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

И.о. директора Пятигорского
института
(филиал) СКФУ
В.А. Фурсов

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по профессиональному модулю ПМ.05 Веб технологии и защита информации

Специальность 09.02.01 Компьютерные системы и комплексы

Форма обучения очная

Пятигорск 2026

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 Гарькавой Н.Д., преподаватель колледжа Пятигорского института (филиал) СКФУ

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

СОГЛАСОВАНО:

Представитель работодателя

Зам. Генерального директора ООО «Миллениум - Плюс»		Давыдов А.А.
должность представителя работодателя, наименование организации и город ее расположения	подпись	Фамилия, инициалы

М.П.

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 Курсовой проект	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:

3.4. **Требования к курсовой работе (проекту):**

Требования к курсовому проекту по дисциплине «Веб программирование»

Курсовая работа по дисциплине должна отвечать ряду требований:

- тематика, предмет и объект исследования должны быть актуальными;
- содержание и форма подачи материала должны быть конкретными;
- работа должны быть оформлена в соответствии требованиями.

Курсовая работа студента должна:

- показать умение студента обосновать актуальность темы, творчески подойти к избранной теме, использовать методы научного исследования, анализировать источники;
- отличаться глубиной изложения, научным подходом и системным анализом существующих в отечественной и зарубежной науке точек зрения;
- содержать четкую формулировку целей, задач и гипотезы, определение предмета и объекта исследования;
- соответствовать всем требованиям, предъявляемым к оформлению курсовых работ.

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 растра.

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.

Темы курсовых проектов по МДК 05.04
Веб программирование

1. Создание веб-сайта на языке гипертекстовой разметки HTML (Вариант 1)
2. Создание веб-сайта на языке гипертекстовой разметки HTML (Вариант 2)
3. Создание веб-сайта на языке гипертекстовой разметки HTML (Вариант 3)
4. Создание веб-сайта на языке гипертекстовой разметки HTML (Вариант 4)
5. Создание веб-сайта на языке гипертекстовой разметки HTML (Вариант 5)
6. Создание веб-сайта на языке гипертекстовой разметки HTML (Вариант 6)
7. Создание веб-сайта на языке гипертекстовой разметки HTML (Вариант 7)
8. Создание веб-сайта на языке гипертекстовой разметки HTML (Вариант 8)
9. Создание веб-сайта на языке гипертекстовой разметки HTML (Вариант 9)
10. Создание веб-сайта на языке гипертекстовой разметки HTML (Вариант 10)
11. Создание веб-сайта на языке гипертекстовой разметки HTML (Вариант 11)
12. Создание веб-сайта на языке гипертекстовой разметки HTML (Вариант 12)
13. Создание веб-сайта на языке гипертекстовой разметки HTML (Вариант 13)
14. Создание веб-сайта на языке гипертекстовой разметки HTML (Вариант 14)
15. Создание веб-сайта на языке гипертекстовой разметки HTML (Вариант 15)
16. Создание веб-сайта на языке гипертекстовой разметки HTML (Вариант 16)
17. Создание веб-сайта на языке гипертекстовой разметки HTML (Вариант 17)
18. Создание веб-сайта на языке гипертекстовой разметки HTML (Вариант 18)
19. Создание веб-сайта на языке гипертекстовой разметки HTML (Вариант 19)

20. Создание веб-сайта на языке гипертекстовой разметки HTML (Вариант 20)
21. Создание веб-сайта на языке гипертекстовой разметки HTML (Вариант 21)
22. Создание веб-сайта на языке гипертекстовой разметки HTML (Вариант 22)
23. Создание веб-сайта на языке гипертекстовой разметки HTML (Вариант 23)
24. Создание веб-сайта на языке гипертекстовой разметки HTML (Вариант 24)
25. Создание веб-сайта на языке гипертекстовой разметки HTML (Вариант 25)

Критерии оценивания компетенций

Оценка «отлично» ставится, если:
- содержание и оформление работы соответствует требованиям данных Методических указаний и теме работы;
- работа актуальна, выполнена самостоятельно, имеет творческий характер, отличается определенной новизной;
- дан обстоятельный анализ степени теоретического исследования проблемы, различных подходов к ее решению;
- в докладе и ответах на вопросы показано знание нормативной базы, учтены последние изменения в законодательстве и нормативных документах по данной проблеме;
- проблема раскрыта глубоко и всесторонне, материал изложен логично;
- теоретические положения органично сопряжены с практикой; даны представляющие интерес практические рекомендации, вытекающие из анализа проблемы;
- в работе широко используются материалы исследования, проведенного автором самостоятельно или в составе группы (в отдельных случаях допускается опора на вторичный анализ имеющихся данных);
- в работе проведен количественный анализ проблемы, который подкрепляет теорию и иллюстрирует реальную ситуацию, приведены таблицы сравнений, графики, диаграммы, формулы, показывающие умение автора формализовать результаты исследования;
- широко представлен список использованных источников по теме работы;
- приложения к работе иллюстрируют достижения автора и подкрепляют его выводы;
- по своему содержанию и форме работа соответствует всем предъявленным требованиям.

