ГАОУ ВО «ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ НАРОДНОГО ХОЗЯЙСТВА»

Утверждены решением
Ученого совета ДГУНХ,
протокол № 11
от 06 июня 2023 г

КАФЕДРА «ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

ПО ДИСЦИПЛИНЕ «ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ WEB-ПРИЛОЖЕНИЙ»

НАПРАВЛЕНИЕ ПОДГОТОВКИ 10.03.01
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, ПРОФИЛЬ
«БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ»

Уровень высшего образования - бакалавриат

Махачкала – 2023

УДК 681.518(075.8)
ББК 32.81.73

Составитель – Гасанова Зарема Ахмедовна, кандидат педагогических наук, заместитель заведующего кафедрой «Информационные технологии и информационная безопасность» ДГУНХ.

Внутренний рецензент – Галяев Владимир Сергеевич, кандидат физико-математических наук, доцент, заведующий кафедрой «Информационные технологии и информационная безопасность» ДГУНХ.

Внешний рецензент – Абдурагимов Гусейн Эльдарханович, кандидат физико-математических наук, доцент кафедры прикладной математики Дагестанского государственного университета.

Представитель работодателя - Зайналов Джабраил Тажутдинович, директор регионального экспертно-аттестационного центра «Экспертиза», эксперт-представитель работодателя.

Оценочные материалы по дисциплине «Обеспечение безопасности web-приложений» разработаны в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 Информационная безопасность, утвержденного приказом Министерства образования и науки Российской Федерации от 17 ноября 2020 г., № 1427, в соответствии с приказом Министерства науки и высшего образования Российской Федерации от 6.04.2021 г. № 245 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры»

Оценочные материалы по дисциплине «Обеспечение безопасности web-приложений» размещены на официальном сайте www.dgunh.ru

Гасанова З.А. Оценочные материалы по дисциплине «Обеспечение безопасности web-приложений» для направления подготовки 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем». – Махачкала: ДГУНХ, 2023 г. – 29 с.

Рекомендованы к утверждению Учебно-методическим советом ДГУНХ 05 июня 2023 г.

Рекомендованы к утверждению руководителем основной профессиональной образовательной программы высшего образования – программы бакалавриата по направлению подготовки 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем», к.пед.н., Гасановой З.А.

Одобрены на заседании кафедры «Информационные технологии и информационная безопасность» 31 мая 2023 г., протокол № 10.

СОДЕРЖАНИЕ

Назначение оценочных материалов

Оценочные материалы для текущего контроля успеваемости (оценивания хода освоения дисциплин), для проведения промежуточной аттестации (оценивания промежуточных и окончательных результатов обучения по дисциплине) обучающихся по дисциплине «Обеспечение безопасности web-приложений» на соответствие их учебных достижений поэтапным требованиям образовательной программы высшего образования 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем»

Оценочные материалы по дисциплине «Обеспечение безопасности web-приложений» включают в себя: перечень компетенций с указанием видов оценочных средств в процессе освоения дисциплины; описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания; типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения ОПОП; методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

Оценочные материалы сформированы 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 для достижения успеха.

Основными параметрами и свойствами оценочных материалов являются:

- предметная направленность (соответствие предмету изучения конкретной дисциплины);
- содержание (состав и взаимосвязь структурных единиц, образующих содержание теоретической и практической составляющих дисциплины);
- объем (количественный состав оценочных материалов);
- качество оценочных материалов в целом, обеспечивающее получение объективных и достоверных результатов при проведении контроля с различными целями.

РАЗДЕЛ 1. Перечень компетенций с указанием видов оценочных средств в процессе освоения дисциплины

1.1 Перечень формируемых компетенций

код компетенции	формулировка компетенции
ПК	**ПРОФЕССИОНАЛЬНЫЕ КОМПЕТЕНЦИИ**
ПК-2.	Способен учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации

1.2. Перечень компетенций с указанием видов оценочных средств

Формируемые компетенции	***Код и наименование индикатора достижения компетенции***	***Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций***	***Уровни освоения компетенций***	***Критерии оценивания сформированности компетенций***	***Виды оценочных средств***
ПК-2. Способен учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации	ИПК-2.2. Обеспечивает безопасность информационных технологий, применяемых в автоматизированных системах	**Знать:** - современные технологии обеспечения информационной безопасности web-приложений.	Пороговый уровень	Обучающийся слабо (частично) знает современные технологии обеспечения информационной безопасности web-приложений..	**Блок А –** задания репродуктивного уровня - тестовые задания; - вопросы для устного опроса
			Базовый уровень	Обучающийся с незначительными ошибками и отдельными пробелами знает современные технологии обеспечения информационной	

