационных и креативных технологий

# РАБОЧАЯ ПРОГРАММА

**МДК.02.04 Безопасность веб-приложений**

**ПМ.02 Разработка и интеграция модулей программного обеспечения**

программы подготовки специалистов среднего звена
специальность
**09.02.11 Разработка и управление программным обеспечением**

Форма обучения - очная

Владивосток 2026

Рабочая программа МДК.02.04 Безопасность веб-приложений разработана на основе федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.11 Разработка и управление программным обеспечением, квалификация программист, утвержденного приказом Министерства просвещения Российской Федерации от 24 февраля 2025 г. № 138.

Разработчик(и): М.Д. Кончаков, преподаватель

Рассмотрено и одобрено на заседании цикловой методической комиссии
Протокол № 9 от «20» мая 2026 г.

Председатель ПЦК _____ П.В. Калашников

**СОДЕРЖАНИЕ**

**1 ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ**

**2 СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ**

**3 УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ**

**4 КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ**

## 1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ МЕЖДИСЦИПЛИНАРНОГО КУРСА

### 1.1. Цель и место междисциплинарного курса в структуре образовательной программы

Междисциплинарный курс МДК.02.04 Безопасность веб-приложений входит в профессиональный цикл учебного плана образовательной программы в структуру профессионального модуля ПМ.02 Разработка и интеграция модулей программного обеспечения.

Цель освоения курса – сформировать умение выявлять и устранять нарушения безопасности веб-приложений и документировать результаты проверок.

### 1.2. Планируемые результаты освоения междисциплинарного курса

По итогам освоения курса, обучающиеся должны продемонстрировать результаты обучения, соотнесённые с результатами освоения ООП СПО, приведенные в таблице.

| Код | Наименование видов деятельности и профессиональных компетенций |
|---|---|
| ВД 2 | Разработка и интеграция модулей программного обеспечения |
| ПК 2.3 | Выполнять интеграцию модулей и компонентов программного обеспечения |
| ПК 2.4 | Выполнять тестирование и отладку программного обеспечения |
| ПК 2.5 | Осуществлять документирование программных модулей программного обеспечения |

В результате освоения междисциплинарного курса обучающийся должен:

| Код ПК | Уметь | Знать | Владеть навыками |
|---|---|---|---|
| ПК 2.3 | интегрировать модули и компоненты, обеспечивая их взаимодействие;<br>работать с API и устанавливать соединения между компонентами;<br>отслеживать и устранять конфликты и ошибки интеграции;<br>анализировать и определять зависимости между модулями и компонентами;<br>работать с различными форматами данных и протоколами передачи данных | общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой информационно-коммуникационной системы;<br>международные стандарты локальных вычислительных сетей;<br>методы и подходы к интеграции модулей и компонентов;<br>принципы версионирования и управления изменениями при интеграции;<br>принципы безопасности при интеграции модулей и компонентов | интеграции программных модулей и компонентов в единое программное решение;<br>работы с API и веб-сервисами для взаимодействия между модулями;<br>работы с интеграционными платформами и инструментами;<br>обеспечения совместимости и стабильности системы |
| ПК 2.4 | анализировать требования к программному обеспечению и составлять планы тестирования;<br>создавать тестовые сценарии и тест-кейсы для проверки функциональности и | принципы и методы тестирования программного обеспечения;<br>основы программирования и архитектуры программного обеспечения;<br>основы баз данных и | отладки программного обеспечения на уровне программных модулей;<br>тестирования программного обеспечения;<br>формирования тестовых сценариев;<br>подготовки тестовых платформ (установка операционной системы, |

