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

Отделение среднего профессионального образования

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ОЦЕНИВАНИЯ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ ПО ДИСЦИПЛИНЕ

"Обеспечение безопасности веб-приложений"

(наименование дисциплины)

Оценочные материалы рекомендованы МС для специальности/профессии:

09.02.11 Разработка и управление программным обеспечением

(код и наименование специальности/профессии ОП СПО)

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

"Разработка и управление программным обеспечением"

(наименование специальности/профессии ОП СПО)

Семестр реализации: 4 курс, 7 семестр

Сочи, 2026

1. НАЗНАЧЕНИЕ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

ФОС создается в соответствии с требованиями Федерального государственного образовательного стандарта для аттестации обучающихся на соответствие их достижений поэтапным требованиям соответствующей образовательной программы для проведения текущего оценивания, а также промежуточной аттестации обучающихся. ФОС является составной частью нормативно-методического обеспечения системы оценки качества освоения образовательной программы, входит в состав образовательной программы.

ФОС – комплект методических материалов, нормирующих процедуры оценивания результатов обучения, т.е. установления соответствия учебных достижений (результатов обучения) запланированным результатам освоения рабочих программ учебных дисциплин (модулей) и образовательных программ.

ФОС сформирован на основе ключевых принципов оценивания:

– валидности: объекты оценки должны соответствовать поставленным целям обучения;

– надежности: использование единообразных стандартов и критериев для оценивания достижений;

– объективности: разные обучающиеся должны иметь равные возможности добиться успеха.

ФОС подлежат ежегодному пересмотру и обновлению.

2. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

В процессе изучения дисциплины предполагается проведение практических занятий для закрепления теоретических знаний, тематика практических занятий учитывает специфику получаемой специальности.

С целью закрепления и систематизации знаний, формирования самостоятельного мышления в программе предусмотрены часы для самостоятельной работы студентов. Результаты самостоятельной работы представляются в следующих формах: доклад, презентация, индивидуальное домашнее задание, расчетно-графическая работа.

Рабочей программой предусмотрены:

- рубежный контроль по окончании изучения отдельных разделов программы;
- промежуточный контроль в форме дифференцированного зачета - по завершению изучения курса.

При изучении дисциплины - внимание студента будет обращено на её прикладной характер, на то, где и когда изучаемые теоретические положения и практические навыки могут быть использованы в будущей практической деятельности.

Перечень контролируемых компетенций

Шифр	Компетенция
ПК 3.3.	Осуществлять техническое сопровождение и восстановление веб-приложений в соответствии с техническим заданием
ПК 3.4.	Производить тестирование разработанного веб-приложения
ПК 3.5.	Осуществлять аудит безопасности веб-приложения в соответствии с регламентом по безопасности

3. ТЕКУЩИЙ КОНТРОЛЬ

3.1. Текущий контроль

Текущий контроль знаний используется для оперативного и регулярного управления учебной деятельностью (в том числе самостоятельной) обучающихся. Текущий контроль успеваемости осуществляется в течение семестра, в ходе повседневной учебной работы. Данный вид контроля стимулирует у обучающихся стремление к систематической самостоятельной работе по изучению дисциплины.

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

Показатель	Критерий	Шкала		
Пороговый (узнавание) «3»	Знает: базовые общие знания; Умеет: основные умения, требуемые для выполнения простых задач; Владеет: работает при прямом наблюдении.	3	2	1
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	4	3	2
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,	5	4	3

Максимальное количество баллов по каждому оценочному средству (соответствует вербальному критерию «высокий») представлено в Паспорте фонда оценочных средств и зависит от сложности темы и количества часов на ее усвоение.

3.2. Описание фонда оценочных средств

3.2.1. Критерии оценивания письменных и устных ответов обучающихся

С целью контроля и подготовки обучающихся к изучению новой темы может проводится устный опрос по предыдущим темам.

