Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение

«Красноярский колледж радиоэлектроники и информационных технологий»

# ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения текущей и промежуточной аттестации

**ПМ.04. Сопровождение и обслуживание программного обеспечения компьютерных систем**

# МДК 04.02 Обеспечение качества функционирования компьютерных систем

для студентов специальности 09.02.07 Информационные системы и программирование

г. Красноярск, 2022

Фонд оценочных средств разработан на основе федерального государственного образовательного стандарта среднего профессионального образования по специальности

09.02.07 Информационные системы и программирование

|  |  |
| --- | --- |
| ОДОБРЕНО  Старший методист  Т.В. Клачкова  « » 2022г. | УТВЕРЖДАЮ  Заместитель директора по учебной работе  М.А. Полютова  « » 2022г. |

РАССМОТРЕНО

на заседании цикловой комиссии

* + 1. Информатика и вычислительная техника Протокол № от « » 2022 г. Председатель ЦК Е.А. Ивашова

АВТОР:

А.В. Селедцова, преподаватель КГБПОУ «Красноярский колледж радиоэлектроник и информационных технологий»

ПРОВЕРЕНО

Методист

Е.И. Макарова

« » 2022г.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **СОДЕРЖАНИЕ** | | |  |
|  |  | | | стр. |
| 1 | ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ | | | 4 |
| 2 | ОРГАНИЗАЦИЯ КОНТРОЛЯ И ОЦЕНКИ ОСВОЕНИЯ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ | | |  |
|  | 7 |
| 3 | КОНТРОЛЬНО-ОЦЕНОЧНЫЕ КОНТРОЛЯ | СРЕДСТВА | ДЛЯ ТЕКУЩЕГО |  |
|  | 11 |
| 4 | КОНТРОЛЬНО-ОЦЕНОЧНЫЕ АТТЕСТАЦИИ | СРЕДСТВА ДЛЯ | ПРОМЕЖУТОЧНОЙ |  |
|  | 34 |
| 5 | ПЕРЕЧНЬ ПЕЧАТНЫХ ИЗДАНИЙ, ЭЛЕКТРОННЫХ ИЗДАНИЙ (ЭЛЕКТРОННЫХ РЕСУРСОВ), ДОПОЛНИТЕЛЬНЫХ ИСТОЧНИКОВ | | |  |
| 43 |

**1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ**

Результатом освоения профессионального модуля является готовность обучающегося к выполнению вида профессиональной деятельности (ВПД) **Сопровождение и обслуживание программного обеспечения компьютерных систем** и составляющих его профессиональных и общих компетенций**,** основной образовательной программы среднего профессионального образования – программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности СПО 09.02.07 Информационные системы и программирование.

Контрольно-измерительные материалы и контрольно-оценочные средства разработаны на основе ФГОС СПО по специальности 09.02.07 Информационные системы и программирование и предназначены для оценки образовательных достижений обучающихся. КИМ и КОС позволяют оценить знания, умения, сформированность общих и профессиональных компетенций, обучающихся на соответствие (или несоответствие) уровня их подготовки требованиям ФГОС СПО по освоению ПМ.04. Сопровождение и обслуживание программного обеспечения компьютерных систем для специальности 09.02.07 Информационные системы и программирование

К формам текущего контроля по ПМ.04. Сопровождение и обслуживание программного обеспечения компьютерных систем относятся:

* устный опрос по теме;
* компьютерное тестирование по отдельным темам;
* отчет по практической работе;
* выполнение аудиторной самостоятельной работы.

Разработка оценочных материалов для включения в КОС проводилась с учетом:

* форм проведения оценочных мероприятий (устный опрос, самостоятельная аудиторная работа, тестирование, в т.ч. компьютерное);
* уровней освоения учебного материала темы (ознакомительный, репродуктивный, продуктивный);
* видов деятельности, которые будут выполнять обучающиеся в процессе оценочных мероприятий (осознанное воспроизведение информации, применение информации, анализ, синтез, оценка);
* обучающих возможностей оценочных материалов;
* возможности принятия решения об освоении обучающимися общих и профессиональных компетенций.