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

| | | | |
|---|---|---|---|
| | такие как ограничения, уязвимости или оптимальные настройки;<br>проводить регулярное обновление документации при изменении модулей или добавлении нового функционала. | | |
| ПК 2.5 | анализировать требования к программному обеспечению и составлять планы тестирования;<br>создавать тестовые сценарии и тест-кейсы для проверки функциональности и соответствия требованиям;<br>выполнять тестирование программного обеспечения вручную и автоматизировать процесс тестирования;<br>анализировать результаты тестирования и документировать найденные ошибки;<br>разрабатывать стратегии отладки и исправлять ошибки в программном обеспечении;<br>выполнять модульные тесты с использованием инструментов тестирования, в том числе автоматизированного тестирования;<br>использовать системы контроля дефектов ПО;<br>составлять отчет о выполнении тестирования ПО описывать функциональность модулей в документации;<br>создавать диаграммы для иллюстрации работы модулей;<br>программировать с | принципы и методы тестирования программного обеспечения;<br>основы программирования и архитектуры программного обеспечения;<br>основы баз данных и SQL-запросов;<br>инструменты для автоматизации тестирования;<br>основы разработки и отладки программного обеспечения на разных языках программирования;<br>понятие дефекта программного обеспечения;<br>критерии качества ПО;<br>виды и типы тестирования ПО;<br>техники ручного тестирования;<br>техники автоматизированного тестирования;<br>жизненный цикл дефекта ПО;<br>принципы работы в системе контроля дефектов;<br>основные понятия о качестве ПО<br>стандарты технической документации;<br>принципы документирования программного обеспечения;<br>инструменты для создания технической документации и комментирования кода | отладки программного обеспечения на уровне программных модулей;<br>тестирования программного обеспечения;<br>формирования тестовых сценариев;<br>подготовки тестовых платформ (установка операционной системы, дополнительного ПО и другого по необходимости);<br>оценки объема тестирования ПО с целью определения необходимых ресурсов для его выполнения;<br>настройки тестовой среды и аппаратных средств для выполнения тестирования ПО в соответствии с заданием на тестирование в пределах своей компетенции;<br>формирования и представления отчетности о подготовке к выполнению задания на тестирование ПО в соответствии с установленными регламентами;<br>выполнения тестовых процедур на тестовых данных<br>создания технической документации для модулей;<br>документирования кода, API и интерфейсов;<br>работы со специализированным ПО по документированию программного кода |

| | | | |
|---|---|---|---|
| | использованием комментариев для документирования кода;<br>использовать специальные метки/теги для отметки важных частей кода в документации;<br>вести журнал изменений и фиксировать обновления программных модулей;<br>разбивать модули на логические блоки и описывать каждый блок отдельн;<br>включать в документацию особенности модулей, такие как ограничения, уязвимости или оптимальные настройки;<br>проводить регулярное обновление документации при изменении модулей или добавлении нового функционала. | | |

## 2. СТРУКТУРА И СОДЕРЖАНИЕ МЕЖДИСЦИПЛИНАРНОГО КУРСА

### 2.1 Объем МДК и виды учебной работы

| Вид учебной работы | Объем в часах | В т. ч. в форме практ. подготовки |
|---|---|---|
| Учебные занятия | 30 | 18 |
| Самостоятельная работа | 18 | |
| Консультации | | |
| Промежуточная аттестация | | |
| **Всего** | **48** | **18** |

### 2.2. Тематический план и содержание МДК

| Наименование разделов и тем | Содержание учебного материала и формы организации деятельности обучающихся | Объем в часах | Коды компетенций, формированию которых способствует элемент программы |
|---|---|---|---|
| **Раздел 1. Безопасность веб-приложений** | | **48** | **ПК 2.3, ПК 2.5, ПК 2.4** |
| **Тема 1.1 Модель угроз веб-приложения** | **Содержание учебного материала** | **2** | |
| | Активы и потоки данных; поверхность атаки; границы доверия; требования безопасности; проверка только в учебном разрешённом контуре. | 2 | ПК 2.3; ПК 2.5 |