Критерии оценки:

– правильность ответа по содержанию задания (учитывается количество и характер ошибок при ответе);

– полнота и глубина ответа (учитывается количество усвоенных фактов, понятий и т.п.);

– осознанность ответа (учитывается понимание излагаемого материала);

– логика изложения материала (учитывается умение строить целостный, последовательный рассказ, грамотно пользоваться специальной терминологией);

– рациональность использованных приемов и способов решения поставленной учебной

задачи (учитывается умение использовать наиболее прогрессивные и эффективные способы достижения цели);
– своевременность и эффективность использования наглядных пособий и технических средств при ответе (учитывается способность грамотно и с пользой применять наглядность и демонстрационный опыт при устном ответе);
– использование дополнительного материала;
– рациональность использования времени, отведенного на задание (не одобряется затянутость устного ответа во времени, с учетом индивидуальных особенностей обучающихся).

Оценка «отлично» выставляется, если обучающийся: полно и аргументировано отвечает по содержанию задания; обнаруживает понимание материала, может обосновать свои суждения, применить знания на практике, привести необходимые примеры не только по учебнику, но и самостоятельно составленные; излагает материал последовательно и правильно.
Оценка «хорошо» выставляется, если обучающийся дает ответ, удовлетворяющий тем же требованиям, что и для оценки «отлично», но допускает 1-2 ошибки, которые сам же исправляет.
Оценка «удовлетворительно» выставляется, если обучающийся обнаруживает знание и понимание основных положений данного задания, но: излагает материал неполно и допускает неточности в определении понятий или формулировке правил; не умеет достаточно глубоко и доказательно обосновать свои суждения и привести свои примеры; излагает материал непоследовательно и допускает ошибки.
Оценка «неудовлетворительно» выставляется, если обучающийся обнаруживает незнание ответа на соответствующее задание, допускает ошибки в формулировке определений и правил, искажающие их смысл, беспорядочно и неуверенно излагает материал. Оценка «неудовлетворительно» отмечает такие недостатки в подготовке обучающегося, которые являются серьезным препятствием к успешному овладению последующим материалом.

3.2.2. Примерный перечень оценочных средств

Изучение материала проводится в форме, доступной пониманию студентов, с учётом преемственности в обучении, единства терминологии и обозначений в соответствии с действующими государственными стандартами.
В процессе обучения используются активные и интерактивные образовательные технологии (формы проведения занятий):
- лекции, беседы, фронтальные опросы, презентации и защита мини-проектов;
- организация «мозгового штурма», управляемой дискуссии, работы в малых группах;
- выполнение практических работ и заданий;
- организации самостоятельной учебно-познавательной деятельности (индивидуальные домашние задания);
- контрольные работы.

3.2.3. Примеры оценочных средств

Примеры оценочных средств (при наличии) представлены в Приложении к рабочей программе дисциплины "Обеспечение безопасности веб-приложений"
Открыть приложение

3.3. Темы докладов, рефератов, презентаций

1. Методы защиты веб-приложений от внедрения вредоносных SQL-запросов.
2. Принципы построения систем аутентификации с применением токенов сессий.
3. Требования Федерального закона «О персональных данных» к веб-ресурсам.
4. Технологии предотвращения межсайтового скриптинга в пользовательском вводе.
5. Стандарты ГОСТ Р в области информационной безопасности веб-приложений.
6. Методы обеспечения отказоустойчивости веб-сервисов при атаках типа «отказ в обслуживании»
7. Применение криптографических алгоритмов для защиты данных пользователей.
8. Организация безопасной загрузки и обработки файлов на веб-серверах.
9. Инструменты автоматизированного сканирования уязвимостей на примере OWASP ZAP.

10. Реализация многофакторной проверки подлинности в веб-приложениях.
11. Анализ уязвимостей управления сессиями и методы их устранения.
12. Принципы сегментации сетей для повышения безопасности веб-инфраструктуры.
13. Меры защиты персональных данных при взаимодействии с внешними программными интерфейсами.
14. Стратегии восстановления данных после инцидентов информационной безопасности.
15. Методика подготовки отчётов по результатам тестирования защищённости веб-ресурсов.