Оценка «хорошо»:

- содержание и оформление работы соответствует требованиям данных Методических указаний;
- содержание работы в целом соответствует заявленной теме;
- работа актуальна, написана самостоятельно;
- дан анализ степени теоретического исследования проблемы;
- в докладе и ответах на вопросы основные положения работы раскрыты на хорошем или достаточном теоретическом и методологическом уровне;
- теоретические положения сопряжены с практикой;
- представлены количественные показатели, характеризующие проблемную ситуацию;
- практические рекомендации обоснованы;
- приложения грамотно составлены и прослеживается связь с положениями курсовой работы;
- составлен список использованных источников по теме работы.

Оценка «удовлетворительно»:
- содержание и оформление работы соответствует требованиям данных Методических указаний;
- имеет место определенное несоответствие содержания работы заявленной теме;
- в докладе и ответах на вопросы исследуемая проблема в основном раскрыта, но не отличается новизной, теоретической глубиной и аргументированностью, имеются не точные или не полностью правильные ответы;
- нарушена логика изложения материала, задачи раскрыты не полностью;
- в работе не полностью использованы необходимые для раскрытия темы научная литература, нормативные документы, а также материалы исследований;
- теоретические положения слабо увязаны с управленческой практикой, практические рекомендации носят формальный бездоказательный характер;

Оценка «неудовлетворительно»:
- содержание и оформление работы не соответствует требованиям данных Методических указаний;
- содержание работы не соответствует ее теме;
- в докладе и ответах на вопросы даны в основном неверные ответы;
- работа содержит существенные теоретико-методологические ошибки и поверхностную аргументацию основных положений;
- курсовая работа носит умозрительный и (или) компилятивный характер;
- предложения автора четко не сформулированы.

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 Обрабатывать информацию с использованием современных технических средств	- конвертировать файлы с цифровой информацией в различные форматы.
ПК 4.2 Работать с информационными системами приема, обработки и регистрации обращений клиентов	- обрабатывать аудио- и визуальный контент средствами звуковых, графических и видеоредакторов.

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.

Вопросы к экзамену по профессиональному модулю 05
Веб технологии и защита информации

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 Керкхоффса.
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.
54. Абсолютный и относительный путь.
55. Адаптивная верстка.

56. Адаптивность.
57. Библиотеки шаблонов.
58. Виды доменов.
59. Виды селекторов.
60. Выбор схемы позиционирования.
61. Выбор хостинга.
62. Домен.
63. Доменные зоны.
64. Загрузка сайта на сервер.
65. Изображение ссылка.
66. Использование тегов.
67. Контентные модели.
68. 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.

Таблица 2 – Ключи к вопросам фонда оценочных средств

№	Компетенция	Содержание вопроса	Правильный ответ
Фонд тестовых заданий МДК.05.01 Вариант 1			
1.	ПК 4.1 ПК 4.2	какой из нижеперечисленных методов является наиболее безопасным для создания пароля? а) использование простого слова или фразы. б) использование комбинации заглавных и строчных букв, цифр и специальных символов. в) использование повторяющихся символов или последовательностей. г) использование одного и того же пароля для разных аккаунтов.	б
2.	ПК 4.1	что такое фишинг? а) атака на компьютер с целью получения доступа к конфиденциальной информации. б) метод обхода защиты, используемый хакерами. в) посылка обманных сообщений с целью обмануть пользователей и получить их личные данные. г) внедрение вредоносного программного обеспечения в компьютер.	в
3.	ПК 4.2	что такое двухфакторная аутентификация? а) процесс проверки подлинности пользователя, который осуществляется на основе двух разных факторов: что-то, что знает пользователь и	а

		что-то, что имеет пользователь. б) хакерская атака, при которой злоумышленник получает доступ к аккаунту пользователя. в) метод шифрования данных для обеспечения их безопасности. г) программа, используемая для защиты компьютера от вредоносных программ.	
4.	ПК 4.1	что такое ddos-атака? а) атака, при которой злоумышленник получает доступ к аккаунту пользователя и контролирует его. б) атака, при которой злоумышленник блокирует доступ к определенному веб-сайту или онлайн-сервису, перегрузив его трафиком. в) программа-вымогатель, которая блокирует доступ к файлам на компьютере пользователя и требует выкуп за их разблокировку. г) метод шифрования данных для защиты их конфиденциальности.	б
5.	ПК 4.2	что такое мощные атаки? а) атаки, которые используются для предотвращения доступа к компьютерной системе или сети. б) атаки, которые используются для взлома системы и получения доступа к конфиденциальным данным. в) атаки, которые осуществляются с использованием мощных вычислительных ресурсов и масштабирования. г) атаки, которые используют	в

