МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Дагестанский государственный университет»
Колледж

УТВЕРЖДАЮ
директор Колледжа ДГУ
_____Д.Ш. Пирбудагова
«30» 04 2022г.

Фонд оценочных средств

по учебной дисциплине

МДК.04.03.02 ОБЕСПЕЧЕНИЕ КАЧЕСТВА ФУНКЦИОНИРОВАНИЯ КОМПЬЮТЕРНЫХ СИСТЕМ

09.02.07. Информационные системы и программирование

Махачкала 2022

Составители:

Магомедова К.К. - заведующая кафедрой специальных дисциплин колледжа ДГУ, к.ю.н., доцент
Гасанова Н.Р. – старший преподаватель кафедры информационных систем и технологий программирования ДГУ

Фонд оценочных средств дисциплины рассмотрен и рекомендован к утверждению кафедрой специальных дисциплин Колледжа ДГУ.

Протокол №__8__ от «30» 04 2022 г.

Зав.кафедрой специальных дисциплин к.ю.н.,доцент _____/Магомедова К.К./

Утвержден на заседании учебно-методического совета Колледжа ДГУ

Ст. методист _____/Шамсутдинова У.А./
подпись *Фамилия И.О.*

ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ по дисциплине **МДК.04.03.02 ОБЕСПЕЧЕНИЕ КАЧЕСТВА ФУНКЦИОНИРОВАНИЯ КОМПЬЮТЕРНЫХ СИСТЕМ**

№	Контролируемые разделы, темы, модули	Код контролируемой компетенции	Наименование оценочного средства
1.	**Раздел 1.** основные методы обеспечения качества функционирования	ОК 1, ОК 2, ОК 3, ОК 4, ОК 10, ПК. 4.1, ПК. 4.2, ПК. 4.4.	коллоквиум; тестирование; практическая работа
2.	**Раздел 2.** методы и средства защиты компьютерных систем	ОК 1, ОК 2, ОК 3, ОК 4, ОК 10, ПК. 4.1, ПК. 4.2, ПК. 4.4	коллоквиум; тестирование; практическая работа

Примерный перечень оценочных средств

№ п/п	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде
1	**2**	**3**	**4**
1.	Деловая и/или ролевая игра	Совместная деятельность группы обучающихся и педагогического работника под управлением педагогического работника с целью решения учебных и профессионально ориентированных задач путем игрового моделирования реальной проблемной ситуации. Позволяет оценивать умение анализировать и решать типичные профессиональные задачи.	Тема (проблема), концепция, роли и ожидаемый результат по каждой игре
2.	Кейс-задача	Проблемное задание, в котором обучающемуся предлагают осмыслить реальную профессионально ориентированную ситуацию, необходимую для решения данной проблемы.	Задания для решения кейс-задачи
3.	Коллоквиум	Средство контроля усвоения учебного материала темы, раздела или разделов дисциплины, организованное как учебное занятие в виде собеседования педагогического работника с обучающимися.	Вопросы по темам/разделам дисциплины
4.	Контрольная работа	Средство проверки умений применять полученные знания для решения задач определенного типа по теме или разделу.	Комплект контрольных заданий по вариантам
5.	Круглый стол, дискуссия, полемика, диспут, дебаты	Оценочные средства, позволяющие включить обучающихся в процесс обсуждения спорного вопроса, проблемы и оценить их умение аргументировать собственную точку	Перечень дискуссионных тем.

		зрения.	
6.	Портфолио	Целевая подборка работ студента, раскрывающая его индивидуальные образовательные достижения в одной или нескольких учебных дисциплинах.	Структура портфолио
7.	Рабочая тетрадь	Дидактический комплекс, предназначенный для самостоятельной работы обучающегося и позволяющий оценивать уровень усвоения им учебного материала.	Образец рабочей тетради
8.	Проект	Конечный продукт, получаемый в результате планирования и выполнения комплекса учебных и исследовательских заданий. Позволяет оценить умение обучающихся самостоятельно конструировать свои знания в процессе решения практических задач и проблем, ориентироваться в информационном пространстве и уровень сформированное аналитических, исследовательских навыков, навыков практического и творческого мышления. Может выполняться в индивидуальном порядке или группой обучающихся.	Темы групповых и/или индивидуальных проектов