Формируемые компетенции	*Код и наименование индикатора достижения компетенции*	*Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций*	*Уровни освоения компетенций*	*Критерии оценивания сформированности компетенций*	*Виды оценочных средств*
				безопасности web-приложений.	
			Продвинутый уровень	Обучающийся с требуемой степенью полноты и точности знает современные технологии обеспечения информационной безопасности web-приложений.	
		Уметь: - разрабатывать средства информационной защиты web-приложений и используемых ими баз данных	Пороговый уровень	Обучающийся слабо (частично) умеет разрабатывать средства информационной защиты web-приложений и используемых ими баз данных.	**Блок В** – задания реконструктивного уровня – практические задания; - тематика рефератов; - тематика презентаций.
			Базовый уровень	Обучающийся с незначительными затруднениями умеет разрабатывать средства информационной защиты web-приложений и используемых ими баз данных.	

Формируемые компетенции	***Код и наименование индикатора достижения компетенции***	***Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций***	***Уровни освоения компетенций***	***Критерии оценивания сформированности компетенций***	***Виды оценочных средств***
			Продвинутый уровень	Обучающийся умеет разрабатывать средства информационной защиты web-приложений и используемых ими баз данных.	
		<u>Владеть:</u> – инструментальными средствами разработки безопасных web-приложений.	Пороговый уровень	Обучающийся слабо (частично) владеет инструментальными средствами разработки безопасных web-приложений	**Блок С** – задания практико-ориентированного уровня – лабораторные работы.
			Базовый уровень	Обучающийся с небольшими затруднениями владеет инструментальными средствами разработки безопасных web-приложений	
			Продвинутый уровень	Обучающийся свободно владеет инструментальными средствами разработки безопасных web-приложений	

РАЗДЕЛ 2. Задания, необходимые для оценки планируемых результатов обучения по дисциплине

Для проверки сформированности компетенции ПК-2. Способен учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации
ИПК-2.2. Обеспечивает безопасность информационных технологий, применяемых в автоматизированных системах
Блок А. Задания репродуктивного уровня («знать»)

А.1 Тестовые задания по дисциплине

1. Присвоение какому-либо объекту (субъекту) уникального образа, имени или числа...
Выберите один из 3 вариантов ответа:
1) идентификация
2) аутентификация
3) авторизация

2. Проверка подлинности пользователя путём сравнения введённого им логина/пароля с данными сохранёнными в базе данных...
Выберите один из 3 вариантов ответа:
1) идентификация
2) аутентификация
3) авторизация

3. Процедура предоставления законному объекту соответствующих полномочий и доступных ресурсов системы (сети)...
Выберите один из 3 вариантов ответа:
1) идентификация
2) аутентификация
3) авторизация

4. Возможные воздействия, которые прямо или косвенно могут нанести ущерб ее безопасности...
Выберите один из 3 вариантов ответа:
1) ущерб безопасности
2) угроза безопасности
3) уязвимость системы

5. Установить соответствие...
Укажите соответствие для всех 4 вариантов ответа:
1) удаляет экранирование символов

2) преобразует специальные символы в HTML-сущности
3) удаляет пробелы (или другие символы) из начала и конца строки
4) удаляет теги HTML и PHP из строки
__ htmlspecialchars
__ trim
__ stripslashes
__ strip_tags

6. Атрибут, который указывает регулярное выражение и используется с тегом input...
Выберите один из 4 вариантов ответа:
1) req
2) pattern
3) reg
4) rel

7. Указать соответствующие описания регулярных выражений...
Укажите соответствие для всех 4 вариантов ответа:
1) только латинская буква в любом регистре
2) не менее трёх цифр
3) не более трёх цифр
4) одна цифра от 0 до 9
__ \d [0-9]
__ [A-Za-z]
__ [0-9]{,3}
__ [0-9]{3,}

8. Как с помощью регулярного выражения задать проверку ввода не менее шести латинских букв?
Выберите один из 4 вариантов ответа:
1) [A-Za-z]{0-6}
2) [A-Za-z]{6}
3) [A-Za-z]{,6}
4) [A-Za-z]{6,}

9. Функция, которая создаёт хеш пароля, используя сильный, необратимый алгоритм хеширования,...
Выберите один из 3 вариантов ответа:
1) hash
2) password_verify
3) password_hash

10. Мощность, которая требуется для вычисления хэша, находится по логарифмической шкале $2^{\text{стоимость}}$ и определяет, сколько раз данные проходят через алгоритм хеширования...
Выберите один из 4 вариантов ответа:
1) стоимость
2) соль
3) хэш
4) алгоритм

11. Криптографическими расширениями являются...
Выберите несколько из 6 вариантов ответа:
1) OpenSSL
2) Sodium
3) Hash
4) GD
5) SPL
6) MD5