		социальную инженерию и манипуляции для получения доступа к информации.	
6.	ПК 4.1	к правовым методам, обеспечивающим информационную безопасность, относятся: а) разработка аппаратных средств обеспечения правовых данных. б) разработка и установка во всех компьютерных правовых сетях журналов учета действий. в) разработка и конкретизация правовых нормативных актов обеспечения безопасности.	в
7.	ПК 4.2	основными источниками угроз информационной безопасности являются все указанное в списке: а) хищение жестких дисков, подключение к сети, инсайдерство. б) перехват данных, хищение данных, изменение архитектуры системы. в) хищение данных, подкуп системных администраторов, нарушение регламента работы.	б
8.	ПК 4.1	виды информационной безопасности: а) персональная, корпоративная, государственная. б) клиентская, серверная, сетевая. в) локальная, глобальная, смешанная.	а
9.	ПК 4.2	цели информационной безопасности – своевременное обнаружение, предупреждение: а) несанкционированного доступа, воздействия в сети.	а

		б) инсайдерства в организации. в) чрезвычайных ситуаций.	
10.	ПК 4.1	основные объекты информационной безопасности: а) компьютерные сети, базы данных. б) информационные системы, психологическое состояние пользователей. в) бизнес-ориентированные, коммерческие системы.	а
11.	ПК 4.2	основными рисками информационной безопасности являются: а) искажение, уменьшение объема, перекодировка информации. б) техническое вмешательство, выведение из строя оборудования сети. в) потеря, искажение, утечка информации.	в
12.	ПК 4.1	к основным принципам обеспечения информационной безопасности относится: а) экономической эффективности системы безопасности. б) много платформенной реализации системы. в) усиления защищенности всех звеньев системы.	а
13.	ПК 4.2	основными субъектами информационной безопасности являются: а) руководители, менеджеры, администраторы компаний. б) органы права, государства, бизнеса. в) сетевые базы данных, фаерволлы.	б

14.	ПК 4.1	к основным функциям системы безопасности можно отнести все перечисленное: а) установление регламента, аудит системы, выявление рисков. б) установка новых офисных приложений, смена хостинг-компании. в) внедрение аутентификации, проверки контактных данных пользователей.	а
15.	ПК 4.2	принципом информационной безопасности является принцип недопущения: а) неоправданных ограничений при работе в сети (системе). б) рисков безопасности сети, системы. в) презумпции секретности.	а
16.	ПК 4.1	принципом политики информационной безопасности является принцип: а) невозможности миновать защитные средства сети (системы). б) усиления основного звена сети, системы. в) полного блокирования доступа при риск-ситуациях.	а
17.	ПК 4.2	принципом политики информационной безопасности является принцип: а) усиления защищенности самого незащищенного звена сети (системы). б) перехода в безопасное состояние работы сети, системы. в) полного доступа пользователей ко всем ресурсам сети, системы.	а

18.	ПК 4.1	принципом политики информационной безопасности является принцип: а) разделения доступа (обязанностей, привилегий) клиентам сети (системы). б) одноуровневой защиты сети, системы. в) совместимых, однотипных программно-технических средств сети, системы.	а
19.	ПК 4.2	к основным типам средств воздействия на компьютерную сеть относится: а) компьютерный сбой. б) логические закладки («мины»). в) аварийное отключение питания.	б
20.	ПК 4.1	когда получен спам по e-mail с приложенным файлом, следует: а) прочитать приложение, если оно не содержит ничего ценного – удалить. б) сохранить приложение в парке «спам», выяснить затем ip-адрес генератора спама. в) удалить письмо с приложением, не раскрывая (не читая) его.	в
фонд тестовых заданий мдк.05.01 вариант 2			
21.	ПК 4.1	что такое защита от вредоносного программного обеспечения? а) программа, предназначенная для удаления вредоносного программного обеспечения с компьютера. б) метод защиты компьютера от вирусов и другого вредоносного программного обеспечения. в) правила и процессы, предназначенные для	в

		предотвращения, обнаружения и ответа на вредоносные атаки. г) атака, при которой злоумышленник получает доступ к чужому компьютеру и контролирует его.	
22.	ПК 4.2	что такое переполнение буфера? а) техника, используемая злоумышленниками для получения доступа к системе через буферы памяти. б) состояние, при котором доступная память на компьютере исчерпана. в) метод аутентификации, используемый для проверки доступа к системе. г) программа, устанавливаемая на компьютер для отслеживания и блокировки вредоносных действий.	а
23.	ПК 4.1	что такое защитный экран (файрвол)? а) устройство или программное обеспечение, которое фильтрует и контролирует сетевой трафик, позволяя разрешить или блокировать доступ в зависимости от заданных правил. б) механизм защиты данных, который шифрует информацию перед передачей по сети. в) программа, предназначенная для удаления вредоносных программ с компьютера. г) метод аутентификации, используемый для проверки подлинности пользователей системы.	а
24.	ПК 4.2	что такое скимминг? а) атака на компьютер пользователя, при которой	б