| | | | |
|---|---|---|---|
| | **В том числе практических занятий** | **2** | |
| | Описать модель угроз учебного приложения. Результат: схема потоков, перечень угроз и план проверок. | 2 | ПК 2.3; ПК 2.5 |
| | **В том числе самостоятельная работа обучающихся**<br>Сопоставить угрозы с компонентами приложения и мерами защиты. | **3** | ПК 2.3; ПК 2.5 |
| **Тема 1.2 Аутентификация и управление доступом** | **Содержание учебного материала** | **2** | |
| | Идентификация пользователей; сессии; жизненный цикл токена; контроль прав на объект; безопасное хранение учётных данных. | 2 | ПК 2.3; ПК 2.4 |
| | **В том числе практических занятий** | **4** | |
| | Проверить и исправить доступ к чужим записям на локальном стенде. Результат: тесты прав, исправление и протокол повторной проверки. | 4 | ПК 2.3; ПК 2.4 |
| | **В том числе самостоятельная работа обучающихся**<br>Разработать матрицу ролей и негативные сценарии доступа. | **3** | ПК 2.3; ПК 2.4 |
| **Тема 1.3 Ввод данных и инъекции** | **Содержание учебного материала** | **2** | |
| | Параметризация SQL; серверная валидация; экранирование вывода; XSS; доверенные и недоверенные данные; ограничение обработки файлов. | 2 | ПК 2.4 |
| | **В том числе практических занятий** | **4** | |
| | Устранить SQL-инъекцию и небезопасный вывод в учебном коде. Результат: патч и регрессионные тесты. | 4 | ПК 2.4 |
| | **В том числе самостоятельная работа обучающихся**<br>Составить тестовые наборы для строк, идентификаторов и файлов. | **3** | ПК 2.4 |
| **Тема 1.4 Защита запросов и конфигурации** | **Содержание учебного материала** | **2** | |
| | CSRF; cookie; CORS; заголовки безопасности; TLS; сообщения об ошибках; управление секретами и зависимостями. | 2 | ПК 2.3; ПК 2.4 |
| | **В том числе практических занятий** | **2** | |
| | Настроить защиту форм и конфигурацию учебного сервера. Результат: проверяемые настройки и контрольные HTTP-ответы. | 2 | ПК 2.3; ПК 2.4 |
| | **В том числе самостоятельная работа обучающихся**<br>Подготовить чек-лист конфигурации и журнал обнаруженных нарушений. | **3** | ПК 2.3; ПК 2.4 |
| **Тема 1.5 Проверки безопасности API** | **Содержание учебного материала** | **2** | |
| | Проверка контракта; валидация схемы; ограничения объёма запроса; обработка ошибок; автоматизация проверок; оценка ложных находок. | 2 | ПК 2.4; ПК 2.5 |
| | **В том числе практических занятий** | **4** | |

| | | | |
|---|---|---|---|
| | Выполнить автоматизированные проверки локального API и разобрать результаты. Результат: воспроизводимые тесты и подтверждённые дефекты. | 4 | ПК 2.4; ПК 2.5 |
| | **В том числе самостоятельная работа обучающихся**<br>Подготовить сценарии злоупотребления бизнес-логикой и ожидаемые ограничения. | **3** | ПК 2.4; ПК 2.5 |
| **Тема 1.6 Документирование и регрессионный контроль** | **Содержание учебного материала** | **2** | |
| | Состав отчёта; воспроизводимость; оценка последствий; приоритет исправления; повторная проверка; критерии безопасной интеграции. | 2 | ПК 2.3; ПК 2.4; ПК 2.5 |
| | **В том числе практических занятий** | **2** | |
| | Подготовить отчёт и защитить исправления учебного приложения. Результат: отчёт с доказательствами и набор регрессионных тестов. Дифференцированный зачёт: демонстрация результата и ответы на вопросы в пределах указанных часов. | 2 | ПК 2.3; ПК 2.4; ПК 2.5 |
| | **В том числе самостоятельная работа обучающихся**<br>Оформить рекомендации разработчику и контрольный список выпуска. | **3** | ПК 2.3; ПК 2.4; ПК 2.5 |
| **Всего** | | **48** | |

## 3. УСЛОВИЯ РЕАЛИЗАЦИИ МЕЖДИСЦИПЛИНАРНОГО КУРСА

### 3.1. Материально-техническое обеспечение

Кабинет «Информатики», оснащенный оборудованием: Основное оборудование: Доска подкатная; Мультимедийный комплект (проектор

Casio XJ-V2, экран Lumien Eco Picture); Парты ученические двойные; Стол преподавателя; Стулья.