В состав КОС включены материалы, выполняющие как контролирующие, так и обучающие функции. Они позволяют не только проверить уровень усвоения знаний, освоения умений, но и оценить различные качества личности обучающегося, уровень сформирован ности профессиональных и общих компетенций.

В материалы для оценочных мероприятий, проводимых в устной форме, включается перечень вопросов для подготовки обучающихся к текущей и промежуточной аттестации.

Тесты (в т.ч. для проведения компьютерного тестирования) формируются в соответствии с общими требованиями к оформлению и содержанию тестов.

МДК 04.02 Обеспечение качества функционирования компьютерных систем является обязательной частью профессионального цикла программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности 09.02.07 Информационные системы и программирование.

МДК 04.02 Обеспечение качества функционирования компьютерных систем направлен на формирование общих и профессиональных компетенций:

|  |  |
| --- | --- |
| **Код** | **Наименование результата обучения** |
| ПК 4.1. | Осуществлять инсталляцию, настройку и обслуживание программного обеспечения компьютерных систем. |
| ПК 4.2 | Осуществлять измерения эксплуатационных характеристик программного  обеспечения компьютерных систем |
| ПК 4.4 | Обеспечивать защиту программного обеспечения компьютерных систем программными средствами. |
| ОК 1. | Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам |
| ОК 2. | Осуществлять поиск, анализ и интерпретацию информации, необходимой для  выполнения задач профессиональной деятельности. |
| ОК 3 | Планировать и реализовывать собственное профессиональное и личностное  развитие. |
| ОК 4 | Планировать и реализовывать собственное профессиональное и личностное  развитие. |
| ОК 5 | Планировать и реализовывать собственное профессиональное и личностное  развитие. |
| ОК 6 | Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей |
| ОК 7 | Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях. |
| ОК 8 | Использовать средства физической культуры для сохранения и укрепления  здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности |
| ОК 9 | Использовать информационные технологии в профессиональной деятельности. |
| ОК 10 | Пользоваться профессиональной документацией на государственном и иностранном языках |

С целью овладения указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями обучающийся в ходе освоения МДК **должен:**

|  |
| --- |
| В результате освоения учебной дисциплины обучающийся должен уметь: |
| * подбирать и настраивать конфигурацию программного обеспечения компьютерных систем; * использовать методы защиты программного обеспечения компьютерных систем; * проводить инсталляцию программного обеспечения компьютерных систем; * производить настройку отдельных компонентов программного обеспечения компьютерных систем; * анализировать риски и характеристики качества программного обеспечения; * иметь практический опыт в: настройке отдельных компонентов программного обеспечения компьютерных систем; выполнении отдельных видов работ на этапе поддержки программного обеспечения компьютерной системы. |
| В результате освоения учебной дисциплины обучающийся должен знать: |
| * основные методы и средства эффективного анализа функционирования программного обеспечения; * основные виды работ на этапе сопровождения программного обеспечения; * основные принципы контроля конфигурации и поддержки целостности конфигурации программного обеспечения; * средства защиты программного обеспечения в компьютерных системах. |