4. ПРОМЕЖУТОЧНЫЙ КОНТРОЛЬ

4.1. Оценочные средства для промежуточной аттестации

ФОС для промежуточной аттестации обучающихся по учебной дисциплине (модулю) Обеспечение безопасности веб-приложений предназначен для оценки степени достижения запланированных результатов обучения по завершению изучения дисциплины в установленной учебным планом форме и позволяют определить результаты освоения дисциплины.
Рабочей программой предусмотрены:
- рубежный контроль по окончании изучения отдельных разделов программы;
- промежуточный контроль.
Формой контроля сформированности компетенций у обучающихся по учебной дисциплине (модулю) является:

Курс	Семестр	Вид контроля
4	7	Зачет с оценкой

4.2. Критерии оценивания

При оценке устного ответа учитываются: полнота и правильность ответа; степень осознанности, понимания изученного; языковое оформление ответа.
«5» ставится в том случае, если обучающийся: правильно понимает сущность вопроса, дает точное определение и истолкование основных понятий; строит ответ по собственному плану, сопровождает ответ новыми примерами, умеет применить знания в новой ситуации; может установить связь между изучаемым и ранее изученным материалом в том числе при изучении других предметов.
«4» ставится, если: ответ удовлетворяет основным требованиям к ответу на 5, но дан без использования собственного плана, новых примеров, применения знаний в новой ситуации, допущена одна ошибка или не более двух недочетов и обучающийся может их исправить самостоятельно или с небольшой помощью преподавателя.
«3» ставится, если обучающийся: правильно понимает сущность вопроса, но в ответе имеются отдельные пробелы в усвоении вопросов курса, не препятствующие дальнейшему усвоению программного материала; умеет применять полученные знания при решении простых задач по готовому алгоритму.
«2» ставится, если: обучающийся не овладел основными знаниями и умениями в соответствии с требованиями программы и допустил больше ошибок и недочетов, чем необходимо для оценки 3.
Оценка «1» ставится в том случае, если обучающийся не может ответить ни на один из поставленных вопросов.
Критерии оценки выполнения практического задания

Критерии оценки практического задания
«5» ставится если: обучающийся выполнил работу в полном объеме с соблюдением необходимой последовательности действий; получил правильные результаты и выводы; правильно и аккуратно выполнил все записи, вычисления, в рассуждениях и обосновании решения нет пробелов и ошибок; в решении нет математических ошибок (возможна одна неточность, описка, не являющаяся следствием незнания или непонимания учебного материала).

«4» ставится, если работа выполнена полностью, но обоснования шагов решения недостаточны; выполнены требования к оценке 5, но допущены 2-3 недочета, или не более одной ошибки и одного недочета.

«3» ставится, если работа выполнена не полностью, но объем выполненной части таков, что позволяет получить правильные результаты и выводы; допущены более одной ошибки или более двух-трёх недочётов в выкладках, но учащийся владеет обязательными умениями по проверяемой теме.

«2» ставится, если работа выполнена не полностью и объем выполненной работы не позволяет сделать правильных выводов; работа проводилась неправильно, допущены существенные ошибки, показавшие, что обучающийся не владеет обязательные умениями по данной теме в полной мере.

«1» ставится, если: работа показала полное отсутствие у учащегося обязательных знаний и умений по проверяемой теме или значительная часть работы выполнена не самостоятельно.

Оценка «5» соответствует высокому уровню, оценка «4» – базовому, оценка «3» – пороговому.

