СОЧИНСКИЙ ИНСТИТУТ (ФИЛИАЛ)
федерального государственного автономного образовательного
учреждения высшего образования
«РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ ИМЕНИ ПАТРИСА ЛУМУМБЫ»

Отделение среднего профессионального образования

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

"Обеспечение безопасности веб-приложений"

(наименование дисциплины)

Освоение учебной дисциплины ведется в рамках реализации основной образовательной программы среднего профессионального образования (ОП СПО):

09.02.11 Разработка и управление программным обеспечением

(код и наименование специальности/профессии ОП СПО)

Квалификация:

программист

(наименование квалификации)

Сочи,
2026 г.

1. ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ
ПМ.03.03 Обеспечение безопасности веб-приложений

название дисциплины

1.1. Область применения программы

Программа учебной дисциплины ПМ.03.03 Обеспечение безопасности веб-приложений является частью программы подготовки специалистов среднего звена в соответствии с ФГОС "Федеральный государственный образовательный стандарт среднего профессионального образования по специальности 09.02.11 РАЗРАБОТКА И УПРАВЛЕНИЕ ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ (приказ Минпросвещения России от 24.02.2025 г. № 138)"

1.2. Место учебной дисциплины в структуре программы подготовки специалистов среднего звена.

Учебная дисциплина ПМ.03.03 Обеспечение безопасности веб-приложений входит в Профессиональный цикл Профессиональной подготовки.

1.3. Цели и задачи – требования к результатам освоения учебной дисциплины.

Основная цель – способствовать формированию общих и профессиональных компетенций посредством приобретения знаний, умений и навыков.

В результате освоения учебной дисциплины студент должен знать:

- Основные принципы проектирования защищённых веб-систем и классификацию угроз информационной безопасности.
- Источники рисков: методы несанкционированного доступа, векторы атак.
- Требования отечественных стандартов и международных регламентов.
- Принципы построения систем аутентификации и авторизации с применением токенов веб-сессий.
- Методы криптографической защиты данных: алгоритмы шифрования, настройка защищённых соединений.
- Подходы к обеспечению отказоустойчивости: защита от атак типа «отказ в обслуживании» (DDoS), резервирование ресурсов.

В результате освоения учебной дисциплины студент должен уметь:

- Проводить анализ веб-приложений на наличие уязвимостей с использованием инструментов.
- Реализовывать механизмы валидации и санитизации пользовательского ввода для предотвращения внедрения вредоносного кода.
- Настраивать безопасные соединения (генерация SSL-сертификатов, принудительное использование HTTPS).
- Проектировать системы управления доступом с соблюдением принципа наименьших привилегий.
- Разрабатывать рекомендации по устранению выявленных уязвимостей в соответствии с требованиями законодательства РФ.

В результате освоения учебной дисциплины студент должен иметь навыки и (или) опыт деятельности:

- Практического тестирования защищённости: выявление точек внедрения SQL-запросов, межсайтового скриптинга, утечек сессионных данных.
- Настройки механизмов аутентификации с применением токенов и многофакторной проверки.
- Обеспечения безопасности загружаемых файлов: валидация типов, размеров, изоляция

в отдельных хранилищах.
- Составления технической документации по результатам аудитов с акцентом на соответствие требованиям 152-ФЗ.
- Применения методов защиты от DDoS-атак: настройка балансировщиков нагрузки, фильтрация трафика.

1.4. Рекомендуемое количество часов на освоение программы учебной дисциплины:

Объем программы 72 часов, в том числе:
аудиторной учебной нагрузки обучающегося 60 часов;
самостоятельной работы обучающегося 12 часов.

2. СТРУКТУРА И ПРИМЕРНОЕ СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ
2.1. Объем учебной дисциплины и виды учебной работы

Таблица 1. Виды учебной работы по периодам освоения ООП СПО для формы обучения - очная.