**2. ОРГАНИЗАЦИЯ КОНТРОЛЯ И ОЦЕНКИ ОСВОЕНИЯ ПРОГРАММЫ ПМ 04. МДК 04.02**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Наименование разделов**  **профессионального модуля (ПМ),**  **междисциплинарных курсов (МДК) и тем** | **Содержание учебного материала, лабораторные работы и практические занятия** | **Контролируемые  компетенции** | | **Наименование  оценочного средства** |
| 1 | 2 | 3 | | 4 |
| МДК 04.02. Обеспечение качества функционирования компьютерных систем | | | | |
| Раздел 1. Основные методы обеспечения качества функционирования | **Содержание учебного материала**  **(практическая подготовка)** | |  |  |
| Многоуровневая модель качества  программного обеспечения | | ВД 4  ПК4.1-ПК 4.3  ОК 1-ОК 10 | Банк тестов |
| Объекты уязвимости | | ВД 4  ПК4.1-ПК 4.4  ОК 1-ОК 10 | Банк тестов |
| Дестабилизирующие факторы и угрозы надежности | | ВД 4  ПК4.1-ПК 4.4  ОК 1-ОК 10 | Банк тестов |
| Методы предотвращения угроз  надежности | | ВД 4  ПК4.1-ПК 4.4  ОК 1-ОК 10 | Банк тестов |
| Оперативные методы повышения надежности: временная,  информационная, программная избыточность | | ВД 4  ПК4.1-ПК 4.4  ОК 1-ОК 10 | Банк тестов |
| Первичные ошибки, вторичные ошибки и их проявления | | ВД 4  ПК4.1-ПК 4.3  ОК 1-ОК 10 | Банк тестов |
| Математические модели описания статистических характеристик ошибок в программах | | ВД 4  ПК4.1-ПК 4.3  ОК 1-ОК 10 | Банк тестов |
| Анализ рисков и характеристик качества программного обеспечения при внедрении. | | ВД 4  ПК4.1-ПК 4.3  ОК 1-ОК 10 | Банк тестов |
| Целесообразность разработки модулей адаптации | | ВД 4  ПК4.1-ПК 4.3  ОК 1-ОК 10 | Банк тестов |
| Практическая работа №1.  «Тестирование программных продуктов» | | ВД 4  ПК4.1-ПК 4.3  ОК 1-ОК 10 | Отчет по  практической работе |
| Практическая работа №2.  «Сравнение результатов тестирования с требованиями технического задания и/или спецификацией» | | ВД 4  ПК4.1-ПК 4.3  ОК 1-ОК 10 | Отчет по практической работе |
| Практическая работа №3. «Анализ рисков» | | ВД 4  ПК4.1-ПК 4.3  ОК 1-ОК 10 | Отчет по  практической работе |
| Практическая работа №4.  «Выявление первичных и вторичных ошибок» | | ВД 4  ПК4.1-ПК 4.3  ОК 1-ОК 10 | Отчет по  практической работе |
| Раздел 2. Методы и средства защиты компьютерных систем | **Содержание учебного материала**  **(практическая подготовка)** | |  |  |
| Вредоносные программы: классификация, методы обнаружения | | ВД 4 ПК4.1-ПК 4.3  ОК 1-ОК 10 | Банк тестов |
|  | Антивирусные программы: классификация, сравнительный анализ | | ВД 4 ПК4.1-ПК 4.3  ОК 1-ОК 10 | Банк тестов |
|  | Файрвол: задачи, сравнительный анализ, настройка | | ВД 4 ПК4.1-ПК 4.3  ОК 1-ОК 10 | Банк тестов |
|  | Групповые политики.  Аутентификация. Учетные записи | | ВД 4 ПК4.1-ПК 4.3  ОК 1-ОК 10 | Банк тестов |
|  | Тестирование защиты программного обеспечения | | ВД 4 ПК4.1-ПК 4.3  ОК 1-ОК 10 | Банк тестов |
|  | Средства и протоколы шифрования сообщений | | ВД 4 ПК4.1-ПК 4.3  ОК 1-ОК 10 | Банк тестов |
|  | Практическая работа №5. «Обнаружение вируса и устранение последствий его влияния» | | ВД 4 ПК4.1-ПК 4.3  ОК 1-ОК 10 | Отчет по практической работе |
|  | Практическая работа №6.  «Установка и настройка антивируса. Настройка обновлений с помощью зеркала» | | ВД 4 ПК4.1-ПК 4.3  ОК 1-ОК 10 | Отчет по практической работе |
|  | Практическая работа №7.  «Настройка политики безопасности» | | ВД 4 ПК4.1-ПК 4.3  ОК 1-ОК 10 | Отчет по практической работе |
|  | Практическая работа №8.  «Настройка браузера» | | ВД 4 ПК4.1-ПК 4.3  ОК 1-ОК 10 | Отчет по практической работе |
|  | Практическая работа № 9.  «Работа с реестром» | | ВД 4 ПК4.1-ПК 4.3  ОК 1-ОК 10 | Отчет по практической работе |
|  | Практическая работа №10.  «Работа с программой восстановления файлов и  очистки дисков» | | ВД 4 ПК4.1-ПК 4.3  ОК 1-ОК 10 | Отчет по практической работе |
|  | Самостоятельная работа при изучении МДК.04.02  Подготовка к лабораторным работам с использованием методических указаний преподавателя, выполнение  индивидуальных заданий к практическим работам с использованием конспекта, дополнительной учебной литературы, ресурсов интернет. Оформление отчётов о выполнении практических работ и подготовка их к защите.  Подготовка рефератов с использованием конспекта, дополнительной учебной литературы, ресурсов интернет по тематике:  Особенности эксплуатации различных видов серверного программного обеспечения.  Методы и средства защиты  компьютерных систем. | | ВД 4 ПК4.1-ПК 4.3  ОК 1-ОК 10 | Отчет по  выполнению самостоятельной работы |