12. Глобальный массив, который содержит информацию о загруженных на сервер файлах...
Выберите один из 4 вариантов ответа:
1) $_FILES
2) $_SERVER
3) $_PATH
4) $_INFO

13. Функция, которая перемещает загруженный файл в новое место...
Выберите один из 4 вариантов ответа:
1) move_file
2) move_uploaded_file
3) basename
4) move

14. Функция, которая используется для определения типа изображения, ...
Выберите один из 4 вариантов ответа:
1) image_type
2) imagetype
3) exif_imagetype
4) image

15. Функция для получения размера изображения...
Выберите один из 4 вариантов ответа:
1) getimagesize
2) imagesize

3) getsize
4) size

16. Функция, которая возвращает размер файла...
Выберите один из 4 вариантов ответа:
1) filesize
2) sizefile
3) file_size
4) fileinfo

17. Международное сообщество, разрабатывает рекомендации, документацию по защите сайтов...
Выберите один из 4 вариантов ответа:
1) GDPR
2) ASVS
3) W3C
4) OWASP

18. Способ тестирования приложений, в основе которого лежит передача некорректных, случайных или непредвиденных логикой приложения данных...
Выберите один из 4 вариантов ответа:
1) фарминг
2) фаззинг
3) фишинг
4) хэшинг

19. Криптографическая функция, которая использует математический алгоритм для преобразования произвольного массива данных в строку фиксированной длины, состоящую из цифр и букв...
Выберите один из 3 вариантов ответа:
1) скрипт-функция
2) хэш-функция
3) функция шифрования

20. Строка данных, которая передаётся хеш-функции вместе с входным массивом данных для вычисления хэша...
Выберите один из 4 вариантов ответа:
1) соль
2) стоимость
3) шифр
4) хэш

21. Особый тип атаки на стороне сервера или SSRF-атаки, связанный с злоупотреблением функциями в XML-синтаксических парсерах...

Выберите один из 4 вариантов ответа:
1) XXE-инъекции
2) SQL-инъекции
3) XSS-инъекции
4) XML-инъекции

22. Тестирование «белого ящика», позволяет находить уязвимости безопасности в исходном коде приложения на ранних этапах жизненного цикла разработки приложения...
Выберите один из 4 вариантов ответа:
1) SAST
2) XSS
3) XSD
4) DAST

23. Тестирование «черного ящика», позволяет обнаруживать уязвимости и слабые места в работающем приложении...
Выберите один из 4 вариантов ответа:
1) DAST
2) IAST
3) RASP
4) XSS

24. Интерактивное тестирование безопасности приложений...
Выберите один из 4 вариантов ответа:
1) DAST
2) IAST
3) RASP
4) XSS

25. Одна из разновидностей атак на веб-системы, которая подразумевает внедрение вредоносного кода на определенную страницу сайта и взаимодействие этого кода с удаленным сервером злоумышленников при открытии страницы пользователем...
Выберите один из 4 вариантов ответа:
1) OWASP
2) SQL
3) XSS
4) XXE

26. Защиту безопасности приложений во время выполнени обеспечивает...
Выберите один из 4 вариантов ответа:
1) DAST
2) IAST

3) RASP
4) XSS

27. Наиболее простой формат, представляющий собой набор произвольных пар имя/значение в формате кодирования HTML form....
Выберите один из 3 вариантов ответа:
1) Simple Web Token (SWT)
2) JSON Web Token (JWT)
3) Security Assertion Markup Language (SAML)

28. Функция, которая генерирует и обновляет идентификатор текущей сессии...
Выберите один из 4 вариантов ответа:
1) session_regenerate_id
2) session_id
3) session_start
4) session_update

29. INI-настройки безопасности сессий, не позволяющая сессионному модулю использовать неинициализированные идентификаторы сессий...
Выберите один из 4 вариантов ответа:
1) session.cache_limiter
2) session.use_trans_sid
3) session.use_strict_mode
4) session.hash_function

30. Криптографический сетевой протокол, обеспечивающий безопасный удаленный доступ и управление...
Выберите один из 4 вариантов ответа:
1) SSH
2) SSL
3) XML
4) TCP

31. Криптографический протокол, обеспечивающий безопасность при соединении между браузером пользователя и сервером на основе SSL-сертификата...
Выберите один из 4 вариантов ответа:
1) SSH
2) SSL
3) XML
4) TCP

32. Уязвимость, которая возникает из-за недостаточной фильтрации вводимых пользователем данных, что позволяет модифицировать запросы к базам данных...
Выберите один из 4 вариантов ответа:

1) SQL-инъекция
2) XXS-инъекция
3) XML-инъекция
4) GET-инъекция

33. Функция, которая используется для создания допустимых в SQL-строк, которые можно использовать в SQL-выражениях...
Выберите один из 4 вариантов ответа:
1) mysqli_set_charset
2) mysqli_real_escape_string
3) prepare
4) mysqli_character_set_name