Вид учебной работы	Всего, ак. ч.	Семестр(-ы)					
		7	2				
Контактная (аудиторная) работа (всего)	60	60	34				
в том числе:	-	-	-	-	-	-	-
лекции (если предусмотрено)	24	24	-				
в том числе в форме практической подготовки (если предусмотрено)	-	-	-				
лабораторные занятия (если предусмотрено)	-	-	-				
в том числе в форме практической подготовки (если предусмотрено)	-	-	-				
практические занятия (если предусмотрено)	36	36	34				
в том числе в форме практической подготовки (если предусмотрено)	-	-	-				
Самостоятельная работа обучающегося (всего)	12	12	4				
в том числе:	-	-	-	-	-	-	-
в форме практической подготовки (если предусмотрено)	-	-	-				
Часов на контроль:	-	-	18				
Промежуточная аттестация в форме: (зачет/дифзачет/ экзамен)	-	ЗаО	Эк				
Общая трудоемкость час	72	72	56				

2.2. Тематический план и содержание учебной дисциплины ПМ.03.03 Обеспечение безопасности веб-приложений

Таблица 2. Содержание дисциплины/МДК по видам учебной работы

НАИМЕНОВАНИЕ РАЗДЕЛА ДИСЦИПЛИНЫ Содержание раздела (темы)	Вид учебной работы*	Кол-во часов
Тема 1. Основы безопасности веб-ресурсов	**8**	
Принципы проектирования защищенных систем. Классификация угроз: внутренние и внешние риски	Лек	2

Сбор данных о веб-приложении: анализ метаданных, структуры URL, заголовков HTTP	Пр	2
Анализ реальных инцидентов информационной безопасности и их последствий	СР	4
Тема 2. Источники угроз и методы противодействия	**6**	
Анализ векторов атак: социальная инженерия, вредоносное ПО, сетевые уязвимости	Лек	2
Превентивные меры: сегментация сетей, мониторинг трафика, обновление ПО	Лек	2
Тестирование механизмов управления доступом: обход ограничений, перехват сессий	Пр	2
Тема 3. Стандарты и регламенты разработки	**12**	
Требования ГОСТ Р, PCI DSS, OWASP Top 10	Лек	2
Методики безопасного кодирования и аудита архитектуры приложений	Лек	2
Использование инструмента OWASP ZAP для автоматизированного сканирования уязвимостей	Пр	4
Изучение требований стандартов PCI DSS и ГОСТ Р в сфере веб-безопасности	СР	4
Тема 4. Системы идентификации и контроля доступа	**8**	
Механизмы аутентификации (многофакторная проверка, токены)	Лек	2
Принципы наименьших привилегий и управление ролями пользователей	Лек	2
Настройка аутентификации на основе токенов веб-сессий (JWT)	Пр	4
Тема 5. Обеспечение отказоустойчивости	**8**	
Защита от атак типа «отказ в обслуживании» (DDoS)	Лек	2
Резервирование ресурсов и восстановление после инцидентов	Пр	2
Имитация атак типа «отказ в обслуживании» и настройка защиты	Пр	4
Тема 6. Валидация данных и защита от внедрения кода	**12**	
Фильтрация пользовательского ввода	Лек	2
Методы противодействия внедрению SQL-запросов и межсайтовому скриптингу (XSS)	Пр	2
Поиск точек внедрения SQL-запросов и методы нейтрализации	Пр	4
Выявление уязвимостей межсайтового скриптинга (XSS) в веб-формах и API	Пр	4
Тема 7. Криптографические методы защиты	**8**	
Алгоритмы шифрования данных (AES, RSA)	Лек	2
Реализация защищенных соединений (протоколы SSL/TLS, HTTPS)	Пр	2
Развертывание защищенных соединений: генерация SSL-сертификатов, настройка HTTPS	Пр	4
Тема 8. Безопасная работа с файлами и медиа	**10**	
Предотвращение загрузки вредоносных файлов	Лек	2
Изоляция ресурсов и ограничение прав доступа к файловой системе	Лек	2
Безопасная обработка загружаемых файлов: валидация типа, размера, изоляция хранилищ	Пр	2
Составление инструкций по противодействию межсайтовому скриптингу (XSS), внедрению SQL-запросов и атакам на сессии пользователей	СР	4

** - Лек – лекции; Пр – практические занятия; СР – самостоятельная работа; ЛР – лабораторные работы.*

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечению

Для реализации программы учебной дисциплины предусмотрены специальные помещения, приведенным в п 6.3 основной образовательной программы специальности.