**3. КОНТРОЛЬНО-ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ**

# Раздел 1. Основные методы обеспечения качества функционирования

*Контрольные вопросы для проведения тестирования*

1. Как называется совокупность технических средств, необходимых для технической поддержки решения всех тех задач защиты информации, решение которых может потребоваться в процессе функционирования СЗИ?

* программное обеспечение
* техническое обеспечение
* информационное обеспечение
* математическое обеспечение

1. Что из перечисленного не включает в себя организационная защита?

* организацию работы с сотрудниками
* организацию работы с документами
* организацию режима и охраны
* организацию разработки инструкции о порядке допуска сотрудников к сведениям, составляющим конфиденциальную информацию

1. Какова конечная цель идентификации и установления подлинности объекта в вычислительной системе?

* получение документа, сформированного непосредственно данной вычислительной системой и на аппаратуре ее документирования
* допуск его к информации ограниченного пользования в случае положительного исхода проверки или отказ в допуске в случае отрицательного исхода проверки
* установление подлинности полученной информации

1. Как называется комплекс мероприятий, исключающих или уменьшающих возможность выхода конфиденциальной информации за пределы контролируемой зоны за счет акустических полей?

* защита информации от утечки по электромагнитным каналам
* защита информации от утечки по акустическому каналу
* защита информации от утечки по визуально-оптическому каналу

1. Что обозначает такой общеметодологический принцип, как концептуальное единство?

* то, что СЗИ должна строиться в строгом соответствии с требованиями к защите, которые, в свою очередь, определяются категорией соответствующего объекта и значениями параметров, влияющих на защиту информации
* такое построение и такую организацию функционирования, при которых функции защиты осуществлялись бы достаточно эффективно при изменении в некотором диапазоне структуры объекта обработки информации, технологических схем или условий функционирования каких-либо ее компонентов
* то, что архитектура, технология, организация и обеспечение функционирования как СЗИ в целом, так и составных компонентов должны рассматриваться и реализовываться в строгом соответствии с основными положениями единой концепции защиты информации

1. В чем заключается ограничение доступа?

* в том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы
* в перекрытии на период эксплуатации всех нештатных и технологических подходов к аппаратуре
* в разделении информации, циркулирующей в ней, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями
* в создании некоторой физической замкнутой преграды вокруг объекта защиты с организацией контролируемого доступа лиц, связанных с объектом защиты по своим функциональным обязанностям

1. Какой общеметодологический принцип предполагает, что все процедуры автоматизированной обработки защищаемой информации должны контролироваться системой защиты в полном объеме, причем основные результаты контроля должны фиксироваться в специальных регистрационных журналах?

* полнота контроля
* экономичность СЗИ
* активность реагирования

1. Согласно каким методам шифрования информации, шифрование выполняется путем сложения символов исходного текста и ключа по модулю, равному числу букв в алфавите?

* методам перестановки
* методам замены (подстановки)
* аддитивным методам

1. Как называется комплекс мероприятий, исключающих или ослабляющих возможность неконтролируемого выхода конфиденциальной информации за пределы контролируемой зоны за счет электромагнитных полей побочного характера и наводок?

* защита информации от утечки по электромагнитным каналам
* защита информации от утечки по визуально-оптическому каналу
* защита информации от утечки по акустическому каналу

1. Что такое система защиты информации?

* организованная совокупность всех средств, методов и мероприятий, выделяемых (предусматриваемых) на объекте обработки информации (ООИ) для решения в ней выбранных задач защиты
* общая организация системы, адекватно отражающая концептуальные подходы к ее созданию
* организованная совокупность.