34. Функция, которая задаёт набор символов по-умолчанию, который будет использоваться при обмене данными с сервером баз данных...
Выберите один из 4 вариантов ответа:
1) mysqli_set_charset
2) mysqli_real_escape_string
3) prepare
4) mysqli_character_set_name

35. Уязвимость, которая заключается во внедрении кода, исполняемого на стороне клиента (JavaScript) в веб-страницу, которую просматривают пользователи...
Выберите один из 4 вариантов ответа:
1) XSS (Межсайтовый скриптинг)
2) SQL-инъекция
3) фишинг
4) JS-инъекция

36. Тип атак, при которой злоумышленник может вставить поддельную форму для входа на страницу, используя манипуляции DOM, установив action атрибуты формы на свой собственный сервер, получить конфиденциальную информацию...
Выберите один из 4 вариантов ответа:
1) фарминг
2) фишинг
3) межсайтовый скриптинг
4) токен-атака

А2. Вопросы для устного опроса

1. Виды уязвимостей web-приложения.
2. Принципы безопасного использования интернет-сайтов.
3. Классификация угроз информационной безопасности.

4. Способы аутентификации пользователей.
5. Технологии и инструменты обеспечения информационной безопасности на этаперазработки web-приложения.
6. Технологии и инструменты обеспечения информационной безопасности на этапетестирования web-приложения.
7. Технологии и инструменты обеспечения информационной безопасности на этапевнедрения web-приложения.
8. Технологии и инструменты обеспечения информационной безопасности на этапеиспользования web-приложения.
9. Защищенные и незащищенные протоколы передачи данных и их использование.
10. Виды DDoS-атак. Обнаружение DDoS-атак.
11. Причины возникновения уязвимостей типа Injection.
12. Подсистемы защиты web-порталов от информационных атак

Блок В. Задания реконструктивного уровня («уметь»)

В1. Практические задания

1. Написать SQL-запрос на получение имени таблиц базы данных и последующееполучение данных из найденных таблиц
2. Написать запрос на получение первого символа у второй записи в таблице.

В2. Тематика рефератов

1. Основные принципы построения безопасных сайтов
2. Понятие безопасности приложений и классификация опасностей
3. Источники угроз информационной безопасности и меры по их предотвращению
4. Регламенты и методы разработки безопасных веб-приложений
5. Безопасная аутентификация и авторизация
6. Повышение привилегий и общая отказоустойчивость системы
7. Проверка корректроности данных, вводимых пользователем
8. Публикация изображений и файлов.
9. Методы шифрования.
10. SQL-инекция.
11. XSS-инъекции
12. Планирование, организация и проектирование web-сайта.
13. Основы web-технологий
14. Web-дизайн

В3. Тематика презентаций

1. Основные принципы построения безопасных сайтов
2. Понятие безопасности приложений и классификация опасностей
3. Источники угроз информационной безопасности и меры по их предотвращению
4. Регламенты и методы разработки безопасных веб-приложений
5. Безопасная аутентификация и авторизация
6. Повышение привилегий и общая отказоустойчивость системы
7. Проверка корректроности данных, вводимых пользователем
8. Публикация изображений и файлов.
9. Методы шифрования.
10. SQL-инекция.
11. XSS-инъекции
12. Планирование, организация и проектирование web-сайта.
13. Основы web-технологий
14. Web-дизайн

Блок С. Задания практикоориентированного уровня для диагностирования сформированности компетенций («владеть»)

С.1. Лабораторная работа

Темы лабораторных работ

Лабораторная работа 1. «Анализ внутренних и внешних угроз информационной безопасности **web**-приложения**».**

1. Приведите примеры внутренних угроз безопасности web-приложения.
2. Приведите примеры внешних угроз безопасности web-приложения.
3. Опишите основные методы анализа уязвимостей web-приложения.

Лабораторная работа 2. «Разработка проекта по построению системы защиты **web**-приложения**».**

1. Приведите примеры отечественных и иностранных стандартов информационнойбезопасности.
2. Опишите безопасный цикл разработки web-приложения.
3. Какие языки программирования используются для разработки web-приложений.

Лабораторная работа 3. «Разработка клиентской части модуля безопасности **web**-приложения**».**

1. Для чего используется Content Security Policy?
2. Что такое межсетевые запросы?
3. Опишите механизм атаки CRLF-инъенкции, направленной на пользователя web-приложения.

Лабораторная работа 4. «Разработка серверной части модуля безопасности **web**-приложения**».**

1. Какие серверные операционные системы чаще всего используют в сети Интернет?
2. Что такое виртуальные хосты в web-серверах Apache и Nginx?
3. Приведите примеры архитектурных анти-паттернов, связанных с безопасностью.