9.	Разноуровне вые задачи и задания	Различают задачи и задания: а) репродуктивного уровня, позволяющие оценивать и диагностировать знание фактического материала (базовые понятия, алгоритмы, факты) и умение правильно использовать специальные термины и понятия, узнавание объектов изучения в рамках определенного раздела дисциплины; б) реконструктивного уровня, позволяющие оценивать и диагностировать умения синтезировать, анализировать, обобщать фактический и теоретический материал с формулированием конкретных выводов, установлением причинно-следственных связей; в) творческого уровня, позволяющие оценивать и диагностировать умения, интегрировать знания различных областей, аргументировать собственную точку зрения.	Комплект разноуровневых задач и заданий
10.	Расчетно графическая	Средство проверки умений применять полученные знания по заранее	Комплект заданий для выполнения

	работа	определенной методике для решения задач или заданий по модулю или дисциплине в целом.	расчетнографической работы
11.	Реферат	Продукт самостоятельной работы студента, представляющий собой краткое изложение в письменном виде полученных результатов теоретического анализа определенной научной (учебно исследовательской) темы, где автор раскрывает суть исследуемой проблемы, приводит различные точки зрения, а также собственные взгляды на нее.	Темы рефератов

КРИТЕРИИ ОЦЕНКИ

по дисциплине

МДК.04.03.02 ОБЕСПЕЧЕНИЕ КАЧЕСТВА ФУНКЦИОНИРОВАНИЯ КОМПЬЮТЕРНЫХ СИСТЕМ

Критерии оценки:

Оценка «отлично»: правильно выполнены все задания практической работы, правильно даны ответы на все контрольные вопросы, выполнены задания самостоятельной работы в полном объеме. Студент отвечает на вопросы, демонстрируя глубокие знания.

Оценка «хорошо»: выполнены все задания практической и контрольной работы с наличием несущественных ошибок, выполнены задания самостоятельной работы в неполном объеме, не противоречащих основным понятиям дисциплины. Студент уверенно отвечает на вопросы, демонстрируя достаточно высокий уровень знаний

Оценка «удовлетворительно»: выполнены все задания практической и контрольной работы с наличием грубых ошибок, выполнены задания самостоятельной работы в неполном объеме, противоречащих или искажающих основные понятия дисциплины. Студент демонстрирует достаточный уровень знаний, однако затрудняется отвечать на некоторые вопросы

Оценка «неудовлетворительно»: выполнены не все задания практической работы, даны не все ответы на контрольные вопросы, имеются грубые ошибки в выполнении практических заданий и/или ответах на контрольные вопросы, противоречащие или искажающие основные понятия дисциплины, самостоятельная работа не выполнена, либо выполнена на 50%. Студент затрудняется отвечать на вопросы.

Вопросов к дифференцированному зачету:

1. Общая структура качества.
2. Методы и средства разработки программных продуктов.
3. Критерии качества.
4. Стандарт ISO 9126.
5. Стандарты в области информационных систем.
6. Многоуровневая модель качества ПО в стандарте ISO 9126.
7. Понятие технологии программирования.
8. Методы и средства разработки программных продуктов.
9. Понятие качества программных продуктов.
10. Критерии качества.
11. Основные критерии качества ПО (criteria of software quality).
12. Определение качества ПО в стандарте ISO 9126.
13. Аспекты качества, их взаимное влияние.
14. Многоуровневая модель качества ПО в стандарте ISO 9126. Модель качества
15. Тестирование программных продуктов
16. Анализ рисков
17. Основные методы обеспечения качества функционирования
18. Методы и средства разработки программных продуктов
19. Классификация уязвимостей.
20. Уязвимости, вызванные дефектами конфигурирования и управления системой.