# Раздел 2. Методы и средства защиты компьютерных систем Контрольные вопросы для проведения тестирования

**Тест №1**

# *Надежность - это:*

А) свойство объекта выполнять заданные функции, сохраняя во времени и в заданных пределах значения установленных эксплуатационных показателей

Б) свойство улучшать в установленных пределах значения всех параметров, характеризующих способность выполнять требуемые функции в заданных режимах и условиях применения, технического обслуживания, ремонтов, хранения и транспортирования

В) свойство, противоположное понятию «Отказ»

Г) состояние объекта, при котором он соответствует всем требованиям, установленным нормативно-технической документацией

Д) состояние объекта, при котором он обеспечивает нормальное применение объекта по назначению

# *Надежность включает в себя в зависимости от назначения объекта или условий его эксплуатации ряд простых свойств (указать неправильный ответ):*

1)срок службы 2)безотказность 3)долговечность 4)ремонтопригодность 5)сохраняемость

1. ***Объект*** *–* ***это****:*

А) техническое изделие определенного целевого назначения, рассматриваемое в периоды проектирования, производства, испытаний и эксплуатации

Б) простейшая составная часть изделия, в задачах надежности может состоять из многих элементов

В) технический элемент любого целевого назначения Г) простейший составной элемент

Д) технический элемент определенного целевого назначения, рассматриваемый исключительно в период эксплуатации

# *Свойства, характеризующие только надежность изделия:*

1. долговечность, ремонтопригодность
2. отказ, дефект;
3. сохраняемость, исправность;
4. исправность, работоспособность.
5. безотказность, работоспособность;

# *К понятию «Состояние изделий» относятся термины:*

1. отказ, повреждение
2. сохраняемость, предельное состояние
3. исправность, работоспособность
4. исправность, сохраняемость
5. отказ, дефект

# *Работоспособность – это:*

А) состояние объекта, при котором он способен выполнять заданные функции, сохраняя значения основных параметров, установленных НТД

Б) состояние объекта, при котором его применение по назначению допустимо, но нецелесообразно

В) состояние объекта, при котором он находится в исправном состоянии

Г) состояние объекта, при котором он может выполнять часть заданных функций Д) состояние объекта, при котором он отвечает требованиям норм НТД

# *Работоспособный объект:*

1. может выполнять все заданные функции, сохраняя значения заданных параметров
2. отвечает требованиям норм НТД
3. находится в исправном состоянии
4. может выполнять часть заданных функций
5. другой вариант

# *Исправность – это:*

А) состояние объекта, при котором он соответствует всем требованиям, установленным нормативно-технической документацией (НТД).

Б) состояние объекта, при котором его применение по назначению допустимо, но нецеле сообразно

В) состояние объекта, при котором он способен выполнять заданные функции находится Г) состояние объекта, при котором он может выполнять часть заданных функций

Д) состояние объекта, при котором он отвечает требованиям части норм НТД

# *Технически исправный объект:*

1. отвечает всем требованиям НТД
2. может выполнять все заданные функции, сохраняя значения заданных параметров
3. находится в работоспособном состоянии
4. может выполнять часть заданных функций
5. другой вариант

# *Предельное состояние – это:*

А) состояние объекта, при котором его применение по назначению недопустимо или нецелесообразно

Б) состояние объекта, при котором его применение по назначению недопустимо, но целесообразно

В) состояние объекта, при котором его применение по назначению нецелесообразно, но допустимо

Г) состояние объекта, при котором его применение по назначению допустимо и целесоо разно

Д)Другой вариант

# *Технический ресурс - это:*

1. наработка до предельного состояния
2. срок сохраняемости
3. срок службы
4. наработка до отказа
5. наработка до списания

# *Невосстанавливаемые объекты – это:*

А) объекты, для которых работоспособность в случае возникновения отказа, не подлежит восстановлению;

Б) объекты, работоспособность которых может быть восстановлена только путем замены В) объекты, работоспособность которых может быть восстановлена, в том числе и путем замены

Г) объекты электроники и нанотехнологии Д) объекты оборонного назначения

# *Восстанавливаемые объекты – это:*

А) объекты, работоспособность которых может быть восстановлена, в том числе и путем замены

Б) объекты, работоспособность которых может быть восстановлена только путем замены В) объекты, для которых работоспособность в случае возникновения отказа, не подлежит восстановлению

Г) любые объекты оборонного назначения или гражданской обороны Д) медпрепараты

# *К отказам функционирования относится:*

А) поломка зубьев шестерни Б) усталость металла,

В) износ оборудования

Г) потеря точности станка Д) коррозия металла

# *Отказы параметрические - это отказы, при которых*:

А) некоторые параметры объекта изменяются в недопустимых пределах

Б) обусловленные непредусмотренными перегрузками, дефектами материала, ошибками персонала или сбоями системы управления и т. п.