Лабораторная работа 5. «Разработка средств защиты базы данных **web**-приложения**».**

1. Опишите цикл безопасной обработки данных.
2. Что такое «SQL-инъекция»?
3. Перечислите способы борьбы с SQL-инъекциями.

Лабораторная работа 6. «Нагрузочное тестирование **web**-приложения**».**

1. Что такое тестирование на проникновение?
2. Для чего нужен балансировщик нагрузки?
3. Влияет ли использование скриптовых языков программирования (например, PHP) напроизводительность web-сервера?

Лабораторная работа 7. «Исследование **web**-приложения на уязвимости**».**

1. Что такое межсайтовый скриптинг?
2. Что такое «XML-инъекция»?
3. Что такое инъекции в HTTP-заголовки?

Лабораторная работа 8. «Создание сценариев атаки и защиты **web**-приложения**».**

1. Поясните суть атак «грубая сила» и «переполнение буфера».
2. Поясните суть атаки «инъекция команд в протоколы электронной почты».
3. Поясните суть атаки «злоупотребление функциональностью».

Лабораторная работа 9. «Настройка специального программного обеспечения для мониторинга безопасной работы **web**-приложений**».**

1. Как используются защищенные и незащищенные протоколы передачи данных?
2. Приведите примеры антивирусов, используемых для организации безопасности web-серверов.
3. Опишите возможную митигацию для всех угроз, найденных приложением

Блок Д. Задания для использования в рамках промежуточной аттестации

Д1. Перечень контрольных вопросов

1. Проблемы безопасности web-приложений.
2. Внутренние и внешние угрозы информационной безопасности web-приложения.
3. Технологии безопасной передачи информации в сети Интернет.
4. Жизненный цикл защиты web-приложения.
5. Технологии и средства безопасной разработки web-приложения.

6. Технологии и средства безопасного развертывания web-приложения.
7. Технологии и средства безопасного использования web-приложения.
8. Основы тестирования безопасности web-приложения.
9. Разработка клиентской части модуля безопасности web-приложения.
10. Разработка серверной части модуля безопасности web-приложения.
11. Средства защиты базы данных web-приложения.
12. Основные виды Интернет-угроз и методы защиты от них.
13. Подсистемы защиты web-порталов от информационных атак.
14. Особенности исследования web-приложения на уязвимости.
15. Специальное программное обеспечение для мониторинга безопасной работы web-приложений.

РАЗДЕЛ 3. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Балльно-рейтинговая система является базовой системой оценивания сформированности компетенций обучающихся очной формы обучения.

Итоговая оценка сформированности компетенции(й) обучающихся в рамках балльно-рейтинговой системы осуществляется в ходе текущего контроля успеваемости, промежуточной аттестации и определяется как сумма баллов, полученных обучающимися в результате прохождения всех форм контроля.

Оценка сформированности компетенции по дисциплине складывается из двух составляющих:

✓ первая составляющая – оценка преподавателем сформированности компетенции в течение семестра в ходе текущего контроля успеваемости (максимум 100 баллов). Структура первой составляющей определяется технологической картой дисциплины, которая в начале семестра доводится до сведения обучающихся;

✓ вторая составляющая – оценка сформированности компетенции обучающихся на зачете (максимум – 20 баллов).

Для студентов очно-заочной формы обучения применяется 4-балльная и бинарная шкалы оценивания результатов текущего контроля успеваемости и промежуточной аттестации обучающихся.

уровни освоения компетенций	продвинутый уровень	базовый уровень	пороговый уровень	допороговый уровень
100 – балльная шкала	85 и ≥	70 – 84	51 – 69	0 – 50
Бинарная шкала	Зачтено			Не зачтено

Шкала оценок при текущем контроле успеваемости по различным показателям

Показатели оценивания сформированности компетенций	***Баллы***	***Оценка***
Устный опрос	0-5	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»
Подготовка реферата	0-5	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»
Подготовка презентации	0-5	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»
Практическая работа	0-10	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»
Тестирование	0-30	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»
Выполнение лабораторной работы	0-15	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»

Соответствие критериев оценивания уровню освоения компетенций по текущему контролю успеваемости

Баллы	***Оценка***	***Уровень освоения компетенций***	***Критерии оценивания***
0-50	«неудовлетворительно»	Допороговый уровень	Обучающийся не приобрел знания, умения и не владеет компетенциями в объеме, закрепленном рабочей программой дисциплины
51-69	«удовлетворительно»	Пороговый уровень	Не менее 50% заданий, подлежащих текущему контролю успеваемости,