Программное обеспечение: Браузер с инструментами разработчика, HTTP-клиент, OWASP ZAP, pytest, Git; изолированное учебное приложение и база данных.

Практические занятия выполняются на рабочих местах с Windows или Linux и доступом к учебным материалам. Для каждого обучающегося предусматривается отдельное окружение и набор тестовых данных. Версии инструментов фиксируются преподавателем в инструкции к учебному стенду.

### 3.2. Учебно-методическое обеспечение

Для реализации программы учебной дисциплины библиотечный фонд ВВГУ укомплектован печатными и электронными изданиями.

Обучающиеся из числа инвалидов и лиц с ограниченными возможностями здоровья обеспечены печатными и (или) электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья.

**Основные источники**

OWASP Foundation. Web Security Testing Guide. – Электронный ресурс. – URL: https://wstg.owasp.org/.

OWASP Foundation. DevSecOps Guideline. – Электронный ресурс. – URL: https://owasp.github.io/DevSecOpsGuideline/.

**Дополнительные источники**

Pallets. Flask Tutorial. – Электронный ресурс. – URL: https://flask.palletsprojects.com/en/stable/tutorial/.

pytest. Документация. – Электронный ресурс. – URL: https://docs.pytest.org/en/stable/.

**Электронные ресурсы**

1. Информационно-справочная система «Консультант Плюс» – http://www.consultant.ru/
2. Профессиональная база данных: "Открытая база ГОСТов"/ Режим доступа: http://standartgost.ru/, доступ свободный
3. Электронная библиотечная система «РУКОНТ» - Режим доступа: https://lib.rucont.ru/
4. Электронная библиотечная система ZNANIUM.COM - Режим доступа: https://znanium.com/
5. Электронно-библиотечная система издательства "Юрайт" - Режим доступа: https://urait.ru/
6. Электронно-библиотечная система издательства "Лань" - Режим доступа: https://e.lanbook.com/
7. Президентская библиотека им. Б.Н. Ельцина (база данных различных профессиональных областей) Режим доступа: https://www.prlib.ru/, доступ свободный

## 4 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ИЗУЧЕНИЮ И РЕАЛИЗАЦИИ МЕЖДИСЦИПЛИНАРНОГО КУРСА

Начиная изучение дисциплины, студенту необходимо:

- ознакомиться с программой, изучить список рекомендуемой литературы;
- внимательно разобраться в структуре курса, в системе распределения учебного материала по видам занятий, формам контроля, чтобы иметь представление о курсе в целом.

Самостоятельная работа студентов (СРС) – это деятельность учащихся, которую они совершают без непосредственной помощи и указаний преподавателя, руководствуясь сформировавшимися ранее представлениями о порядке и правильности выполнения операций. Цель СРС в процессе обучения заключается, как в усвоении знаний, так и в формировании умений и навыков по их использованию в новых условиях на новом учебном материале. Самостоятельная работа призвана обеспечивать возможность осуществления студентами самостоятельной познавательной деятельности в обучении, и является видом учебного труда, способствующего формированию у студентов самостоятельности. Кроме того, для расширения и углубления знаний по дисциплине целесообразно использовать: публикации в тематических журналах; полнотекстовые базы данных библиотеки; имеющиеся в библиотеках вуза. Успешное освоение дисциплины предполагает активную работу студентов на всех занятиях аудиторной формы: лекций и практических занятий, выполнение аттестационный мероприятий, эффективную самостоятельную работу.