В) обусловленные закономерными и неизбежными явлениями, вызывающими постепенное накопление повреждений

Г) обусловленные непредусмотренными перегрузками, дефектами материала, ошибками персонала или сбоями системы управления и т. п.

Д) обусловленные закономерными и неизбежными явлениями, вызывающими постепен ное накопление повреждений

# *Отказы случайные - это отказы:*

А) обусловленные непредусмотренными перегрузками, дефектами материала, ошибками персонала или сбоями системы управления и т. п.

Б) обусловленные непредусмотренными перегрузками, дефектами материала, ошибками персонала или сбоями системы управления и т. п.

В) обусловленные закономерными и неизбежными явлениями, вызывающими постепен ное накопление повреждений

Г) при которых некоторые параметры объекта изменяются в недопустимых пределах

Д) обусловленные закономерными и неизбежными явлениями, вызывающими постепенное накопление повреждений

# *Отказы систематические - это отказы:*

А) обусловленные закономерными и неизбежными явлениями, вызывающими постепен ное накопление повреждений

Б) обусловленные непредусмотренными перегрузками, дефектами материала, ошибками персонала или сбоями системы управления и т. п.

В) некоторые параметры объекта изменяются в недопустимых пределах

Г) обусловленные непредусмотренными перегрузками, дефектами материала, ошибками персонала или сбоями системы управления и т. п.

Д) обусловленные закономерными и неизбежными явлениями, вызывающими постепенное накопление повреждений

# *К систематическим отказам относится (указать неправильный ответ):*

А) поломка зубьев шестерни Б) усталость металла,

В) износ оборудования

Г) старение оборудования Д) коррозия металла

# *К параметрическим отказам относится:*

А) потеря точности станка Б) усталость металла,

В) износ оборудования

Г) поломка зубьев шестерни Д) коррозия металла

# *Безотказность – это:*

А) свойство объекта непрерывно сохранять работоспособность в течение некоторой наработки или в течение некоторого времени

Б) свойство объекта сохранять работоспособность до наступления предельного состояния при установленной системе технического обслуживания и ремонтов

В) свойство объекта непрерывно сохранять требуемые эксплуатационные показатели в течение (и после) срока хранения и транспортирования

Г) свойство объекта, заключающееся в его приспособленности к предупреждению и обнаружению причин возникновения отказов, поддержанию и восстановлению работоспособности путем проведения ремонтов и технического обслуживания

Д) Другое

# *Долговечность – это:*

А) свойство объекта сохранять работоспособность до наступления предельного состояния при установленной системе технического обслуживания и ремонтов

Б) свойство объекта непрерывно сохранять требуемые эксплуатационные показатели в течение (и после) срока хранения и транспортирования

В) свойство объекта, заключающееся в его приспособленности к предупреждению и обнаружению причин возникновения отказов, поддержанию и восстановлению работоспособности путем проведения ремонтов и технического обслуживания

Г) свойство объекта непрерывно сохранять работоспособность в течение некоторой наработки или в течение некоторого времени

Д) Другое

# *Ремонтопригодность – это:*

А) свойство объекта, заключающееся в его приспособленности к предупреждению и обнаружению причин возникновения отказов, поддержанию и восстановлению работоспособности путем проведения ремонтов и технического обслуживания

Б) свойство объекта сохранять работоспособность до наступления предельного состояния при установленной системе технического обслуживания и ремонтов

В) свойство объекта непрерывно сохранять требуемые эксплуатационные показатели в течение (и после) срока хранения и транспортирования

Г) свойство объекта непрерывно сохранять работоспособность в течение некоторой наработки или в течение некоторого времени