		злоумышленник получает доступ к его личным данным. б) форма мошенничества, при которой злоумышленник получает доступ к финансовым данным пользователя, используя специальное устройство для чтения информации с магнитных полос карты. в) взлом системы путем обхода механизмов защиты. г) программа, которая преобразует данные в зашифрованный формат для повышения безопасности.	
25.	ПК 4.1	что такое шифрование данных? а) процесс преобразования данных в зашифрованный формат для обеспечения их конфиденциальности и безопасности. б) метод защиты компьютера от вредоносного программного обеспечения. в) техника, используемая злоумышленниками для получения доступа к компьютеру или сети. г) атака, при которой злоумышленник получает доступ к аккаунту пользователя и контролирует его.	а
26.	ПК 4.2	когда получен спам по e-mail с приложенным файлом, следует: а) прочитать приложение, если оно не содержит ничего ценного – удалить. б) сохранить приложение в парке «спам», выяснить затем ip-адрес генератора спама.	в

		в) удалить письмо с приложением, не раскрывая (не читая) его.	
27.	ПК 4.1	принцип кирхгофа: а) секретность ключа определена секретностью открытого сообщения. б) секретность информации определена скоростью передачи данных. в) секретность закрытого сообщения определяется секретностью ключа.	в
28.	ПК 4.2	эцп – это: а) электронно-цифровой преобразователь. б) электронно-цифровая подпись. в) электронно-цифровой процессор.	б
29.	ПК 4.1	наиболее распространены угрозы информационной безопасности корпоративной системы: а) покупка нелицензионного по. б) ошибки эксплуатации и неумышленного изменения режима работы системы. в) сознательного внедрения сетевых вирусов.	б
30.	ПК 4.2	наиболее распространены угрозы информационной безопасности сети: а) распределенный доступ клиент, отказ оборудования. б) моральный износ сети, инсайдерство. в) сбой (отказ) оборудования, нелегальное копирование данных.	в
31.	ПК 4.1	наиболее распространены средства воздействия на сеть офиса:	б

		а) слабый трафик, информационный обман, вирусы в интернет. б) вирусы в сети, логические мины (закладки), информационный перехват. в) компьютерные сбои, изменение администрирования, топологии.	
32.	ПК 4.2	утечкой информации в системе называется ситуация, характеризуемая: а) потерей данных в системе. б) изменением формы информации. в) изменением содержания информации.	а
33.	ПК 4.1	свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются: а) целостность. б) доступность. в) актуальность.	а
34.	ПК 4.2	угроза информационной системе (компьютерной сети) – это: а) вероятное событие. б) детерминированное (всегда определенное) событие. в) событие, происходящее периодически.	а
35.	ПК 4.1	информация, которую следует защищать (по нормативам, правилам сети, системы) называется: а) регламентированной. б) правовой. в) защищаемой.	в
36.	ПК 4.2	разновидностями угроз безопасности (сети, системы) являются все перечисленное в списке:	а

		а) программные, технические, организационные, технологические. б) серверные, клиентские, спутниковые, наземные. в) личные, корпоративные, социальные, национальные.	
37.	ПК 4.1	окончательно, ответственность за защищенность данных в компьютерной сети несет: а) владелец сети. б) администратор сети. в) пользователь сети.	а
38.	ПК 4.2	политика безопасности в системе (сети) – это комплекс: а) руководств, требований обеспечения необходимого уровня безопасности. б) инструкций, алгоритмов поведения пользователя в сети. в) нормы информационного права, соблюдаемые в сети.	а
39.	ПК 4.1	наиболее важным при реализации защитных мер политики безопасности является: а) аудит, анализ затрат на проведение защитных мер. б) аудит, анализ безопасности. в) аудит, анализ уязвимостей, риск-ситуаций.	в
40.	ПК 4.2	к основным типам средств воздействия на компьютерную сеть относится: а) компьютерный сбой. б) логические закладки («мины»). в) аварийное отключение питания.	б
фонд тестовых заданий мдк.05.02 вариант 1			
41.	ПК 4.1	к правовым методам, обеспечивающим	в