21.Уязвимости, вызванные дефектами проектирования.
22.Уязвимости программного обеспечения.
23.Объекты уязвимости.
24.Внешние дестабилизирующие факторы.
25.Методы повышения надежности.
26.Дестабилизирующие факторы и угрозы надежности.
27.Методы предотвращения угроз надежности.
28.Методы повышения надежности.
29.Последствия нарушения надежности.
30.Методы обеспечения НПО.
31.CASE-технологии и языки IV поколения
32.Сравнение результатов тестирования с требованиями технического задания и/или спецификацией
33.Оперативные методы повышения надежности: временная, информационная, программная избыточность
34.Первичные ошибки, вторичные ошибки и их проявления
35.Математические модели описания статистических характеристик ошибок в программах
36.Способы оперативного повышения надежности ПО.
37.Избыточность как эффективный методом повышения надежности ПО.
38.Понятие временной, информативной и программной избыточности.
39.Организация программного резервирования.
40.Понятие дуального и n-версионного программирования.
41.Модифицированное дуальное программирование.
42.Метод контрольных функций как экономный способ повышения надежности ПО. Классификация методов обеспечения надежной работы программного обеспечения
43.Выявление первичных и вторичных ошибок
44.Показатели и характеристики качества программного продукта
45.Виды метрик качества программного продукта
46.Понятия «компьютерный вирус» и «программа - антивирус».
47.Значение и функции антивирусного программного обеспечения.
48.Критерии антивирусного программного обеспечения.
49.Деятельность компании Symantes.
50.Режимы проверки антивирусных программ.
51.Виды антивирусных программ (программы-детекторы; программыдоктора или фаги; программы-ревизоры; программы-фильтры;
программы-вакцины или иммунизаторы) и их характеристики.
52.Методы поиска вирусов, применимые антивирусными программами. Способы уничтожения вирусов
53.Понятие тестирования безопасности и проникновение хакеров ПО.
54.Функции и возможности тестирования защиты программного обепечения. Уровень тестирования.
55.Цель и объекты тестирования.
56.Прослеживание связи с базисом тестирования (при наличии).
57.Критерии входа и выхода.
58.Артефакты процесса тестирования, тестовые сценарии, протоколы тестирования, отчетность о результатах.
59.Тестовые методики. Измерения и метрики. Инструментарий
60.Обнаружение вируса и устранение последствий его влияния
61.Работа с программой восстановления файлов и очистки дисков
62.Технологии программирования отказоустойчивых систем

63.Понятие «шифрование». Методы и виды шифрования.
64.Средства шифрования.
65.Основные способы шифрования.
66.Понятия о криптографии и стеганографии.
67.Криптографический протокол и ее функции.
68.Классификация криптографических протоколов.
69.Коммуникационный протокол.
70.Разновидности атак на протоколы.
71.Требования к безопасности протокола.
72.Функция и роль шифрования.
73.Составные части процесса шифрования.
74.Понятие конфиденциальности информации, целостности информации и доступности информации
75.Настройка политики безопасности и браузера.
76.Работа с реестром
77.Методы и средства защиты компьютерных систем

Правила выполнения практических работ:

При выполнении практических работ (ПР), студенты должны соблюдать и выполнять следующие правила:

1. Прежде, чем приступить к выполнению ПР, обучающийся должен подготовить ответы на теоретические вопросы к ПР.

2. Перед началом каждой работы проверяется готовность обучающегося к ПР.

3. После выполнения ПР студент должен представить отчет о проделанной работе в рабочей тетради или в собственном файле (в ПК) и подготовиться к обсуждению полученных результатов и выводов.

4. Студент (обучающийся), пропустивший выполнение ПР по уважительной или неуважительной причинам, обязан выполнить работу в дополнительно назначенное время.

5. Оценка за ПР выставляется с учетом предварительной подготовки к работе, доли самостоятельности при ее выполнении, точности и грамотности оформления отчета по работе.

Критерии оценки практических работ

Практические работы оцениваются по пятибалльной шкале.

Оценка «отлично»: ставится, если ПР выполнена в полном объеме, в соответствии с заданием, с соблюдением последовательности выполнения, необходимые программы запущены и работают без ошибок; работа оформлена аккуратно;

Оценка «хорошо»: ставится, если ПР выполнена в полном объеме, в соответствии с заданием, с соблюдением последовательности выполнения, частично с помощью преподавателя, присутствуют незначительные ошибки при запуске и эксплуатации (работе) необходимых программ; работа оформлена аккуратно;

Оценка «удовлетворительно»: частично с помощью преподавателя, присутствуют ошибки при запуске и работе требуемых программ; по оформлению работы имеются замечания.