### 4.1 Методические рекомендации обучающимся по обеспечению самостоятельной работы

Самостоятельная работа проводится с целью: систематизации, закрепления, углубления и расширения теоретических знаний и практических умений, приобретаемых студентами в ходе аудиторных занятий; формирования умений использовать специальную литературу; развития познавательных способностей и активности обучающихся; формирования самостоятельности мышления, способности к саморазвитию, самосовершенствованию и самореализации; развития исследовательских умений.

Для лучшего освоения материала и систематизации знаний по дисциплине необходимо отвечать на вопросы для самоконтроля. Во время самостоятельной проработки лекционного материала особое внимание следует уделять возникшим вопросам, непонятным терминам, спорным точкам зрения. В случае необходимости обращаться к преподавателю за консультацией. Студент должен четко уяснить, что именно с лекции начинается его подготовка к практическому занятию. Вместе с тем, лекция лишь организует мыслительную деятельность, но не обеспечивает глубину усвоения программного материала.

При подготовке к практическому занятию особое внимание необходимо обратить на содержание основных положений и выводов, объяснение явлений и фактов, уяснение практического приложения рассматриваемых теоретических вопросов. В процессе этой работы студент должен стремиться понять и запомнить основные положения рассматриваемого материала, примеры, поясняющие его, а также разобраться в иллюстративном материале. В процессе подготовки рекомендуется взаимное обсуждение материала, во время которого закрепляются знания, а также приобретается практика в изложении и разъяснении полученных знаний, развивается речь.

При необходимости следует обращаться за консультацией к преподавателю. Перед консультацией, необходимо хорошо продумать вопросы, которые требуют разъяснения.

В процессе изучения дисциплины студенту необходимо ориентироваться на самостоятельную проработку лекционного материала, подготовку к практическим занятиям, выполнение тестов, кейсовых заданий, самостоятельное изучение некоторых разделов курса. Для проведения занятий лекционного типа используются учебно-наглядные пособия в форме презентационных материалов, обеспечивающих тематические иллюстрации, соответствующие темам лекций.

### 4.2 Особенности организации обучения для лиц с ограниченными возможностями здоровья и инвалидов

При необходимости обучающимся из числа лиц с ограниченными возможностями здоровья и инвалидов (по заявлению обучающегося) предоставляется учебная информация в доступных формах с учетом их индивидуальных психофизических особенностей:

для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания, консультации и др.

для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания, консультации и др.

для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; индивидуальные задания, консультации и др.

## 5 КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ КУРСА

| Код ПК | Критерии оценки результата (показатели освоенности компетенций) | Формы контроля и методы оценки |
|---|---|---|
| ПК 2.3 | Оценка «отлично»: интерфейсы согласованы, доступ разграничен, настройки защиты и передача данных проверены по требованиям.<br>Оценка «хорошо»: интеграция защищена в основных сценариях, отдельные конфигурационные недочёты исправляются самостоятельно.<br>Оценка «удовлетворительно»: компоненты взаимодействуют, но настройки защиты запросов или контроля доступа требуют доработки. | Проверка конфигурации интеграции, сессий и прав доступа, демонстрация контрольных запросов. |
| ПК 2.4 | Оценка «отлично»: значимые риски покрыты тестами, находки воспроизводимы, исправления подтверждены | Запуск негативных тестов API, проверка |

| | | |
|---|---|---|
| | регрессионной проверкой.<br>Оценка «хорошо»: основные риски проверены, отдельные граничные сценарии или пояснения результатов требуют уточнения.<br>Оценка «удовлетворительно»: выполнены базовые проверки, но часть дефектов описана или повторно проверена недостаточно. | воспроизводимости дефектов и демонстрация исправлений. |
| ПК 2.5 | Оценка «отлично»: отчёт содержит воспроизводимые шаги, оценку последствий и приоритета, меры исправления и результаты повторной проверки.<br>Оценка «хорошо»: основные результаты документированы, имеются незначительные пробелы в доказательствах или приоритетах.<br>Оценка «удовлетворительно»: отчёт фиксирует основные дефекты, но воспроизводимость и подтверждение исправлений требуют дополнения. | Защита отчёта, воспроизведение выбранных дефектов по описанию и проверка полноты документации. |

МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Колледж информационных и креативных технологий

# ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения текущего контроля и промежуточной аттестации

**по МДК.02.04 Безопасность веб-приложений**

**ПМ.02 Разработка и интеграция модулей программного обеспечения**

программы подготовки специалистов среднего звена

**09.02.11 Разработка и управление программным обеспечением**

Форма обучения: очная

Владивосток 2026

## 1. Общие сведения

Фонд оценочных средств (далее – ФОС) предназначен для контроля и оценки образовательных достижений обучающихся, освоивших программу МДК.02.04 Безопасность веб-приложений.

ФОС включают в себя контрольные материалы для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине. Промежуточная аттестация – дифференцированный зачёт (с использованием оценочных средств – устный опрос в форме ответов на вопросы билетов, устный опрос в форме собеседования, выполнение письменных заданий, тестирование и т. д.).

## 2. Планируемые результаты обучения, обеспечивающие результаты освоения образовательной программы

| Код ПК | Код результата обучения | Наименование результата обучения |
|---|---|---|
| ПК 2.3 | З1 | Границы доверия, контракты интерфейсов и требования безопасности при интеграции веб-компонентов. |
| | З2 | Правила настройки сессий, CORS, CSRF-защиты, TLS и передачи секретов. |
| | У1 | Настраивать безопасное взаимодействие компонентов и проверку прав на ресурсы. |
| | У2 | Проверять конфигурацию интеграции и обработку недоверенных данных. |
| | П1 | Интеграции веб-компонентов с проверкой требований безопасности. |
| ПК 2.4 | З1 | Методы проверки инъекций, XSS, нарушений доступа и некорректного ввода. |
| | З2 | Принципы автоматизации проверок API, анализа ложных находок и регрессионного тестирования. |
| | У1 | Разрабатывать негативные тесты для входных данных и доступа к объектам. |
| | У2 | Воспроизводить выявленную уязвимость в учебном контуре, исправлять её и выполнять повторную проверку. |
| | П1 | Тестирования безопасности и отладки учебного веб-приложения. |
| ПК 2.5 | З1 | Состав модели угроз и отчёта о проверке безопасности веб-приложения. |
| | З2 | Правила описания условий воспроизведения, последствий, приоритета и результатов повторной проверки. |
| | У1 | Оформлять отчёт о найденных уязвимостях с доказательствами и рекомендациями. |
| | У2 | Документировать требования безопасной интеграции и результаты регрессионного контроля. |
| | П1 | Подготовки документации по проверке и обеспечению безопасности веб-приложения. |

## 3. Описание процедуры оценивания

Результаты обучения по модулю, уровень сформированности компетенций оцениваются по четырёх бальной шкале оценками: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно» (по бальной системе. Максимальная сумма баллов по дисциплине равна 100 баллов.)

Текущая аттестация по модулю проводится с целью систематической проверки достижений обучающихся. Объектами оценивания являются: степень усвоения теоретических знаний, уровень овладения практическими умениями и навыками по всем видам учебной работы, качество выполнения самостоятельной работы, учебная дисциплина (активность на занятиях, своевременность выполнения различных видов заданий, посещаемость всех видов занятий по аттестуемой дисциплине).

При проведении промежуточной аттестации оценивается достижение студентом запланированных по модулю результатов обучения, обеспечивающих результаты освоения образовательной программы в целом. Оценка на зачете / экзамене выставляется с учетом оценок, полученных при прохождении текущей аттестации.