		информационную безопасность, относятся: а) разработка аппаратных средств обеспечения правовых данных. б) разработка и установка во всех компьютерных правовых сетях журналов учета действий. в) разработка и конкретизация правовых нормативных актов обеспечения безопасности.	
42.	ПК 4.2	основными источниками угроз информационной безопасности являются все указанное в списке: а) хищение жестких дисков, подключение к сети, инсайдерство. б) перехват данных, хищение данных, изменение архитектуры системы. в) хищение данных, подкуп системных администраторов, нарушение регламента работы.	б
43.	ПК 4.1	виды информационной безопасности: а) персональная, корпоративная, государственная. б) клиентская, серверная, сетевая. в) локальная, глобальная, смешанная.	а
44.	ПК 4.2	цели информационной безопасности – своевременное обнаружение, предупреждение: а) несанкционированного доступа, воздействия в сети. б) инсайдерства в организации. в) чрезвычайных ситуаций.	а
45.	ПК 4.1	основные объекты информационной безопасности:	а

		а) компьютерные сети, базы данных. б) информационные системы, психологическое состояние пользователей. в) бизнес-ориентированные, коммерческие системы.	
46.	ПК 4.2	основными рисками информационной безопасности являются: а) искажение, уменьшение объема, перекодировка информации. б) техническое вмешательство, выведение из строя оборудования сети. в) потеря, искажение, утечка информации.	в
47.	ПК 4.1	к основным принципам обеспечения информационной безопасности относится: а) экономической эффективности системы безопасности. б) много платформенной реализации системы. в) усиления защищенности всех звеньев системы.	а
48.	ПК 4.2	основными субъектами информационной безопасности являются: а) руководители, менеджеры, администраторы компаний. б) органы права, государства, бизнеса. в) сетевые базы данных, фаерволлы.	б
49.	ПК 4.1	к основным функциям системы безопасности можно отнести все перечисленное: а) установление регламента, аудит системы, выявление рисков.	а

		б) установка новых офисных приложений, смена хостинг-компании. в) внедрение аутентификации, проверки контактных данных пользователей.	
50.	ПК 4.2	принципом информационной безопасности является принцип недопущения: а) неоправданных ограничений при работе в сети (системе). б) рисков безопасности сети, системы. в) презумпции секретности.	а
51.	ПК 4.1	принципом политики информационной безопасности является принцип: а) невозможности миновать защитные средства сети (системы). б) усиления основного звена сети, системы. в) полного блокирования доступа при риск-ситуациях.	а
52.	ПК 4.2	принципом политики информационной безопасности является принцип: а) усиления защищенности самого незащищенного звена сети (системы). б) перехода в безопасное состояние работы сети, системы. в) полного доступа пользователей ко всем ресурсам сети, системы.	а
53.	ПК 4.1	принципом политики информационной безопасности является принцип: а) разделения доступа (обязанностей, привилегий) клиентам сети (системы).	а

		б) одноуровневой защиты сети, системы. в) совместимых, однотипных программно-технических средств сети, системы.	
54.	ПК 4.2	к основным типам средств воздействия на компьютерную сеть относится: а) компьютерный сбой. б) логические закладки («мины»). в) аварийное отключение питания.	б
55.	ПК 4.1	когда получен спам по e-mail с приложенным файлом, следует: а) прочитать приложение, если оно не содержит ничего ценного – удалить. б) сохранить приложение в парке «спам», выяснить затем ip-адрес генератора спама. в) удалить письмо с приложением, не раскрывая (не читая) его.	в
фонд тестовых заданий мдк.05.02 вариант 2			
56.	ПК 4.1	принцип кирхгофа: а) секретность ключа определена секретностью открытого сообщения. б) секретность информации определена скоростью передачи данных. в) секретность закрытого сообщения определяется секретностью ключа.	в
57.	ПК 4.2	эцп – это: а) электронно-цифровой преобразователь. б) электронно-цифровая подпись. в) электронно-цифровой процессор.	б

58.	ПК 4.1	наиболее распространены угрозы информационной безопасности корпоративной системы: а) покупка нелицензионного по. б) ошибки эксплуатации и неумышленного изменения режима работы системы. в) сознательного внедрения сетевых вирусов.	б
59.	ПК 4.2	наиболее распространены угрозы информационной безопасности сети: а) распределенный доступ клиент, отказ оборудования. б) моральный износ сети, инсайдерство. в) сбой (отказ) оборудования, нелегальное копирование данных.	в
60.	ПК 4.1	наиболее распространены средства воздействия на сеть офиса: а) слабый трафик, информационный обман, вирусы в интернет. б) вирусы в сети, логические мины (закладки), информационный перехват. в) компьютерные сбои, изменение администрирования, топологии.	б
61.	ПК 4.2	утечкой информации в системе называется ситуация, характеризуемая: а) потерей данных в системе. б) изменением формы информации. в) изменением содержания информации.	а
62.	ПК 4.1	свойствами информации, наиболее актуальными при	а