4.3. Вопросы для промежуточной аттестации

1. Основные принципы построения защищённых веб-систем.
2. Классификация угроз информационной безопасности веб-приложений.
3. Источники внутренних и внешних рисков для веб-ресурсов.
4. Требования ГОСТ Р 57580.1-2017 к разработке безопасных приложений.
5. Положения Федерального закона «О персональных данных» в контексте защиты веб-сервисов.
6. Методы противодействия внедрению вредоносных SQL-запросов.
7. Способы предотвращения межсайтового скриптинга при обработке пользовательских данных.
8. Принципы организации аутентификации с использованием токенов веб-сессий.
9. Механизмы контроля доступа на основе ролей пользователей.
10. Технологии криптографической защиты данных: симметричные и асимметричные алгоритмы.
11. Настройка защищённых соединений с применением протоколов SSL/TLS.
12. Методы защиты от атак типа «отказ в обслуживании».
13. Стратегии резервирования ресурсов для обеспечения отказоустойчивости.
14. Валидация и фильтрация пользовательского ввода для предотвращения уязвимостей.
15. Безопасная обработка загружаемых файлов: ограничение типов и изоляция хранилищ.
16. Применение инструмента OWASP ZAP для выявления уязвимостей.
17. Реализация многофакторной проверки подлинности пользователей.
18. Принцип наименьших привилегий в системах управления доступом.
19. Методы мониторинга сетевого трафика для обнаружения аномалий.
20. Стандарты PCI DSS и их роль в защите финансовых операций.
21. Классификация уязвимостей по методике OWASP Top 10.
22. Меры защиты сессионных данных от перехвата и подделки.
23. Организация обновления программного обеспечения для устранения уязвимостей.
24. Работа с системами веб-аналитики с соблюдением требований к конфиденциальности.
25. Методы сегментации сетей для ограничения распространения атак.
26. Анализ логов сервера с целью выявления следов несанкционированного доступа.
27. Принципы проектирования архитектуры с учётом безопасности на этапе разработки.
28. Требования к генерации и хранению паролей в системах аутентификации.
29. Стратегии восстановления данных после инцидентов информационной безопасности.
30. Оформление отчётов по результатам тестирования защищённости веб-приложений.

4.4. Перечень компетенций, которые сформированы у обучающихся при успешном выполнении заданий

В результате изучения учебной дисциплины обучающиеся осваивают следующие компетенции:

Раздел/Тема	Компетенции
Дифференцированный зачет	ПК 3.3., ПК 3.4., ПК 3.5.
Тема 1. Основы безопасности веб-ресурсов	ПК 3.3., ПК 3.4., ПК 3.5.
Тема 2. Источники угроз и методы противодействия	ПК 3.3., ПК 3.4., ПК 3.5.
Тема 3. Стандарты и регламенты разработки	ПК 3.3., ПК 3.4., ПК 3.5.
Тема 4. Системы идентификации и контроля доступа	ПК 3.3., ПК 3.4., ПК 3.5.
Тема 5. Обеспечение отказоустойчивости	ПК 3.3., ПК 3.4., ПК 3.5.
Тема 6. Валидация данных и защита от внедрения кода	ПК 3.3., ПК 3.4., ПК 3.5.
Тема 7. Криптографические методы защиты	ПК 3.3., ПК 3.4., ПК 3.5.
Тема 8. Безопасная работа с файлами и медиа	ПК 3.3., ПК 3.4., ПК 3.5.

5. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРЫ ОЦЕНИВАНИЯ ЗНАНИЙ, УМЕНИЙ, ПРАКТИЧЕСКОГО ОПЫТА, ХАРАКТЕРИЗУЮЩИЕ ЭТАПЫ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ

Изучение дисциплины Обеспечение безопасности веб-приложений является базой для освоения студентами курсов профессионального цикла, формирует базу для овладения профессиональными компетенциями, которые могут быть применены в видах профессиональной деятельности в соответствии с Государственным образовательным стандартом профессионального образования.

В процессе изучения дисциплины предполагается проведение практических занятий для закрепления теоретических знаний, тематика практических занятий учитывает специфику получаемой специальности.

С целью закрепления и систематизации знаний, формирования самостоятельного мышления в программе предусмотрены часы для самостоятельной работы студентов.

При изучении дисциплины - внимание студента будет обращено на её прикладной характер, на то, где и когда изучаемые теоретические положения и практические навыки могут быть использованы в будущей практической деятельности.