			выполнены без существенных ошибок
70-84	«хорошо»	Базовый уровень	Обучающимся выполнено не менее 75% заданий, подлежащих текущему контролю успеваемости, или при выполнении всех заданий допущены незначительные ошибки; обучающийся показал владение навыками систематизации материала и применения его при решении практических заданий; задания выполнены без ошибок
85-100	«отлично»	Продвинутый уровень	100% заданий, подлежащих текущему контролю успеваемости, выполнены самостоятельно и в требуемом объеме; обучающийся проявляет умение обобщать, систематизировать материал и применять его при решении практических заданий; задания выполнены с подробными пояснениями и аргументированными выводами

Шкала оценок по промежуточной аттестации

Наименование формы промежуточной аттестации	***Баллы***	***Оценка***
Зачет	0-20	«не зачтено» «зачтено»

Соответствие критериев оценивания уровню освоения компетенций по промежуточной аттестации обучающихся

Баллы	***Оценка***	***Уровень освоения компетенций***	***Критерии оценивания***
0-9	«не зачтено»	Допороговый уровень	Обучающийся не приобрел знания, умения и не владеет компетенциями в объеме, закрепленном рабочей программой дисциплины; обучающийся не смог ответить на вопросы
10-14	«зачтено»	Пороговый уровень	Обучающийся дал неполные ответы на вопросы, с недостаточной аргументацией, практические задания выполнены не полностью,

			компетенции, осваиваемые в процессе изучения дисциплины сформированы не в полном объеме.
15-17	«зачтено»	Базовый уровень	Обучающийся в целом приобрел знания и умения в рамках осваиваемых в процессе обучения по дисциплине компетенций; обучающийся ответил на все вопросы, точно дал определения и понятия, но затрудняется подтвердить теоретические положения практическими примерами; обучающийся показал хорошие знания по предмету, владение навыками систематизации материала и полностью выполнил практические задания
18-20	«зачтено»	Продвинутый уровень	Обучающийся приобрел знания, умения и навыки в полном объеме, закрепленном рабочей программой дисциплины; терминологический аппарат использован правильно; ответы полные, обстоятельные, аргументированные, подтверждены конкретными примерами; обучающийся проявляет умение обобщать, систематизировать материал и выполняет практические задания с подробными пояснениями и аргументированными выводами

РАЗДЕЛ 4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков, характеризующие этапы формирования компетенций

Устный опрос проводится в первые 15 минут занятий семинарского типа в формате обсуждения с названными преподавателем студентами. Остальные обучающиеся вправе дополнить или уточнить ответ по своему желанию (соблюдаю очередность ответа). Основной темой для опроса являются вопросы для обсуждения, соответствующие теме предыдущей лекции, но преподаватель может уточнять задаваемый вопрос, задавать наводящие вопросы или сужать вопрос до

отдельного аспекта обсуждаемой темы.

Методика оценивания ответов на устные вопросы

Баллы	***Оценка***	***Показатели***	***Критерии***
5	«отлично»	1. Полнота данных ответов; 2. Правильность ответов на вопросы.	Полно и аргументировано даны ответы по содержанию задания. Обнаружено понимание материала, может обосновать свои суждения, привести необходимые примеры. Изложение материала последовательно и правильно.
3-4	«хорошо»		Студент дает ответ, удовлетворяющий тем же требованиям, что и для оценки «отлично», но допускает 1-2 ошибки, которые сам же исправляет.
1-2	«удовлетворительно»		Студент обнаруживает знание и понимание основных положений данного задания, но: 1) излагает материал неполно и допускает неточности в определении понятий или формулировке правил; 2) не умеет достаточно глубоко и доказательно обосновать свои суждения и привести свои примеры; 3) излагает материал непоследовательно и допускает ошибки.
0	«неудовлетвори-тельно»		Студент обнаруживает незнание ответа на соответствующее задание, допускает ошибки в формулировке определений и правил, искажающие их смысл, беспорядочно и неуверенно излагает материал.

Тестирование проводится с помощью системы дистанционного обучения «Прометей», входящей в состав электронной информационно-образовательной среды Дагестанского государственного университета народного хозяйства.

На тестирование отводится 45 минут. Каждый вариант тестовых заданий включает 30 вопросов.

Методика оценивания выполнения тестов

Баллы	**Оценка**	**Показатели**	**Критерии**
25-30	«отлично»	1. Полнота выполнения тестовых заданий; 2. Своевременность выполнения;	Выполнено более 85 % заданий предложенного теста, в заданиях открытого типа дан полный, развернутый ответ на поставленный вопрос
19-24	«хорошо»		Выполнено более 70 % заданий

		3. Правильность ответов на вопросы.	предложенного теста, в заданиях открытого типа дан полный, развернутый ответ на поставленный вопрос; однако были допущены неточности в определении понятий, терминов и др.
15-18	«удовлетворительно»		Выполнено более 54 % заданий предложенного теста, в заданиях открытого типа дан неполный ответ на поставленный вопрос, в ответе не присутствуют доказательные примеры, текст со стилистическими и орфографическими ошибками.
0-14	«неудовлетвори-тельно»		Выполнено не более 53 % заданий предложенного теста, на поставленные вопросы ответ отсутствует или неполный, допущены существенные ошибки в теоретическом материале (терминах, понятиях).