Оценка «неудовлетворительно»: ставится, если обучающийся не подготовился к ПР, при запуске и эксплуатации (работе) требуемых программ студент допустил грубые ошибки, по оформлению работы имеются множественные замечания.

Список тем практических работ:

1. Тестирование программных продуктов
2. Анализ рисков
3. Сравнение результатов тестирования с требованиями технического

задания и/или спецификацией
4. Оперативные методы повышения надежности: временная, информационная, программная избыточность
5. Выявление первичных и вторичных ошибок
6. Установка и настройка антивируса.
7. Настройка обновлений с помощью зеркала
8. Обнаружение вируса и устранение последствий его влияния
9. Работа с программой восстановления файлов и очистки дисков
10. Настройка политики безопасности и браузера.
11. Работа с реестром

Критерии оценки эссе (рефератов, докладов, сообщений)

Оценка «отлично»: выполнены все требования к написанию и защите реферата: обозначена проблема и обоснована ее актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объем, соблюдены требования к внешнему оформлению, даны правильные ответы на дополнительные вопросы.

Оценка «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; на дополнительные вопросы при защите даны неполные ответы.

Оценка «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.

Оценка «неудовлетворительно»: тема освоена лишь частично; допущены грубые ошибки в содержании реферата или при ответе на дополнительные вопросы; во время защиты отсутствует вывод. Тема реферата не раскрыта, обнаруживается существенное непонимание проблемы.

Темы для эссе (рефератов, докладов, сообщений):

1. Тестирование как часть процесса верификации программного обеспечения
2. Виды ошибок. Методы отладки
3. Методы тестирования
4. Классификация тестирования по уровням
5. Тестирование производительности
6. Регрессионное тестирование
7. Тестирование «белым ящиком»
8. Тестирование «черным ящиком»
9. Модульное тестирование
10. Интеграционное тестирование
11. Основные методы обеспечения качества функционирования
12. Методы и средства разработки программных продуктов
13. Первичные ошибки, вторичные ошибки и их проявления
14. Математические модели описания статистических характеристик ошибок в программах
15. Показатели и характеристики качества программного продукта
16. Виды метрик качества программного продукта
17. Принцип работы антивирусной программы Doctor Web.
18. Антивирус лаборатории Касперского
19. Технологии программирования отказоустойчивых систем
20. Методы и средства защиты компьютерных систем

Структура итогового теста:

Тест состоит из 20 вопросов случайным образом выбранных их списка. Тест проводится на персональном компьютере в оболочке для тестирования MyTest. Результат выдается сразу после тестирования и формируется отчет протестированных студентов на сервере.

Время на подготовку и выполнение: Выполнение тестового задания - 40 минут. За правильный ответ выставляется по 1 баллу, затем результаты суммируются, и выставляется оценка. За неправильный ответ 0 баллов.

Критерии оценки промежуточной аттестации:

Оценка «отлично» выставляется, если имеются все конспекты лекции, обучающимися выполнены 100% практических работ, оценка за итоговое тестирование – «отлично», средний балл по аттестациям не ниже 4,5.

Оценка «хорошо» выставляется, если имеются все конспекты лекции, обучающимися выполнены 100% практических работ, оценка за итоговое тестирование – «хорошо», средний балл по аттестациям не ниже 3,5.

Оценка «удовлетворительно» выставляется, если имеются все конспекты лекции, обучающимися выполнены 100% практических работ, оценка за итоговое тестирование – «удовлетворительно», средний балл по аттестациям не ниже 2,5.

Оценка «неудовлетворительно» выставляется, если имеются все конспекты лекции обучающимися выполнено менее 100% практических работ, оценка за итоговое тестирование – «неудовлетворительно», средний балл по аттестациям ниже 2,5.

Цель итогового тестирования:

Тестирование по учебной дисциплине «**Обеспечение качества функционирования компьютерных систем»** специальности 09.02.07 Информационные системы и программирование предназначено для проверки теоретических знаний и понятийного аппарата, которые лежат в основе профессионального образования и найдут свое применение в будущей профессиональной деятельности студентов.

