

ПМ 04 Сопровождение и обслуживание программного обеспечения компьютерных систем

Задания для подготовки к квалификационному экзамену ПМ04

Часть №3

1. Решить тест.
2. Гугл Формы. В сервисе Google Forms Оформить тест по 15 вопросов в соответствии с таблицей.
3. Установить разрешение редактирования формы для аккаунта ifizmat@gmail.com
4. Яндекс Формы. В сервисе Яндекс Формы Оформить тест по 15 вопросов в соответствии с таблицей.
5. Расчитать на отдельной странице электронной таблицы оценку за прохождение теста. Пример формулы расчета оценки теста

```
=IF(test2!C2="Это оператор присваивания, он помещает значение, расположенное справа от него, в переменную, стоящую слева", 1, 0)  
+IF(test2!D2="Это ключевое слово для определения типа данных как целое число", 1, 0)  
+IF(test2!E2="транзистор", 1, 0)  
+IF(test2!F2="Потенциометр можно рассматривать как два резистора с переменным сопротивлением и использовать для регулировки напряжения", 1, 0)  
+IF(test2!G2="Для включения на входе встроенного подтягивающего к напряжению питания резистора", 1, 0)  
+IF(AND(test2!H2="Организация программного последовательного интерфейса передачи данных", test2!I2="Управление сервомотором", test2!J2="Управление шаговым двигателем", test2!K2="Работа с сетевым интерфейсом"), 1, 0)  
+IF(AND(test2!L2="Передачик аппаратного последовательного интерфейса", test2!M2="Приемник аппаратного последовательного интерфейса", test2!N2="Подача входного питания платы Arduino", test2!O2="Первый аналоговый вход аппаратного АЦП"), 1, 0)
```
6. Документ Гугл Таблиц с оценками сохранить в папке ПМ04DevOps/test/.

Тест 1	Тест 2	Тест 3	Тест 4	Тест 5	Тест 6	Тест 7
1	2	3	4	5	6	7
7	8	9	10	11	12	13
13	14	15	16	17	18	19
19	20	21	22	23	24	25
25	26	27	28	29	30	61
31	32	33	34	35	36	62
37	38	39	40	41	42	63
43	44	45	46	47	48	64
49	50	51	52	53	54	65
55	56	57	58	59	60	66

Тема: Экзаменационное задание с открытыми вариантами ответов

Вопрос 1. Свойство, которое гарантирует, что информация не может быть доступна или раскрыта для неавторизованных личностей, объектов или процессов – это:

- Ответ: конфиденциальность

Вопрос 2. Удачная криптоатака называется:

- Ответ: взломом

Вопрос 3. Задачей анализа модели политики безопасности на основе анализа угроз системе является:

- Ответ: минимизация вероятности преодоления системы защиты⁷⁶

Вопрос 4. С доступом к информационным ресурсам внутри организации связан уровень

ОС:

- Ответ: сетевой

Вопрос 5. Достоинством матричных моделей безопасности является:

- Ответ: легкость представления широкого спектра правил обеспечения безопасности

Вопрос 6. Конфигурация из нескольких компьютеров, выполняющих общее приложение,

называется:

- Ответ: кластером

Вопрос 7. Защита от форматирования жесткого диска со стороны пользователей обеспечивается:

- Ответ: аппаратным модулем, устанавливаемым на системную шину ПК

Вопрос 8. Битовые протоколы передачи данных реализуются на _____ уровне модели взаимодействия открытых систем.

- Ответ: физическом

Вопрос 9. Регистрацией в системе Windows 2000 управляет:

- Ответ: процедура winlogon

Вопрос 10. Обеспечение взаимодействия удаленных процессов реализуется на _____ уровне модели взаимодействия открытых систем.

- Ответ: транспортном

Вопрос 11. Проверка подлинности пользователя по предъявленному им идентификатору

– это:

- Ответ: аутентификация

Вопрос 12. Соответствие средств безопасности решаемым задачам характеризует:

- Ответ: эффективность

Вопрос 13. Как предотвращение возможности отказа одним из участников коммуникаций

от факта участия в передаче данных определяется:

- Ответ: причастность

Вопрос 14. Формирование пакетов данных реализуется на _____ уровне

модели взаимодействия открытых систем.

- Ответ: канальном

Вопрос 15. Для реализации технологии RAID создается:

- Ответ: псевдодрайвер

Вопрос 16. Недостатком модели политики безопасности на основе анализа угроз системе является:

- Ответ: изначальное допущение вскрываемости системы

Вопрос 17. Нормативный документ, регламентирующий все аспекты безопасности продукта информационных технологий, называется:

- Ответ: профилем защиты

Вопрос 18. Преднамеренные дефекты, внесенные в программные средства для целенаправленного скрытого воздействия на ИС, называются:

- Ответ: программными закладками

Вопрос 19. Содержанием параметра угрозы безопасности информации "конфиденциальность" является:

- Ответ: несанкционированное получение

Вопрос 20. "Уполномоченные серверы" были созданы для решения проблемы

- Ответ: имитации IP-адресов

Вопрос 21. Запись определенных событий в журнал безопасности сервера называется:

- Ответ: аудитом

Вопрос 22. Достоинствами программной реализации криптографического закрытия данных являются:

- Ответ: практичность и гибкость

Вопрос 23. Процесс имитации хакером дружественного адреса называется: 77

- Ответ: "спуфингом"

Вопрос 24. Первым этапом разработки системы защиты ИС является:

- Ответ: анализ потенциально возможных угроз информации

Вопрос 25. Система, позволяющая разделить сеть на две или более частей и реализовать

набор правил, определяющих условия прохождения пакетов из одной части в другую, называется:

- Ответ: брандмауэром

Вопрос 26. Недостатком дискретных моделей политики безопасности является:

- Ответ: статичность

Вопрос 27. Достоинством модели конечных состояний политики безопасности является:

- Ответ: высокая степень надежности

Вопрос 28. Защита исполняемых файлов обеспечивается:

- Ответ: обязательным контролем попытки запуска

Вопрос 29. Маршрутизация и управление потоками данных реализуются на _____ уровне модели взаимодействия открытых систем.