Таблица 3. Материально-техническое обеспечение дисциплины

Тип аудитории	**Оснащение аудитории** **Специализированное учебное оборудование, ПО и материалы для освоения дисциплины (при необходимости)**
Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации (компьютерный класс)	Комплект специализированной мебели; доска аудиторная меловая, кондиционер «General», технические средства: автоматизированные рабочие места (процессор не ниже Intel Core i3, оперативная память объемом не менее 8Гб; SSD память объемом не менее 240 gb, HDD память объемом не менее 500 gb) в количестве 11 штук, проектор BenQ MS521P, проекционный экран Lumien Master Picture. Имеется выход в интернет. Программное обеспечение: Операционная система Windows 10 Pro; Office Professional 2007, Kaspersky Endpoint security для бизнеса - Стандартный
Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации (компьютерный класс)	Комплект специализированной мебели; доска аудиторная меловая, технические средства: автоматизированные рабочие места (процессор не ниже Intel Core i3, оперативная память объемом не менее 8Gb, SSD память объемом не менее 240 GB/ HDD память объемом не менее 500 GB, видеокарта NVIDIA 1050TI 4G) в количестве 11 штук, проектор EPSON EB-W05, проекционный экран Lumen Master Picture. Имеется выход в интернет. Программное обеспечение: Операционная система Windows 10 Pro; Office Professional 2007, Kaspersky Endpoint security для бизнеса - Стандартный
Аудитория для самостоятельной работы обучающихся	Комплект специализированной мебели; Телевизор LED LG 42", автоматизированные рабочие места (процессор не ниже AMD Quad-Core, оперативная память объемом не менее 4Гб; HD500gb), имеется выход в интернет Программное обеспечение: Операционная система Windows 10 Pro; Office Professional 2007, Kaspersky Endpoint security для бизнеса - Стандартный

3.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. Тузовский А. Ф. Проектирование и разработка web-приложений : учебное пособие для спо. - Москва: Юрайт, 2024. - 219 с - Текст : электронный. - URL: https://urait.ru/bcode/541917

2. Полуэктова Н. Р. Разработка веб-приложений : учебное пособие для спо. - Москва: Юрайт, 2024. - 204 с - Текст : электронный. - URL: https://urait.ru/bcode/545237

Дополнительные источники:

3. Маркин А. В. Программирование на SQL : учебное пособие для спо. - Москва: Юрайт, 2024. - 435 с - Текст : электронный. - URL: https://urait.ru/bcode/542484
4. Грекул В. И., Коровкина Н. Л., Левочкина Г. А. Проектирование информационных систем : учебник и практикум для спо. - Москва: Юрайт, 2024. - 418 с - Текст : электронный. - URL: https://urait.ru/bcode/556554
5. Федоров Д. Ю. Программирование на языке высокого уровня Python : учебное пособие для спо. - Москва: Юрайт, 2024. - 187 с - Текст : электронный. - URL: https://urait.ru/bcode/556852
6. Гуриков С.Р. Основы алгоритмизации и программирования на Python : Учебное пособие. - Москва: ООО "Научно-издательский центр ИНФРА-М", 2025. - 343 с. - Текст : электронный. - URL: https://znanium.ru/catalog/document?id=453296
7. Шитов В.Н. Внедрение информационных систем : Учебное пособие. - Москва: КноРус, 2024. - 341 с. - Текст : электронный. - URL: https://book.ru/book/952297

Ресурсы информационно-телекоммуникационной сети «Интернет»:

1. ЭБС РУДН и сторонние ЭБС, к которым студенты университета имеют доступ на основании заключенных договоров:

- Образовательная платформа Юрайт https://urait.ru
- ЭБС «Университетская библиотека онлайн» http://biblioclub.ru
- ЭБС Znanium https://znanium.ru
- Электронно-библиотечная система РУДН – ЭБС РУДН http://mega.rudn.ru/MegaPro/Web

2. Базы данных и поисковые системы:

- Учебный портал института https://portal.rudn-sochi.ru/

Методические материалы для обучающихся

Самостоятельная работа студента является ключевой составляющей учебного процесса, которая определяет формирование навыков, умений и знаний, приемов познавательной деятельности и обеспечивает интерес к творческой работе.
Правильно спланированная и организованная самостоятельная работа студентов позволяет:
-сделать образовательный процесс более качественным и интенсивным;
-способствует созданию интереса к избранной профессии и овладению ее особенностями;
-приобщить студента к творческой деятельности;
-проводить в жизнь дифференцированный подход к обучению.
При организации самостоятельной работы студентов в качестве методологической основы должен применяться деятельный подход, когда обучение ориентировано на формирование умений решать не только типовые, но и нетиповые задачи, когда студент должен проявить творческую активность, инициативу, знания, умения и навыки, полученные при изучении конкретной дисциплины.
Учебно-методические материалы для самостоятельной работы обучающихся размещаются в соответствии с действующим порядком на странице дисциплины на Учебном портале.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в процессе проведения практических занятий, тестирования, а также выполнения

обучающимися индивидуальных заданий.

