

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Шебзухова Татьяна Александровна

Должность: Директор Пятигорского института (филиал) Северо-Кавказского

федерального университета

Дата подписания: 13.06.2024 15:51:50

Уникальный программный ключ:

d74ce93cd40e39275c3ba2f58486412a1c8ef96f

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Северо-Кавказский федеральный университет»
Пятигорский институт (филиал) СКФУ
Колледж Пятигорского института (филиал) СКФУ

УТВЕРЖДАЮ

Директор Пятигорского института
(филиал) СКФУ
Т.А. Шебзухова

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по профессиональному модулю
информации

ПМ.05 Веб технологии и защита

Специальность 09.02.01 Компьютерные системы и комплексы

Форма обучения очная

Пятигорск

Фонд оценочных средств по профессиональному модулю ПМ.05 Веб технологии и защита информации разработан на основании федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.01 Компьютерные системы и комплексы.

Разработчики:

- 1 Хаджиев А.А., преподаватель колледжа Пятигорского института (филиал) СКФУ

фамилия, имя, отчество, ученая степень, ученое звание, место работы преподавателя

- 2 Темирбулатова Х.А., преподаватель колледжа Пятигорского института (филиал) СКФУ

фамилия, имя, отчество, ученая степень, ученое звание, место работы преподавателя

СОГЛАСОВАНО:

Представитель работодателя

Зам. Генерального директора
ООО «Миллениум - Сервис»

должность представителя работодателя, наименование
организации и город ее расположения

Давыдов А.А.

Фамилия, инициалы

1. Паспорт фонда оценочных средств

1.1. Область применения

Фонд оценочных средств (далее - ФОС) предназначен для проверки результатов освоения вида деятельности (ВД) Веб технологии и защита информации и составляющих его профессиональных и общих компетенций, образовательной программы СПО по специальности 09.02.01 Компьютерные системы и комплексы.

ФОС разработан на основании ФГОС, образовательной программы СПО и рабочей программы профессионального модуля ПМ.05 Веб технологии и защита информации (далее - ПМ).

1.2. Планируемые результаты освоения профессионального модуля

Результатом освоения ПМ является готовность обучающегося к выполнению вида профессиональной деятельности (в соответствии с рабочей программой ПМ) и сформированность профессиональных и общих компетенций.

Формой аттестации по ПМ является экзамен по модулю.

2. Формы контроля и оценивания элементов профессионального модуля

Таблица 1

Элемент профессионального модуля	Форма контроля и оценивания	
	Промежуточная аттестация	Текущий контроль
МДК.05.01 Персональная кибербезопасность	Дифференцированный зачет	Контрольный срез
МДК.05.02 Техническая защита информации	Дифференцированный зачет	Контрольный срез
МДК.05.03 Компьютерная графика	Дифференцированный зачет	Контрольный срез
МДК.05.04 Веб программирование	Дифференцированный зачет	Контрольный срез
УП.05.01 Учебная практика	Дифференцированный зачет	
ПМ (в целом)	Экзамен по модулю	

3. Результаты освоения профессионального модуля

3.1. Оценка профессиональных и общих компетенций

В результате контроля и оценки по ПМ осуществляется комплексная проверка следующих профессиональных и общих компетенций:

Таблица 2

Профессиональные компетенции	Показатели оценки результата
ПК 4.1	Обрабатывать информацию с использованием современных технических средств.
ПК 4.2	Работать с информационными системами приема, обработки и регистрации обращений клиентов.

Общие компетенции	Показатели оценки результата
ОК 01	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам
ОК 02	Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности.
ОК 04	Эффективно взаимодействовать и работать в коллективе и команде.
ОК 09	Пользоваться профессиональной документацией на государственном и иностранном языках.

3.2. Общие и (или) профессиональные компетенции, проверяемые дополнительно: (не предусмотрено)

3.3. Требования к портфолио: (не предусмотрено)

3.4. Требования к курсовому проекту: представлены в методических указаниях к выполнению курсового проекта.

4. Оценка освоения теоретического курса профессионального модуля

4.1. Оценочные средства текущего контроля успеваемости и критерии оценки

МДК.05.01 Персональная кибербезопасность

Комплект заданий для контрольного среза

1-й вариант

1. Основные понятия кибербезопасности.
2. Социальные причины киберпреступлений.
3. Методы защиты данных.
4. Электронная цифровая подпись.

2-й вариант

1. Кибербезопасность и информационная безопасность.
2. Экономические причины киберпреступлений.
3. Криптография.
4. Криптостойкость.

3-й вариант

1. Составляющие информационной безопасности.
2. Правовые причины киберпреступлений.
3. Криптоанализ.
4. Электронная цифровая подпись.

4-й вариант

1. Уровни критической инфраструктуры.
2. Проблемы кибербезопасности.
3. Криптология.
4. Криптостойкость.

МДК.05.02 Техническая защита информации

Комплект заданий для контрольного среза

1-й вариант

1. Анализ источников, каналов распространения и каналов утечки информации.
2. Требования к безопасности информационных систем.

2-й вариант

1. Проведение анализа информации на предмет целостности.
2. Оценка состояния безопасности ИС США.