**Критерии оценивания устного ответа**

(оценочные средства: контрольная работа, собеседование, устное сообщение.)

**5 баллов** - ответ показывает прочные знания основных процессов изучаемой предметной области, отличается глубиной и полнотой раскрытия темы; владение терминологическим аппаратом; умение объяснять сущность, явлений, процессов, событий, делать выводы и обобщения, давать аргументированные ответы, приводить примеры; свободное владение монологической речью, логичность и последовательность ответа; умение приводить примеры современных проблем изучаемой области.

**4 балла** - ответ, обнаруживающий прочные знания основных процессов изучаемой предметной области, отличается глубиной и полнотой раскрытия темы; владение терминологическим аппаратом; умение объяснять сущность, явлений, процессов, событий, делать выводы и обобщения, давать аргументированные ответы, приводить примеры; свободное владение монологической речью, логичность и последовательность ответа. Однако допускается одна - две неточности в ответе.

**3 балла** – ответ, свидетельствующий в основном о знании процессов изучаемой предметной области, отличающийся недостаточной глубиной и полнотой раскрытия темы; знанием основных вопросов теории; слабо сформированными навыками анализа явлений, процессов, недостаточным умением давать аргументированные ответы и приводить примеры; недостаточно свободным владением монологической речью, логичностью и последовательностью ответа. Допускается несколько ошибок в содержании ответа; неумение привести пример развития ситуации, провести связь с другими аспектами изучаемой области.

**2 балла** – ответ, обнаруживающий незнание процессов изучаемой предметной области, отличающийся неглубоким раскрытием темы; незнанием основных вопросов теории, несформированными навыками анализа явлений, процессов; неумением давать аргументированные ответы, слабым владением монологической речью, отсутствием логичности и последовательности. Допускаются серьезные ошибки в содержании ответа; незнание современной проблематики изучаемой области.

**Критерии оценивания письменной работы**

(оценочные средства: реферат, конспект, контрольная работа, письменный отчет по практической работе, портфолио, доклад (сообщение), в том числе выполненный в форме презентации, творческое задание, курсовая работа).

**5 баллов** - студент выразил своё мнение по сформулированной проблеме, аргументировал его, точно определив ее содержание и составляющие. Проблема раскрыта полностью, выводы обоснованы. Приведены данные отечественной и зарубежной литературы, статистические сведения, информация нормативно-правового характера. Студент владеет навыком самостоятельной работы по заданной теме; методами и приемами анализа теоретических и/или практических аспектов изучаемой области. Фактических ошибок, связанных с пониманием проблемы, нет; графически работа оформлена правильно.

**4 балла** - работа характеризуется смысловой цельностью, связностью и последовательностью изложения; допущено не более 1 ошибки при объяснении смысла или содержания проблемы. Проблема раскрыта. Не все выводы сделаны и/или обоснованы. Для аргументации приводятся данные отечественных и зарубежных авторов. Продемонстрированы исследовательские умения и навыки. Фактических ошибок, связанных с пониманием проблемы, нет. Допущены одна-две ошибки в оформлении работы.

**3 балла** – студент проводит достаточно самостоятельный анализ основных этапов и смысловых составляющих проблемы; понимает базовые основы и теоретическое обоснование выбранной темы. Проблема раскрыта не полностью. Выводы не сделаны и/или выводы не обоснованы Проведен анализ проблемы без привлечения дополнительной литературы. Допущено не более 2 ошибок в смысле или содержании проблемы, оформлении работы.

**2 балла** - работа представляет собой пересказанный или полностью переписанный исходный текст без каких бы то ни было комментариев, анализа. Не раскрыта структура и теоретическая составляющая темы. Проблема не раскрыта. Выводы отсутствуют. Допущено три или более трех ошибок в смысловом содержании раскрываемой проблемы, в оформлении работы.