Критерии оценки знаний:

Процент правильных ответов, %	Оценка знаний
86-100	5 «отлично»
66-85	4 «хорошо»
51-65	3 «удовлетворительно»
Менее 51	2 «неудовлетворительно»

Список теоретических заданий для подготовки к итоговому тестированию (ТЗ) по дисциплине «Обеспечение качества функционирования компьютерных систем»:

1. Информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации и представляет собой коммерческую, служебную или личную тайны, охраняющиеся еѐ владельцем, называется

а) конфиденциальной

б) доступной

в) целостной

г) все варианты верны

2. Набор правил, которые регламентируют функционирование механизма информационной безопасности называются:
   а) политикой
   б) идентификацией
   в) конфиденциальностью
   г) все варианты верны
3. Формирование профиля прав для конкретного участника процесса информационного обмена, называется:
   а) авторизацией
   б) идентификацией
   в) аутентификацией
   г) все варианты верны
4. Устройства контроля доступа из одной информационной среды в другую предоставляют:
   а) межсетевые экраны
   б) антивирусное обеспечение
   в) сканеры безопасности
   г) все варианты верны
5. Устройства проверки качества функционирования модели безопасности для конкретной информационной системы обеспечивают:
   а) сканеры безопасности
   б) антивирусные программы
   в) межсетевые экраны
   г) все варианты верны
6. Возможность реализации нарушения правил информационной безопасности, является:
   а) угрозой
   б) атакой
   в) уязвимостью
   г) все варианты верны
7. Ошибка в объекте информационной системы, которая приводит или может привести к возникновению угрозы, называется:
   а) уязвимостью
   б) атакой
   в) аварией
   г) все варианты верны
8. Набор установок и конфигураций, специфичный для данного субьекта и определяющий его работу в информационной системе, называется:
   а) профилем
   б) информационной средой
   в) паролем
   г) все варианты верны
9. Управление доступом обеспечивает защиту от несанкционированного использования ресурсов, доступных по сети
   а) несанкционированного получения информации из сети
   б) несанкционированной отправки информации по сети
   в) все ответы верны
10. Какое самое слабое звено в безопасности?
   а) люди
   б) программное обеспечение
   в) техническое обеспечение
   г) все варианты верны

11.Понятие распределенной компьютерной сети относится к компьютерам, находящимся
а) на разных территориях
б) в одном здании
в) на одной территории
г) все варианты верны
12.Основной функцией коммуникационных модулей является
а) передача полученного пакета к другому коммутационному модулю в соответствии с маршрутом передачи
б) получение переданного пакета от другого коммутационного модуля в соответствии с маршрутом отправки
в) передача и получение пакета в соответствии с маршрутом передачи/приемки
г) все варианты верны
13.Концентраторы используются для:
а) уплотнения информации перед передачей ее по высокоскоростным каналам;
б) шифрования информации перед передачей ее по высокоскоростным каналам;
в) для связи сети с ЛВС или для связи сегментов глобальных сетей;
г) все варианты верны
14.Получение информации о системе путем прослушивания каналов связи относится к:
а) пассивным угрозам
б) активным угрозам
в) адаптивным угрозам
г) все варианты верны
15.Воздействие на передаваемые сообщения в сети с целью воздействия на информационные ресурсы объектов РКС и дестабилизацию функционирования системы относится к:
а) активным угрозам
б) пассивным угрозам
в) адаптивным угрозам
г) все варианты верны
16.Моделью TCP/IP все функции сети разбиваются на:
а) 5 уровней;
б) 7 уровней;
в) 3 уровня;
г) 2 уровня
17.Для защиты информации, передаваемой по каналам связи наиболее надежным методом является:
а) шифрование;
б) хеширование;
в) методы аутентификации и идентификации;
г) все варианты верны
18.Сетевой/межсетевой экран - это
а) комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов по различным протоколам в соответствии с заданными правилами.
б) программа, с помощью которой можноможно настраивать различные параметры компьютеров и пользовательской рабочей среды сразу в масштабах сайта AD, домена, организационного подразделения

в) математический алгоритм, преобразовывающий произвольный массив данных в состоящую из букв и цифр строку фиксированной длины.