3-й вариант

1. Требования к безопасности информационных систем в России.
2. Оценка уязвимости информации.

МДК.05.03 Веб графика

Комплект заданий для контрольного среза

1-й вариант

1. Компьютерная графика.
2. Классификация изображений.
3. Достоинства и недостатки КГ.
4. Программы для работы с растровой графикой.

2-й вариант

1. Этапы развития компьютерной графики.
2. Произвольное сканирование луча и растровое сканирование луча.
3. Разрешение изображения.
4. Понятие раstra.

3-й вариант

1. Сферы применения КГ.
2. Классификация КГ.

- 3.Виды компьютерной графики.
- 4.Программы для работы с векторной графикой.

4-й вариант

- 1.Свет и цвет.
- 2.Теория цвета.
- 3.Запоминающие трубки и плазменная панель.
- 4.Жидкокристаллические индикаторы, электролюминесцентные индикаторы, дисплеи с эмиссией полем.

МДК.05.04 Веб программирование

Комплект заданий для контрольного среза

1-й вариант

- 1.Развитие HTML.
- 2.Адаптивность.
- 3.Развитие языков Веб программирования.
- 4.Основные теги.

2-й вариант

- 1.Развитие Веб-серверов.
- 2.Адаптивная верстка.
- 3.Развитие мультимедийных платформ.
- 4.Ссылки.

Критерии оценивания компетенций

Оценка «5» (отлично) выставляется в случае полного выполнения контрольного среза, отсутствия ошибок, грамотного текста, точность формулировок и т.д.

Оценка «4» (хорошо) выставляется в случае полного выполнения всего объема контрольного среза при наличии несущественных ошибок, не повлиявших на общий результат работы и т.д.

Оценка «3» (удовлетворительно) выставляется в случае недостаточно полного выполнения всех разделов контрольного среза, при наличии ошибок, которые не оказали существенного влияния на окончательный результат, при очень ограниченном объеме используемых понятий и т.д.

Оценка «2» (неудовлетворительно) выставляется в случае, если допущены принципиальные ошибки, контрольный срез выполнен крайне небрежно и т.д.

4.2. Оценочные средства промежуточной аттестации и критерии оценки

Промежуточная аттестация по всем МДК проводится в форме дифференцированного зачета.

5. Фонд оценочных средств для экзамена по модулю

1. Паспорт

Назначение: ФОС предназначен для контроля и оценки результатов освоения профессионального модуля ПМ.05 Веб технологии и защита информации по специальности 09.02.01 Компьютерные системы и комплексы

Профессиональные компетенции	Показатель оценки результатов
ПК 4.1. Обращаться с информацией с использованием современных технических средств.	- обрабатывать информацию с использованием современных технических средств.
ПК 4.2. Работать с информационными системами приема, обработки и регистрации обращений клиентов.	- работать с информационными системами приема, обработки и регистрации обращений клиентов.

Общие компетенции	Показатель оценки результатов
ОК 01. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам.	- выбирать способы решения задач профессиональной деятельности применительно к различным контекстам.
ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности.	- использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности.
ОК 04. Эффективно взаимодействовать и работать в коллективе и команде.	- эффективно взаимодействовать и работать в коллективе и команде.
ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.	- пользоваться профессиональной документацией на государственном и иностранном языках.

2. Вопросы к экзамену по профессиональному модулю

МДК.05.01 Персональная кибербезопасность

1. Кибербезопасность и информационная безопасность.
2. Составляющие информационной безопасности.
3. Уровни критической инфраструктуры.
4. Социальные причины киберпреступлений.
5. Экономические причины киберпреступлений.
6. Правовые причины киберпреступлений.
7. Проблемы кибербезопасности.
8. Методы защиты данных.
9. Криптография.
10. Криптоанализ.
11. Криптология.

12. Криптостойкость.
13. Электронная цифровая подпись.
14. Требования к системе защиты информации.
15. Криптографические атаки.
16. Виды атак.
17. Принцип Керкхоффа.
18. Виды шифрования данных.
19. Симметричное шифрование.
20. Ассиметричное шифрование.
21. Криптоанализ.
22. Частотный анализ.
23. Метод полного перебора.
24. Атака по ключам.
25. Криптоанализ симметричных шифров.
26. Криптоанализ асимметричных шифров.
27. Криптоанализ по побочным каналам.
28. Компьютерный вирус.
29. Червь.
30. Троянские программы.
31. Логические бомбы.
32. Файловые вирусы.
33. Стелс вирус.
34. Полиморфные вирусы.
35. Антивирусные программы.
36. Брандмауэр.
37. Firewall.
38. Аппаратная защита информации.
39. Виды аппаратных средств защиты.
40. Защита от НСД.
41. Методы аутентификации.
42. Дактилоскопия.
43. Динамические методы биометрической аутентификации.
44. Верификация подписи.
45. Защита биометрических данных.
46. Идентификация.
47. Аутентификация.
48. Авторизация.
49. Многофакторная аутентификация.
50. Однофакторная двухэтапная аутентификация.
51. Электронная цифровая подпись.
52. Виды электронных цифровых подписей.
53. Применение разных видов подписей.