		обеспечении информационной безопасности являются: а) целостность. б) доступность. в) актуальность.	
63.	ПК 4.2	угроза информационной системе (компьютерной сети) – это: а) вероятное событие. б) детерминированное (всегда определенное) событие. в) событие, происходящее периодически.	а
64.	ПК 4.1	информация, которую следует защищать (по нормативам, правилам сети, системы) называется: а) регламентированной. б) правовой. в) защищаемой.	в
65.	ПК 4.2	разновидностями угроз безопасности (сети, системы) являются все перечисленное в списке: а) программные, технические, организационные, технологические. б) серверные, клиентские, спутниковые, наземные. в) личные, корпоративные, социальные, национальные.	а
66.	ПК 4.1	окончательно, ответственность за защищенность данных в компьютерной сети несет: а) владелец сети. б) администратор сети. в) пользователь сети.	а
67.	ПК 4.2	политика безопасности в системе (сети) – это комплекс: а) руководств, требований обеспечения необходимого уровня безопасности.	а

		б) инструкций, алгоритмов поведения пользователя в сети. в) нормы информационного права, соблюдаемые в сети.	
68.	ПК 4.1	наиболее важным при реализации защитных мер политики безопасности является: а) аудит, анализ затрат на проведение защитных мер. б) аудит, анализ безопасности. в) аудит, анализ уязвимостей, риск-ситуаций.	в
69.	ПК 4.2	к основным типам средств воздействия на компьютерную сеть относится: а) компьютерный сбой. б) логические закладки («мины»). в) аварийное отключение питания.	б
70.	ПК 4.1	когда получен спам по e-mail с приложенным файлом, следует: а) прочитать приложение, если оно не содержит ничего ценного – удалить. б) сохранить приложение в парке «спам», выяснить затем ip-адрес генератора спама. в) удалить письмо с приложением, не раскрывая (не читая) его.	в
фонд тестовых заданий мдк.05.03 вариант 1			
71.	ПК 4.1	пиксель является- а) основой растровой графики. б) основой векторной графики. в) основой фрактальной графики. г) основой трехмерной графики.	а
72.	ПК 4.2	при изменении размеров растрового изображения- а) качество остается	б

		неизменным. б) качество ухудшается при увеличении и уменьшении. в) при уменьшении остается неизменным, а при увеличении ухудшается. г) при уменьшении ухудшается, а при увеличении остается неизменным.	
73.	ПК 4.1	что можно отнести к устройствам ввода информации а) мышь клавиатуру экраны. б) клавиатуру принтер колонки. в) сканер клавиатура мышь. г) колонки сканер клавиатура.	в
74.	ПК 4.2	какие цвета входят в цветовую модель rgb а) черный синий красный. б) желтый розовый голубой. в) красный зеленый голубой. г) розовый голубой белый.	в
75.	ПК 4.1	что такое интерполяция- а) разлохмачивание краев при изменении размеров растрового изображения. б) программа для работы с фрактальными редакторами. в) инструмент в photoshop. г) это слово не как не связано с компьютерной графикой.	а
76.	ПК 4.2	наименьшим элементом изображения на графическом экране монитора является? а) курсор. б) символ. в) линия. г) пиксель.	г
77.	ПК 4.1	выберете устройства являющееся устройством вывода а) принтер. б) сканер. в) дисплей монитора.	а,в,е

		г) клавиатура. д) мышь. е) колонки.	
78.	ПК 4.2	наименьший элемент фрактальной графики а) пиксель. б) вектор. в) точка. г) фрактал.	г
79.	ПК 4.1	к какому виду графики относится данный рисунок а) фрактальной. б) растровой. в) векторной. г) ко всем вышеперечисленным.	б
80.	ПК 4.2	какие программы предназначены для работы с векторной графикой а) компас3д. б) photoshop. в) corel draw. г) blender. д) picasa. е) gimp.	а,в
81.	ПК 4.1	при изменении размеров векторной графики его качество а) при уменьшении ухудшается а при увеличении остается неизменным. б) при уменьшении остается неизменным а при увеличении ухудшается. в) качество ухудшается при увеличении и уменьшении. г) качество остается неизменным.	г
82.	ПК 4.2	чем больше разрешение, тем …. изображение а) качественнее. б) светлее. в) темнее. г) не меняется.	а

83.	ПК 4.1	пиксилизация эффект ступенек это один из недостатков а) растровой графики. б) векторной графики. в) фрактальной графики. г) масленой графики.	а
84.	ПК 4.2	графика которая представляется в виде графических примитивов а) растровая. б) векторная. в) трехмерная. г) фрактальная.	г
85.	ПК 4.1	недостатки трех мерной графики а) малый размер сохраненного файла. б) не возможность посмотреть объект на экране только при распечатывании. в) необходимость значительных ресурсов на пк для работы с данной графикой в программах.	в
фонд тестовых заданий мдк.05.03 вариант 2			
86.	ПК 4.1	к достоинствам ламповых мониторов относится а) низкая частота обновления экрана. б) хорошая цветопередача. в) высокая себестоимость.	б
87.	ПК 4.2	к недостаткам жк мониторов можно отнести а) громоздкость. б) излучение. в) узкий угол обзора. г) широкий угол обзора.	в
88.	ПК 4.1	какое расширение имеют файлы графического редактора paint? а) exe. б) doc. в) bmp. г) com.	в

