

**ЧАСТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«СТАВРОПОЛЬСКИЙ МНОГОПРОФИЛЬНЫЙ КОЛЛЕДЖ»**

РАССМОТРЕНО

на заседании методического объединения
укрупненной группы специальностей
09.00.00 «Информатика и вычислительная
техника»; 10.00.00 «Информационная
безопасность» Протокол №6 от «26» мая
2022 г.

УТВЕРЖДАЮ

Директор

_____ Н.В.Кандаурова

РЕКОМЕНДОВАНО

Методическим советом СМК
Протокол № 6 от «26» мая 2022г.

**КОНТРОЛЬНО-ИЗМЕРИТЕЛЬНЫЕ МАТЕРИАЛЫ К ПРОМЕЖУТОЧНОЙ
АТТЕСТАЦИИ**

ФОРМА ПРОВЕДЕНИЯ – ДИФФЕРЕНЦИРОВАННЫЙ ЗАЧЕТ

Дисциплина: Компьютерная экспертиза

Форма обучения: очная

Курс: 7

Специальности: 10.02.05 Обеспечение информационной безопасности
автоматизированных систем

Разработчики:

Преподаватель _____

Ставрополь, 2022 г.

1. Общие положения

Контрольно-измерительные материалы предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины моделирование систем.

КИМ включают контрольные материалы для проведения промежуточной аттестации в форме экзамена.

2. Результаты освоения дисциплины, подлежащие проверке

<i>Код ОК, ПК, ЛР</i>	<i>Освоенные умения</i>	<i>Усвоенные знания</i>
ПК 3.1 ЛР 1 ЛР 3 ЛР 4 ЛР 7	✓ методы разработки применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных	✓ порядок технического обслуживания технических средств защиты информации; ✓ номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам

3. Измерительные материалы для оценивания результатов освоения учебной дисциплины

Задания для проведения дифференцированного зачета

Форма зачета смешанная: первый вопрос – теоретический, второй вопрос – решение задачи

Условия выполнения задания

1. Место (время) выполнения задания: компьютерный класс, установленное программное обеспечение VirtualBox
2. Максимальное время выполнения задания: 40 мин.
3. Источники информации, разрешенные к использованию на зачете, оборудование: ручки, рисунки, схемы, таблицы.

Задания для проведения зачета.

Теоретические вопросы

1. Что такое компьютерная криминалистика?
2. Кто и как может проводить компьютерно-техническую экспертизу?
3. Какие средства используются при проведении компьютерно-технических экспертиз?
4. Что такое расследование инцидентов информационной безопасности?
5. Каковы цели и субъекты таких расследований инцидентов информационной безопасности?
6. Каковы действия после инцидента информационной безопасности и алгоритм действий при расследовании?
7. Каковы принципы и технологии анализа с лог-файлов.
8. Как проводится анализ лог-файлов сетевого трафика.
9. Какую информацию можно анализировать в лог-файлах провайдеров?
10. Какие нормы права регламентируют деятельность эксперта?
11. Какие нормы права регламентируют деятельность следователя?
12. Каков правовой статус эксперта?
13. Каковы типовые требования к экспертному заключению?
14. Каковы специальные требования к экспертному заключению?
15. Что означает расширенное экспертное заключение?
16. Что такое блокираторы записи и дубликаторы?
17. Какие бывают экспертные системы для анализа компьютерных систем?
18. Что такое поиск уликовой информации на компьютерах?
19. Какие действия необходимо производить при начале исследований?
20. Как определяется основное направление исследования?
21. Какие бывают виды проводимых исследований?
22. В каких объектах содержится уликовая информация?
23. Какие бывают методы сокрытия уликовых данных от обнаружения?
24. Как проводится исследование реестра ОС?
25. Системы сбора и анализа журналов ОС. Корреляция событий.
26. Как проводится исследование журналов браузеров?

Практические вопросы

1. Как обосновать выбор ОС, аппаратной платформы, сетевых решений при построении информационной системы (в экономике, промышленности, образовании)?
2. Можно ли заразить вирусами ОС UNIX и почему?
3. Что нужно для подключения к компьютеру периферийных устройств (модема, сканера, принтера)?
4. Нужно ли хранить дистрибутивы ОС и драйверы после того, как все установлено на компьютер и почему?
5. Как установить несколько ОС на один компьютер?
6. Всегда ли нужно иметь на диске активный раздел?

7. Нужно ли делать активный раздел на съемном диске и почему?
8. Как выбрать пароль, который легко запомнить и трудно подобрать?
9. Сколько комбинаций можно составить из N двоичных разрядов и почему?
10. Сколько комбинаций можно закодировать с помощью 1 байта?
11. Сколько бит в одном байте?
12. Сколько байт в 1 кб, 1 Гб, 1 Мб, 1 Эб, 1 Тб?
13. За сколько времени можно передать 100 Мб по сети при скорости 10 Мбит/сек?
14. Сколько информации умещается на дискете, винчестере, стриммерной кассете, компакт-диске?
15. На файловом сервере установлена ОС Win 2000, но он медленно работает. Можно ли улучшить его быстродействие, не меняя оборудование?
16. Где найти драйверы устройств?
17. Как компьютерные вирусы используют прерывания ОС?
18. Чем удобна буферизация печати в многозадачных ОС?
19. Как организовать печать на одном принтере с нескольких компьютеров?
20. Как можно использовать возможности Ява в интернет и интранет?
21. Облегчается ли составление программ с использованием стандартного ввода-вывода?
22. Может ли пользователь изменить приоритет процесса?
23. Как влияет выбор метода восстановления после блокировки на надежность вычислительной системы и защиту информации?
24. В чем разница между микросхемами ОЗУ и флэш-памяти?
25. Как провести дефрагментацию диска?
26. В чем различие между атрибутами файлов в DOS/Win 98 и UNIX/Win 2000?
27. Что упрощается при использовании технологии Web/DB?
28. Как можно скопировать файлы с одного компьютера на другой?
29. Чем определяется уровень безопасности вычислительной системы?
30. Почему рекомендуется периодически выполнять перезагрузку сервера?
31. При какой организации памяти нужна аппаратная поддержка и почему?
32. В чем состоят трудности использования DLL в Win NT/2000/XP?
33. Возможно ли преобразование тома FAT в том NTFS и наоборот?
34. Чем отличаются атрибуты файлов в UNIX и Win 98/ME?
35. Что дает использование распределенной файловой системы NFS?
36. Почему OS/2 не стала самой распространенной ОС для ПК, несмотря на свои преимущества?
37. Чем различается информация, передаваемая по сети в базах данных с файловым сервером и технологией клиент-сервер?
38. Как влияет наличие активного раздела на порядок обозначения дисков?
39. Как организовать несколько дисков на одном винчестере?