МДК.05.02 Техническая защита информации

1. Лицензирование деятельности в области защиты конфиденциальной информации.
2. Виды деятельности по ТЗИ подлежащие лицензированию.
3. Лицензионные требования.
4. Действия, приводящие к неправомерному овладении конфиденциальной информацией.
5. Демаскирующие признаки объектов.
6. Классификация демаскирующих признаков.
7. Техническая разведка.
8. Классификация технических разведок.
9. Технические каналы утечки информации.
10. Материально-вещественный канал утечки информации.
11. Оптический канал утечки информации.
12. Каналы утечки речевой информации.
13. Закладное устройство.
14. Классификация закладных устройств.
15. Типы закладных устройств.
16. Основные характеристики закладных устройств.
17. Лазерные системы акустической разведки. Принцип работы.
18. Способы скрытого видеонаблюдения и съёмки.
19. Основные характеристики современных скрытых камер.
20. Возможности систем видеонаблюдения и съёмки.
21. Средства перехвата радиосигналов.
22. Средства и методы пеленгации источника радиосигнала,
23. Сканирующие радиоприёмники: назначение, основные характеристики.
24. Перехват информации в каналах сотовой связи.
25. Утечка информации в волоконно-оптических линиях связи
26. Методы выявления закладных устройств.
27. Средства выявления закладных устройств.
28. Технические средства подавления сигналов радио закладных устройств.
29. Демаскирующие признаки закладных устройств.
30. Методы подавления записи речевой информации на диктофон.
31. Способы и средства подавления.
32. Пассивные методы защиты речевой информации от её утечки через ограждающие конструкции.
33. Рекомендации по выбору ограждающих конструкций.
34. Организация защиты речевой информации от утечки по техническим каналам в защищаемом помещении.
35. Основные способы и методы защита информации от утечки по акустическим каналам

36. Защита от утечки в волоконно-оптических линиях и системах связи
37. Активные методы и средства защиты речевой информации от утечки по техническим каналам.
38. Методы и средства защиты информации в телефонных линиях связи.
39. Защита речевой информации от утечки информации за счёт «микрофонного эффекта».
40. Защита речевой информации от утечки информации за счёт «ВЧ-навязывания».
41. Экранирование электромагнитных волн.
42. Экранирование проводов и катушек индуктивности.
43. Экранированные помещения.
44. Заземление технических средств и подавление информационных сигналов в цепях заземления.
45. Фильтрация информационных сигналов.
46. Основные сведения о помехоподавляющих фильтрах.
47. Скрытие речевой информации в телефонных системах с использованием криптографических методов.
48. Перехват информации в телефонных линиях связи.
49. Организация защиты информации от утечки по цепям питания.
50. Методы, способы, средства защиты информации от утечки по материально-вещественному каналу.

МДК.05.03 Веб графика

1. Классификация изображений.
2. Сферы применения КГ.
3. Классификация КГ.
4. Виды компьютерной графики.
5. Достоинства и недостатки КГ.
6. Программы для работы с растровой графикой.
7. Программы для работы с векторной графикой.
8. Этапы развития компьютерной графики.
9. Классификация графических стандартов.
10. Графические системы класса 2D.
11. Графические системы класса 3D.
12. Open GL.
13. Группы стандартов обмена данными.
14. Форматы графических файлов.
15. Виды переплета.
16. Параметры переплетных машин.
17. Ламинатор.
18. Резак.
19. Виды электронных изданий.
20. Электронное учебное пособие.

21. Виды интерактивного взаимодействия.
22. Формат SVG, его преимущества.
23. Возможности GIMP.
24. Основные принципы GIMP.

МДК.05.04 Веб программирование

1. Абсолютный и относительный путь.
2. Адаптивная верстка.
3. Адаптивность.
4. Библиотеки шаблонов.
5. Виды доменов.
6. Виды селекторов.
7. Выбор схемы позиционирования.
8. Выбор хостинга.
9. Домен.
10. Доменные зоны.
11. Загрузка сайта на сервер.
12. Изображение ссылка.
13. Использование тегов.
14. Контентные модели.
15. Метаданные.

Критерии оценивания компетенций

Оценка «5» (отлично) выставляется студенту, глубоко и прочно усвоившему программный, в том числе лекционный материал, последовательно, четко и самостоятельно (без наводящих вопросов) отвечающему на вопрос билета.

Оценка «4» (хорошо) выставляется студенту, твердо знающему программный, в том числе лекционный материал, грамотно и по существу, отвечающему на вопрос билета и не допускающему при этом существенных неточностей (неточностей, которые не могут быть исправлены наводящими вопросами или не имеют важного практического значения). То же относится к освещению практически важных вопросов.

Оценка «3» (удовлетворительно) выставляется студенту, который обнаруживает знание основного материала, но не знает его деталей, допускает неточности, недостаточно правильные формулировки, излагает материал с нарушением последовательности, отвечает на практически важные вопросы с помощью или поправками экзаменатора.

Оценка «2» (неудовлетворительно) выставляется студенту, который не знает значительной части программного, в том числе лекционного материала.