Тема реферата выбирается студентом самостоятельно из предложенного списка с учетом минимизации количества повторений выбранных тем. На написание реферата отводится одна неделя. Реферат оформляется согласно действующим в Дагестанском государственном университете народного хозяйства требованиям к оформлению письменных работ. Объем представленного реферата должен быть не менее 10 страниц машинописного текста без учета титульного листа.

Публичная защита реферата проводится в присутствии остальных студентов, защищающих рефераты. На выступление отводится не более 5 минут. Во время выступления студент должен обозначить основную цель реферата, а также цельно сформулировать базовую идею, отраженную в реферате.

Методика оценивания выполнения рефератов

Баллы	***Оценка***	***Показатели***	***Критерии***
5	«отлично»	1. Полнота выполнения рефератов; 2. Своевременность выполнения; 3. Четкость изложения идеи реферата во время защиты.	Выполнены все требования к написанию и защите реферата: обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объём, соблюдены требования к внешнему оформлению, четкое и последовательное выступление во время защиты.

3-4	«хорошо»		Основные требования к реферату и его защите выполнены, но при этом допущены недочеты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объем реферата; имеются упущения в оформлении; выступление во время защиты требует дополнительных вопросов.
1-2	«удовлетворительно»		Имеются существенные отступления от требований к реферированию. В частности: тема освещена лишь частично; допущены фактические ошибки в содержании реферата или при ответе на дополнительные вопросы во время выступления.
0	«неудовлетвори-тельно»		Тема реферата не раскрыта, обнаруживается существенное непонимание проблемы, не проведена защита реферата.

Тема презентации выбирается студентом самостоятельно из предложенного списка с учетом минимизации количества повторений выбранных тем. На подготовку презентации отводится одна неделя.

Публичная презентация проводится в присутствии остальных студентов. На выступление отводится не более 5 минут. Во время выступления студент должен обозначить основную цель презентации, а также цельно сформулировать базовую идею.

Методика оценивания выполнения презентаций

Баллы	***Оценка***	***Показатели***	***Критерии***
5	«отлично»	4. Полнота выполнения; 5. Своевременность выполнения; 6. Четкость изложения идеи презентации во время защиты.	Выполнены все требования к подготовке презентации: обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объём, соблюдены требования к внешнему оформлению, четкое и последовательное выступление во время демонстрации.
3-4	«хорошо»		Основные требования к подготовке презентации выполнены, но при этом допущены недочеты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в

			суждениях; не выдержан объем презентации; имеются упущения в оформлении; выступление во время демонстрации требует дополнительных вопросов.
1-2	«удовлетворительно»		Имеются существенные отступления от требований к презентации. В частности: тема освещена лишь частично; допущены фактические ошибки в содержании презентации или при ответе на дополнительные вопросы во время выступления.
0	«неудовлетвори-тельно»		Тема презентации не раскрыта, обнаруживается существенное непонимание проблемы, не проведена демонстрация презентации.

Практические задание выполняются непосредственно во время занятий семинарского типа (одно задание на одну пару согласно текущей тематике занятия). Студенты должны выполнять задание самостоятельно, но имеют возможность обратиться к преподавателю за разъяснениями постановки задачи или оценкой правильности представленного решения. Если преподаватель вынужден разъяснять аспекты непосредственного выполнения задания, то это негативно отражается на оценке выполняющего задание студента.

Методика оценивания выполнения задач

Баллы	***Оценка***	***Показатели***	***Критерии***
9-10	«отлично»	1. Полнота выполнения задания; 2. Своевременность выполнения задачи; 3. Самостоятельность решения.	Основные требования к выполнению задания выполнены. Продемонстрировано умение анализировать ситуацию и находить оптимальное количества решений, умение работать с информацией, в том числе умение затребовать дополнительную информацию, необходимую для достижения поставленной цели
6-8	«хорошо»		Основные требования к выполнению задания реализованы, но при этом допущены недочеты. В частности, недостаточно раскрыты навыки критического оценивания различных точек зрения, осуществление самоанализа, самоконтроля и самооценки, креативности, нестандартности предлагаемых решений
3-5	«удовлетворительно»		Имеются существенные отступления от выполнения работы. В частности отсутствуют навыки умения моделировать решения в соответствии с заданием, представлять различные подходы к разработке планов

			действий, ориентированных на конечный результат
1-2	«неудовле твори-тельно»		Задача не нешена, обнаруживается существенное непонимание проблемы

Лабораторные работы выполняются в специализированной аудитории во время лабораторных занятий. Предусмотрено выполнение одной лабораторной работы в течение одного занятия согласно текущей тематике. Студенты должны выполнять задание самостоятельно, но имеют возможность обратиться к преподавателю за разъяснениями постановки задачи или оценкой правильности полученного результата. Если преподаватель вынужден разъяснять аспекты непосредственного выполнения шагов лабораторной работы, то это негативно отражается на оценке выполняющего задание студента.