г) причем при условии использования того же типа длина эта будет оставаться неизменной, вне зависимости от объема вводных данных.

19.Основной задачей межсетевого экрана является

а) защита компьютерных сетей и/или отдельных узлов от несанкционированного доступа.

б) защита файлов от несанкционированного изменения состояния.

в) защита информации от любого изменения

20.Политика безопасности это

а) совокупность документированных руководящих принципов, правил, процедур и практических приѐмов в области безопасности, которые регулируют управление, защиту и распределение ценной информации.

б) любые групповые политики

в) автоматизация процесса управления рабочими станциями, серверами, пользователями

21.В зависимости от охвата контролируемых потоков данных межсетевые экраны подразделяются на

а) традиционный сетевой (или межсетевой) экран, персональный межсетевой экран

б) простая фильтрация, фильтрация с учѐтом контекста

в) простые и сложные

22. К способам аутентификации в информационных системах относятся

а) электронная подпись, вход по паролю

б) личная подпись

в) доверенность от клиента

г) биометрическая

23.Тестирование по требованиям безопасности - это

а) процесс выявления наличия или отсутствия уязвимостей в продукте в искусственно созданных ситуациях и на ограниченном наборе тестов, выбранных определенным образом

б) процесс проверки соответствия заявленных к продукту требований и реально реализованной функциональности,

в) процесс проверки соответствия заявленных к продукту требований и реально реализованной надежности

24.К приемам выявления уязвимостей относятся

а) экспертный анализ, статический анализ безопасности, динамический анализ безопасности

б) тестирование программного продукта

в) аудит программного обеспечения

25.Автоматизированный подход поиска уязвимостей используется при ручном подходе к поиску уязвимостей?

а) да

б) нет

в) не всегда

г) всегда

26.Конфиденциальность информации означает, что

а) данные не могут быть получены или прочитаны неавторизованными пользователями

б) уверенность в том, что информация 100% останется нетронутой и не будет изменена злоумышленником.

в) получение доступа к данным, когда это необходимо

27.Целостность информации означает, что

а) данные не могут быть получены или прочитаны неавторизованными пользователями

б) уверенность в том, что информация 100% останется нетронутой и не будет изменена злоумышленником.

в) получение доступа к данным, когда это необходимо

28.Доступность информации означает, что

а) данные не могут быть получены или прочитаны неавторизованными пользователями

б) уверенность в том, что информация 100% останется нетронутой и не будет изменена злоумышленником.

в) получение доступа к данным, когда это необходимо

29.Основные способы шифрования - это

а) Симметричное, асимметричное, хеширование, цифровая подпись

б) программируемые и выполняемые вручную

в) аппаратные, программные и программно-аппаратные шифровальные (криптографические) средства

30.Уголовная ответственность в Информационной безопасности может наступить:

а) за уничтожение, блокирование, модифицирование или копирование информации, хранящейся в электронном виде.

б) проникновение в чужую информационную систему без каких-либо неблагоприятных последствии.

в) верны оба утверждения

31.Компьютерная безопасность – это:

а) охрана персональных данных, государственной и служебной тайны и других видов информации ограниченного распространения

б) набор аппаратных и программных средств для обеспечения сохранности, доступности и конфиденциальности данных в компьютерных сетях

в) методы физической защиты ПК

г) Разграничение прав доступа и применение антивирусной защиты

32.Какие основные понятия предмета и объекта защиты существуют в Информационной безопасности

а) рассматривается как единое целое трех компонентов: человека, ПО, системы

б) конфиденциальность, целостность, доступность информации

в) законодательная, нормативно-правовая и научная база

33.Информационная безопасность – это:

а) состояние защищѐнности информационной среды

б) состав трех компонентов: ПО, информация, компьютерная система

в) конфиденциальность, целостность, доступность информации

34. Что входит в понятие Компьютерной системы

а) обслуживающий персонал

б) компьютерные системы и вычислительные сети

в) вычислительные сети

35.С чего начинается процесс входа пользователя в систему

а) аутентификация пользователя

б) идентификация пользователя

в) получение доступ.