- Ответ: сетевом

Вопрос 30. Недостатком многоуровневых моделей безопасности является:

- Ответ: невозможность учета индивидуальных особенностей субъекта

Вопрос 31. Поддержка диалога между удаленными процессами реализуется на _____ уровне модели взаимодействия открытых систем.

- Ответ: сеансовом

Вопрос 32. Основу политики безопасности составляет:

- Ответ: способ управления доступом

Вопрос 33. "Троянский конь" является разновидностью модели воздействия программных закладок

- Ответ: искажение

Вопрос 34. Администратором базы данных является:

- Ответ: любой пользователь, создавший БД

Вопрос 35. Предоставление легальным пользователем дифференцированных прав доступа

к ресурсам системы – это:

- Ответ: авторизация

Вопрос 36. Математические методы нарушения конфиденциальности и аутентичности информации без знания ключей объединяет:

- Ответ: криптоанализ

Вопрос 37. Степень защищенности информации от негативного воздействия на неё с точки

зрения нарушения её физической и логической целостности или несанкционированного

использования – это:

- Ответ: безопасность информации

Вопрос 38. Процесс определения риска, применения средств защиты для сокращения

риска с последующим определением приемлемости остаточного риска, называется:

- Ответ: управлением риском

Вопрос 39. Выделения пользователем и администраторам только тех прав доступа, которые им необходимы это:

- Ответ: принцип минимизации привилегий

Вопрос 40. Проверка подлинности субъекта по предъявленному им идентификатору для

принятия решения о предоставлении ему доступа к ресурсам системы – это:

- Ответ: аутентификация

Вопрос 41. Получение и анализ информации о состоянии ресурсов системы с помощью

специальных средств контроля называется:

- Ответ: мониторингом

Вопрос 42. Наукой, изучающей математические методы защиты информации путем ее преобразования, является: 78

- Ответ: криптология

Вопрос 43. Защита от программных закладок обеспечивается:

- Ответ: аппаратным модулем, устанавливаемым на системную шину ПК

Вопрос 44. Список объектов, к которым может быть получен доступ, вместе с доменом

защиты объекта называется:

- Ответ: перечнем возможностей

Вопрос 45. Сетевой службой, предназначенной для централизованного решения задач

аутентификации и авторизации в крупных сетях, является:

- Ответ: Kerberos

Вопрос 46. Оконечное устройство канала связи, через которое процесс может передавать

или получать данные, называется:

- Ответ: сокетом

Вопрос 47. Достоинством модели политики безопасности на основе анализа угроз системе

является:

- Ответ: числовая вероятностная оценка надежности

Вопрос 48. Присвоение субъектам и объектам доступа уникального номера, шифра, клда

и т.п. с целью получения доступа к информации – это:

- Ответ: идентификация

Вопрос 49. Присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность

сообщения, называется:

- Ответ: электронной подписью

Вопрос 50. Обеспечением скрытности информации в информационных массивах занимается:

- Ответ: стеганография

Вопрос 51. Достоинством дискретных моделей политики безопасности является:

- Ответ: простой механизм реализации

Вопрос 52. Трояские программы – это:

- Ответ: часть программы с известными пользователю функциями, способная выполнять действия с целью причинения определенного ущерба

Вопрос 53. Достоинствами аппаратной реализации криптографического закрытия данных

являются:

- Ответ: высокая производительность и простота

Вопрос 54. Недостатком модели конечных состояний политики безопасности является:

- Ответ: сложность реализации

Вопрос 55. Совокупность свойств, обуславливающих пригодность информации удовлетворять определенные потребности в соответствии с ее назначением, называется:

- Ответ: качеством информации

Вопрос 56. Гарантия сохранности данными правильных значений, которая обеспечивается

запретом для неавторизованных пользователей каким-либо образом модифицировать, разрушать или создавать данные — это:

- Ответ: целостность

Вопрос 57. Наиболее надежным механизмом для защиты содержания сообщений является:

- Ответ: криптография

Вопрос 58. Применение услуги причастности рекомендуется на _____ уровне модели OSI.

- Ответ: прикладном

Вопрос 59. "Уполномоченные серверы" фильтруют пакеты на уровне

- Ответ: приложений

Вопрос 60. Конечное множество используемых для кодирования информации знаков называется:

- Ответ: алфавитом

Вопрос 61. Цель прогресса внедрения и тестирования средств защиты — ...

- Ответ: гарантировать правильность реализации средств защиты

Вопрос 62. С управлением доступа к ресурсам ОС связан уровень ОС:

- Ответ: системный

Вопрос 63. Присвоение субъектам и объектам доступа уникального номера, шифра, кода

и т.п. с целью получения доступа к информации — это:

- Ответ: идентификация

Вопрос 64. Недостатком матричных моделей безопасности является:

- Ответ: отсутствие контроля за потоками информации

Вопрос 65. Метод управления доступом, при котором каждому объекту системы присваивается метка критичности, определяющая ценность информации, называется:

- Ответ: мандатным

Вопрос 66. Политика информационной безопасности — это:

- Ответ: совокупность законов, правил, определяющих управленческие и проектные решения в области защиты информации