89.	ПК 4.2	сетка из горизонтальных и вертикальных столбцов, которую на экране образуют пиксели, называется а) видеопамять. б) видеоадаптер. в) растр. г) дисплейный процессор.	в
90.	ПК 4.1	графический редактор paint находится в группе программ а) утилиты. б) стандартные. в) microsoft office.	б
91.	ПК 4.2	к какому типу компьютерной графики относится программа paint а) векторная. б) фрактальная. в) растровая. г) трехмерная.	в
92.	ПК 4.1	способ хранения информации в файле, а также форму хранения определяет а) пиксель. б) формат. в) графика. г) гифка.	б
93.	ПК 4.2	с помощью растрового редактора можно: а) создать коллаж. б) улучшить яркость. в) раскрашивать черно белые фотографии. г) печатать текст. д) выполнять расчет.	а,б,в
94.	ПК 4.1	для ввода изображения в компьютер используются а) принтер. б) сканер. в) диктофон. г) цифровой микрофон.	б
95.	ПК 4.2	графический редактор это а) устройство для создания и	г

		редактирования рисунков. б) устройство для печати рисунков на бумаге. в) программа для создания и редактирования текстовых документов. г) программа для создания и редактирования рисунков.	
96.	ПК 4.1	графическим объектом не является а) чертеж. +б) текст письма. в) рисунок. г) схема.	б
97.	ПК 4.2	растровым графическим редактором не является а) gimp. б) paint. в) corel draw. г) photoshop.	в
98.	ПК 4.1	в процессе сжатия растровых графических изображений по алгоритму jpeg его информационный объем обычно уменьшается в … а) 10-15 раз. б) 100раз. в) ни разу. г) 2-3 раза.	а
99.	ПК 4.2	в модели смук используется а) красный, голубой, желтый, синий. б) голубой, пурпурный, желтый, черный. в) голубой, пурпурный, желтый, белый. г) красный, зеленый, синий, черный.	б
100	ПК 4.1	в цветовой модели rgb установлены следующие параметры: 0, 255, 0. какой цвет будет соответствовать этим параметрам?	а

		а) красный. б) черный. в) голубой. г) зеленый.	
фонд тестовых заданий мдк.05.04 вариант 1			
101	ПК 4.1	о чем говорит тэг ... ? а) текст, заключенный в тэг, будет расположен по центру страницы. б) текст, заключенный в тэг, будет расположен по левому краю страницы. в) текст, заключенный в тэг, будет расположен по центру страницы.	в
102	ПК 4.2	какие единицы измерения могут использоваться для атрибута ширины? а) пиксели и %. б) миллиметры и сантиметры. в) пиксели и миллиметры.	а
103	ПК 4.1	использование тэга … позволяет добавлять одну строку текста без начала нового абзаца. а) <line/>. б) . в) <td/>.	б
104	ПК 4.2	напишите код html, который бы создавал кнопку отправки заполненной формы. имя кнопки – ок. а) <input type="ок" value="submit"/>. б) input type="submit" value="ok"< /p>. в) <input type="submit" value="ок"/>.	в
105	ПК 4.1	какой тэг при создании страницы добавляет имя страницы, которое будет	а

		отображаться в строке заголовка в браузере пользователя? а) <title> … </title>. б) <header> … </header>. в) <body> … </body>.	
106	ПК 4.2	что содержит в себе атрибут href? а) url страницы, на которую произойдет перенаправление. б) имя страницы, на которую произойдет перенаправление. в) указание на то, где будет открываться новая страница: в том же или новом окне.	а
107	ПК 4.1	какие из перечисленных тэгов относятся к созданию таблицы? а) <header> <body> <footer>. б) <table> <tr> <td>. в) <tr> <td>.	б
108	ПК 4.2	укажите тэг, который соответствует элементу списка: а) . б) . в) .	а
109	ПК 4.1	о чем говорит следующая запись: <form action="url" method="post">? а) создается форма, при заполнении которой вводимые данные будут отображаться. б) создается форма, при заполнении которой вводимые данные не будут отображаться. в) создается форма, которая будет служить для внесения информации, представленной в виде ссылки (url).	б
110	ПК 4.2	какое значение следует задать атрибуту type, чтобы оно превращало входной тэг в форму отправки? а) submit.	а