Таблица 4. Контроль и оценка результатов освоения дисциплины

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
Знания: - Основные принципы проектирования защищённых веб-систем и классификацию угроз информационной безопасности. - Источники рисков: методы несанкционированного доступа, векторы атак. - Требования отечественных стандартов и международных регламентов. - Принципы построения систем аутентификации и авторизации с применением токенов веб-сессий. - Методы криптографической защиты данных: алгоритмы шифрования, настройка защищённых соединений. - Подходы к обеспечению отказоустойчивости: защита от атак типа «отказ в обслуживании» (DDoS), резервирование ресурсов.	Анализ и оценка выполнения индивидуальных заданий, расчетных работ, опрос, тематический диктант, контрольная работа, практические занятия, домашние работы, компьютерное тестирование, Взаимоконтроль и самоконтроль студентов. Полнота и грамотность подготовленных докладов, сообщений, презентаций.
Умения: - Проводить анализ веб-приложений на наличие уязвимостей с использованием инструментов. - Реализовывать механизмы валидации и санитизации пользовательского ввода для предотвращения внедрения вредоносного кода. - Настраивать безопасные соединения (генерация SSL-сертификатов, принудительное использование HTTPS). - Проектировать системы управления доступом с соблюдением принципа наименьших привилегий. - Разрабатывать рекомендации по устранению выявленных уязвимостей в соответствии с требованиями законодательства РФ.	Наблюдение, контроль преподавателя за деятельностью обучающихся, анализ и оценка оптимальности метода решения задач, беседа, опрос, практические занятия, домашние работы, компьютерное тестирование

Практический опыт: - Практического тестирования защищённости: выявление точек внедрения SQL-запросов, межсайтового скриптинга, утечек сессионных данных. - Настройки механизмов аутентификации с применением токенов и многофакторной проверки. - Обеспечения безопасности загружаемых файлов: валидация типов, размеров, изоляция в отдельных хранилищах. - Составления технической документации по результатам аудитов с акцентом на соответствие требованиям 152-ФЗ. - Применения методов защиты от DDoS-атак: настройка балансировщиков нагрузки, фильтрация трафика.	Наблюдение, контроль преподавателя за деятельностью обучающихся, анализ и оценка оптимальности метода решения задач, выполнение и защита индивидуальных заданий.

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

6.1. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине «Обеспечение безопасности веб-приложений»

Перечень вопросов для подготовки к занятиям и промежуточной аттестации, контрольных работ, содержание заданий для выполнения практических и самостоятельных работ, рекомендации по выполнению и критерии оценивания представлены в фонде оценочных средств по дисциплине «Обеспечение безопасности веб-приложений» в Приложении к настоящей Рабочей программе дисциплины.

Оценочные средства позволяют провести текущий контроль по дисциплине. По каждому средству оценивается полнота и глубина освоения, характеризующиеся показателями и критериями оценивания

Таблица 6. Показатели и критерии оценивания

Показатель	Критерий
Пороговый (узнавание) «3»	Знает: базовые общие знания; Умеет: основные умения, требуемые для выполнения простых задач; Владеет: работает при прямом наблюдении.
Базовый (воспроизведение) «4»	Знает: факты, принципы, процессы, общие понятия в пределах области исследования; Умеет: диапазон практических умений, требуемых для решения определенных проблем в области исследования; Владеет: берет ответственность за завершение задач в исследовании, приспосабливает свое поведение к обстоятельствам в решении проблем
Высокий (компетентность) «5» max балл	Знает: фактическое и теоретическое знание в пределах области исследования с пониманием границ применимости; Умеет: диапазон практических умений, требуемых для развития творческих решений, абстрагирования проблем; Владеет: контролирует работу, проводит оценку, совершенствует действия работы

Максимальное количество баллов по каждому оценочному средству соответствует вербальному критерию «высокий».

7. ИНЫЕ СВЕДЕНИЯ И (ИЛИ) МАТЕРИАЛЫ

7.1 Перечень образовательных технологий, используемых при осуществлении образовательного процесса по дисциплине

В процессе обучения используются активные и интерактивные образовательные технологии (формы проведения занятий):

-лекции, фронтальные опросы, презентации и защита мини-проектов;

-кейс-стади (разбор конкретных ситуаций),

-имитационные компьютерные модели;

-организации самостоятельной учебно-познавательной деятельности (индивидуальные домашние задания).