**Критерии оценивания тестового задания**

| Оценка | Отлично | Хорошо | Удовлетворительно | Неудовлетворительно |
|---|---|---|---|---|
| Количество правильных ответов | 91 % и ≥ | от 81% до 90,9 % | не менее 70% | менее 70% |

**Критерии выставления оценки студенту на зачете/ экзамене**

(оценочные средства: устный опрос в форме ответов на вопросы билетов, устный опрос в форме собеседования, выполнение письменных разноуровневых задач и заданий, комплексная расчетно-графическая работа, творческое задание, кейс-задача, портфолио, проект и т.п.)

| **Оценка по промежуточной аттестации** | **Характеристика качества сформированности компетенций** |
|---|---|
| «зачтено» / «отлично» | Студент демонстрирует сформированность дисциплинарных компетенций на продвинутом уровне: обнаруживает всестороннее, систематическое и глубокое знание учебного материала, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, правильно обосновывает принятое решение, владеет разносторонними навыками и приемами выполнения практических задач. |
| «зачтено» / «хорошо» | Студент демонстрирует сформированность дисциплинарных компетенций на базовом уровне: основные знания, умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации. |
| «зачтено» / «удовлетворительно» | Студент демонстрирует сформированность дисциплинарных компетенций на пороговом уровне: имеет знания только основного материала, но не усвоил его деталей, в ходе контрольных мероприятий допускаются значительные ошибки, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ, при оперировании знаниями и умениями при их переносе на новые ситуации. |
| «не зачтено» / «неудовлетворительно» | Студент демонстрирует сформированность дисциплинарных компетенций на уровне ниже порогового: выявляется полное или практически полное отсутствие знаний значительной части программного материала, студент допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы, умения и навыки не сформированы. |

## 4. Примеры оценочных средств для проведения промежуточной аттестации

### Вопросы для промежуточной аттестации

1. Активы и потоки данных; поверхность атаки; границы доверия; требования безопасности; проверка только в учебном разрешённом контуре.

2. Идентификация пользователей; сессии; жизненный цикл токена; контроль прав на объект; безопасное хранение учётных данных.

3. Параметризация SQL; серверная валидация; экранирование вывода; XSS; доверенные и недоверенные данные; ограничение обработки файлов.

4. CSRF; cookie; CORS; заголовки безопасности; TLS; сообщения об ошибках; управление секретами и зависимостями.

5. Проверка контракта; валидация схемы; ограничения объёма запроса; обработка ошибок; автоматизация проверок; оценка ложных находок.

6. Состав отчёта; воспроизводимость; оценка последствий; приоритет исправления; повторная проверка; критерии безопасной интеграции.

## Билеты для промежуточной аттестации

**Билет 1**

1. Активы и потоки данных; поверхность атаки; границы доверия; требования безопасности; проверка только в учебном разрешённом контуре.

2. Описать модель угроз учебного приложения.

**Билет 2**

1. Идентификация пользователей; сессии; жизненный цикл токена; контроль прав на объект; безопасное хранение учётных данных.

2. Проверить и исправить доступ к чужим записям на локальном стенде.

**Билет 3**

1. Параметризация SQL; серверная валидация; экранирование вывода; XSS; доверенные и недоверенные данные; ограничение обработки файлов.

2. Устранить SQL-инъекцию и небезопасный вывод в учебном коде.

**Билет 4**

1. CSRF; cookie; CORS; заголовки безопасности; TLS; сообщения об ошибках; управление секретами и зависимостями.

2. Настроить защиту форм и конфигурацию учебного сервера.

**Билет 5**

1. Проверка контракта; валидация схемы; ограничения объёма запроса; обработка ошибок; автоматизация проверок; оценка ложных находок.

2. Выполнить автоматизированные проверки локального API и разобрать результаты.

**Билет 6**

1. Состав отчёта; воспроизводимость; оценка последствий; приоритет исправления; повторная проверка; критерии безопасной интеграции.

2. Подготовить отчёт и защитить исправления учебного приложения.