36.Что представляет собой защита на основе вирусных сигнатур

а) программа предполагает наличие вредоносного кода по определенному сочетанию букв и цифр
б) программа проверяет наличие вредоносного кода на основе программной базы кодов
в) программа не предполагает наличие вредоносного кода по определенному сочетанию букв и цифр

37.Защита информации в сетях представляет собой
а) совокупные методы антивирусной программы и работы брендмауера
б) совокупность методов и средств, обеспечивающих целостность
в) методы правового регулирования
г) методы организационной защиты

38.Конфиденциальность, достоверность и доступность информации в условиях воздействия на нее угроз естественного или искусственного характера:
а) процесс присвоения пользователю логина и пароля
б) процесс проверки пользователя на соответствие логина и пароля
в) методы организационной защиты на предприятии
г) метод присвоения пользователю определенного номера

39.Какие бывают вирусы по способу заражения
а) резидентные, нерезидентные
б) сетевые, файловые, загрузочные
в) безвредные, неопасные, опасные
г) спутники, черви, стелсы, макровирусы

40.В чем заключается защита ПК при кратковременных отлучках
а) блокировка специальными ключами
б) блокировка заставкой
в) отсоединение жесткого диска
г) выключение компьютера

Основная литература:

1. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/495525
2. Казарин О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения [Электронный ресурс]: учебник и практикум для СПО. М.: Юрайт, 2021. - 312 с. URL: https://urait.ru/bcode/476997
3. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения [Электронный ресурс]: учебное пособие для среднего профессионального образования. М.: Юрайт, 2021. - 342 с. URL: https://urait.ru/bcode/475889
4. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В.Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2021. — 416 с. — (Среднее профессиональное образование). - ISBN 978-5-8199-0754-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/1189327

Дополнительная литература:

1. Илюшечкин В. М. Основы использования и проектирования баз данных [Электронный ресурс]: учебник для среднего профессионального образования М.: Юрайт, 2020. - 213 с. URL: https://urait.ru/bcode/452874

2. Максимов, Н. В. Компьютерные сети [Электронный ресурс]: учебное пособие / Н.В. Максимов, И.И. Попов. - 6-е изд., перераб. и доп. - Москва : ФОРУМ : ИНФРАМ, 2021. - 464 с. - (Среднее профессиональное образование). - ISBN 978-5-00091-454-0. URL: https://znanium.com/catalog/product/1189333
3. Стружкин, Н. П. Базы данных: проектирование. [Электронный ресурс]: практикум и учебное пособие для СПО. М.: Юрайт, 2020. - 291 с. URL: https://urait.ru/bcode/455865
4. Голицына, О. Л. Основы проектирования баз данных : учебное пособие / О.Л. Голицына, Т.Л. Партыка, И.И. Попов. - 2-е изд., перераб. и доп. - Москва : ФОРУМ : ИНФРА-М, 2021. - 416 с. - (Среднее профессиональное образование). - ISBN 978-5-91134-655-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1190668
5. Самуйлов К. Е. Сети и телекоммуникации [Электронный ресурс]: учебник и практикум для СПО. М.: Юрайт, 2020. - 363 с. URL:https://urait.ru/bcode/456638

6. Зверева В.П. Сопровождение и обслуживание программного обеспечения компьютерных систем: учебник для студентов, учреждений СПО / В.П. Зверева, А.В. Назаров. – 3-е издание, стер. – М.: Издательский центр Академия, 2021. – 256 с.

Интернет – ресурсы

1. Образовательная платформа «Юрайт» для вузов и сузов [Электронный ресурс]. URL: https://urait.ru /
2. Электронно-библиотечная система «Университетская библиотека онлайн» www.biblioclub.ru
3. Национальная электронная библиотека [Электронный ресурс]. URL: http://нэб.рф/ .
4. Справочно-правовая http://www.consultant.ru система «КонсультантПлюс». URL:
5. Федеральный правовой портал «Юридическая Россия». http://www.law.edu.ru/
6. Справочно-правовая система «Гарант». URL: http://www.garant.ru
7. ЭБС IPRbooks: URL: http://www.iprbookshop.ru