Методика оценивания выполнения *лабораторных работ*

Баллы	***Оценка***	***Показатели***	***Критерии***
13-15	«отлично»	4. Полнота выполнения задания лабораторной работы; 5. Своевременность выполнения задания лабораторной работы; 6. Самостоятельность решения.	Основные требования к выполнению задания лабораторной работы выполнены. Продемонстрировано умение анализировать ситуацию и находить оптимальное количества решений, умение работать с информацией, в том числе умение затребовать дополнительную информацию, необходимую для достижения поставленной цели
9-12	«хорошо»		Основные требования к выполнению задания лабораторной работы реализованы, но при этом допущены недочеты. В частности, недостаточно раскрыты навыки критического оценивания различных точек зрения, осуществление самоанализа, самоконтроля и самооценки, креативности, нестандартности предлагаемых решений
5-8	«удовлетв орительно »		Имеются существенные отступления от выполнения лабораторной работы. В частности отсутствуют навыки умения моделировать решения в соответствии с заданием, представлять различные подходы к разработке планов действий, ориентированных на конечный результат
0-4	«неудовле твори-тельно»		Шаги выполнения лабораторной работы не выполнены, обнаруживается существенное непонимание проблемы.

Зачет принимается в письменной форме на последнем практическом занятии. В задании к зачету даются два теоретических вопроса и одна задача. Студенту предоставляется 90 минут для письменного изложения ответов на

вопросы и решению задачи. За ответы на теоретические вопросы студент максимально может получить 14 баллов. За решение задачи – максимально 6 баллов. Проходной балл на зачете – 12 баллов.

Методика оценивания ответов на зачете

Баллы	Оценка	Показатели	Критерии
12-20	«Зачтено»	*1.* Полнота изложения теоретического материала; *2.* Полнота и правильность решения практического задания; *3.* Правильность и/или аргументированность изложения (последовательность действий); *4.* Самостоятельность ответа т.д.	Дан полный, в логической последовательности развернутый ответ на поставленный вопрос, где обучающийся продемонстрировал знание дисциплины в полном объеме учебной программы, достаточно глубоко осмысливает дисциплину, самостоятельно и исчерпывающе отвечает на дополнительные вопросы, приводит собственные примеры по проблематике поставленного вопроса, решил предложенные практические задания без ошибок. Дан развернутый ответ на поставленный вопрос, где студент демонстрирует знания, приобретенные на лекционных и семинарских занятиях, а также полученные посредством изучения обязательных учебных материалов по курсу, дает аргументированные ответы, приводит примеры. Однако допускается неточность в ответе. Решил предложенные практические задания с небольшими неточностями. Дан ответ, свидетельствующий в основном о знании процессов изучаемой дисциплины, 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. Допускается несколько ошибок в содержании ответа и решении практических

			заданий.
0-11	«Не зачтено»		Дан ответ, который содержит ряд серьезных неточностей, обнаруживающий незнание процессов изучаемой предметной области, отличающийся неглубоким раскрытием темы, незнанием основных вопросов теории, несформированными навыками анализа явлений, процессов, неумением давать аргументированные ответы. Выводы поверхностны. Решение практических заданий не выполнено, т.е. студент не способен ответить на вопросы даже при дополнительных наводящих вопросах преподавателя.

Лист актуализации оценочных материалов по дисциплине «Обеспечение безопасности web-приложений»

Оценочные материалы пересмотрены,
обсуждены и одобрены на заседании кафедры

Протокол от «_____»_____ 20___ г. №_____

Зав. кафедрой _____

Оценочные материалы пересмотрены,
обсуждены и одобрены на заседании кафедры

Протокол от «_____»_____ 20___ г. №_____

Зав. кафедрой _____

Оценочные материалы пересмотрены,
обсуждены и одобрены на заседании кафедры

Протокол от «_____»_____ 20___ г. №_____

Зав. кафедрой _____

Оценочные материалы пересмотрены,
обсуждены и одобрены на заседании кафедры

Протокол от «_____»_____ 20___ г. №_____

Зав. кафедрой _____