		б) checkbox. в) radiobutton.	
111	ПК 4.1	для задания размеров тэгу <frameset> требуются следующие атрибуты: а) высока и ширина. б) площадь и толщина границ. в) строки и столбцы.	в
112	ПК 4.2	что определяет тэг <aside>? а) дополнительное содержимое, т.е. то, что не включает основной документ. б) ссылку на подключенный документ. в) цветовое решение документа.	а
113	ПК 4.1	какие тэги делают шрифт текста жирным? а) <ins> и <del>. б) и . в) <b> и .	в
114	ПК 4.2	какие тэги используются для определения заголовков? а) h1-h6. б) header. в) heading.	а
115	ПК 4.1	неотображаемые комментарии в html задаются следующим образом: а) <! - your comment -!>. б) <! - - your comment - -!>. в) <!p> your comment </!p>.	б
116	ПК 4.2	какой атрибут html указывает альтернативный текст для изображения, если данное изображение не отобразится? а) imgalt. б) imgvar. в) alt.	в
117	ПК 4.1	какой html-тэг используется для определения футера документа или раздела? а) <footer>. б) <bottom>.	а

		в) <section>.	
118	ПК 4.2	html-тэг, позволяющий воспроизводить аудиозаписи – это: а) <music>. б) <audio>. в) <sound>.	б
119	ПК 4.1	в html 5, onblur и onfocus – это: а) атрибуты событий. б) атрибуты стиля. в) атрибуты подключения базы данных.	а
120	ПК 4.2	графика, определенная svg, отображается в формате: а) css. б) jsom. в) xml.	в
фонд тестовых заданий мдк.05.04 вариант 2			
121	ПК 4.1	перечислите основные модули контента, существующие в html 5. а) image, media, metadata, link, heading, color, input value. б) metadata, embedded, interactive, heading, phrasing, flow, sectioning. в) flow, static, link, header, body, footer, processing, chase.	б
122	ПК 4.2	укажите, какой элемент html 5 отвечает за воспроизведение видео: а) <video>. б) <media>. в) <movie>.	а
123	ПК 4.1	элемент <canvas> используется для: а) прикрепления таблиц excel. б) управления данными в базе данных. в) прорисовки графики.	в
124	ПК 4.2	какой тэг содержит навигацию? а) <nav>. б) <geo>.	а

		в) <metanav>.	
125	ПК 4.1	sessionstorage – это клиентское решение в html 5, которое позволяет: а) извлекать и использовать данные предыдущих сессий при условии того, что не были очищены cash и cookie. б) создавать базу данных решений пользователей в памяти браузера. в) извлекать и использовать данные только текущей сессии.	в
126	ПК 4.2	функция html 5 а) встроенную в основной функционал сайта карту мира. б) данные о местонахождении пользователя. в) данные о местонахождении сервера.	б
127	ПК 4.1	html – это а) язык разметки. б) библиотека гипертекста. в) скриптовый язык.	а
128	ПК 4.2	обязательно ли использование тэгов <html> … </html>? а) да, без них браузер не распознает html-документ. б) да, если html-документ создается в блокноте или другом текстовом редакторе. в специальном компиляторе html эти тэги можно не использовать. в) не обязательно.	а
129	ПК 4.1	какой атрибут позволяет объединить ячейки таблицы по вертикали? а) union. б) colspan. в) rowspan.	в

130	ПК 4.2	допустимое число заголовков первого уровня в html-документе составляет: а) 1. б) 3. в) 7.	а
131	ПК 4.1	текст, выделенный курсивом, представлен в следующей записи: а) <del> курсив </del>. б) курсив . в) <hr> курсив </hr>.	б
132	ПК 4.2	в html не существует … тэгов. а) одиночных. б) парных. в) тройных.	в
133	ПК 4.1	при создании сайтов используют кодировку: а) utf8. б) ascii. в) utf-32.	а
134	ПК 4.2	html-документ может иметь расширения: а) .html. б) .html или .htm. в) .html или .txt.	б

135	ПК 4.1	укажите устаревшие тэги для html 5.
		а) <applet>, <blink>, <u>.
		б) , <audio>, <pre>.
		в) <code>, <s>, <embed>.
			а

136	ПК 4.2	тэг, подключающий к существующему html-документу скрипты, которые выполняются на клиентской стороне – это: а) <object>. б) <script>. в) <client>.	б
137	ПК 4.1	какой символ обозначает конец тэга? а) ^. б) ;.	в

		в) /.	
138	ПК 4.2	список, в котором элементы перечисления отмечаются буллетами, позволяет создать тэг: а) . б) . в) <bl>.	а
139	ПК 4.1	укажите корректную запись для создания чек-бокса: а) <input checkbox>. б) <type input=”checkbox”>. в) <input type=”checkbox”>.	в
140	ПК 4.2	укажите корректную запись для создания выпадающего списка: а) <input type=”dropdown”>. б) <input dropdown list>. в) <dropdown list>.	а