Д) Другое

# *Сохраняемость – это:*

А) свойство объекта непрерывно сохранять требуемые эксплуатационные показатели в течение (и после) срока хранения и транспортирования

Б) свойство объекта сохранять работоспособность до наступления предельного состояния при установленной системе технического обслуживания и ремонтов

В) свойство объекта, заключающееся в его приспособленности к предупреждению и обнаружению причин возникновения отказов, поддержанию и восстановлению работоспособности путем проведения ремонтов и технического обслуживания

Г) свойство объекта непрерывно сохранять работоспособность в течение некоторой наработки или в течение некоторого времени

Д) Другое

# *Внезапный отказ – это:*

А) отказ, проявляющийся в резком (мгновенном) изменении характеристик объекта

Б) отказ, происходящий в результате медленного, постепенного ухудшения качества объ екта

В) отказ, вызванный недостатками и неудачной конструкцией объекта;

Г) отказ, связанный с ошибками при изготовлении объекта по причине несовершенства или нарушения технологии

Д)

# *Постепенный отказ – это:*

А) отказ, происходящий в результате медленного, постепенного ухудшения качества объекта.

Б) отказ, проявляющийся в резком (мгновенном) изменении характеристик объекта В) отказ, вызванный недостатками и неудачной конструкцией объекта;

Г) отказ, связанный с ошибками при изготовлении объекта по причине несовершенства или нарушения технологии

Д)

# *К внезапным отказам относится (указать неправильный ответ):*

А) коррозионное растрескивание

Б) образование хрупкого разрушения В) пробои изоляции

Г) образование трещины Д) обрывы тросов

1. Свойства, которые характеризуют надежность объекта:
2. работоспособность, долговечность, безотказность, исправность;
3. долговечность, безотказность, эргономичность, ремонтопригодность;
4. безотказность, долговечность, ремонтопригодность, сохраняемость;
5. срок службы, безотказность, ремонтопригодность

# *Конструкционный отказ – это:*

А) отказ, вызванный недостатками и неудачной конструкцией объекта;

Б) отказ, связанный с ошибками при изготовлении объекта по причине несовершенства или нарушения технологии

В) отказ, вызванный нарушением правил эксплуатации

Г) отказ, вызванный необратимыми процессами износа деталей, старения материалов Д) отказ, вызывающий вторичные отказы

# *Производственный отказ – это:*

А) отказ, связанный с ошибками при изготовлении объекта по причине несовершенства или нарушения технологии;

Б) отказ, вызванный недостатками и неудачной конструкцией объекта;

В) отказ, вызванный нарушением правил эксплуатации

Г) отказ, вызванный необратимыми процессами износа деталей, старения материалов Д) отказ, вызывающий вторичные отказы

# *Эксплуатационный отказ – это:*

А) отказ, вызванный нарушением правил эксплуатации.

Б) отказ, связанный с ошибками при изготовлении объекта по причине несовершенства или нарушения технологии;

В) отказ, вызванный недостатками и неудачной конструкцией объекта;

Г) отказ, вызванный необратимыми процессами износа деталей, старения материалов Д) отказ, вызывающий вторичные отказы

# *Тяжелый отказ – это:*

А) отказ, вызывающий вторичные отказы или приводящий к угрозе жизни и здоровью че ловека.

Б) отказ, исключающий возможность любой работы объекта до его устранения;

В) отказ, вызванный необратимыми процессами износа деталей, старения материалов и пр.

Г) отказ, возникающий в начальный период эксплуатации;

Д) отказ, вызванный недостатками и неудачной конструкцией объекта

# *31 Полные отказы – это:*

А) отказы, исключающие возможность работы объекта до их устранения; А) отказы, при которых объект может частично использоваться

А) отказы, возникающие в начальный период эксплуатации

отказы, вызванные необратимыми процессами износа деталей, старения материалов и пр. отказ, вызывающие вторичные отказы или приводящие к угрозе жизни и здоровью человека

# Тест №2

***1. Создание и использование средств опасного воздействия на информационные сферы других стран мира и нарушение нормального функционирования информационных и телекоммуникационных систем это….***

# информационная война

1. информационное оружие
2. информационное превосходство

***2. Информация не являющаяся общедоступной, которая ставит лиц, обладающих ею в силу своего служебного положения в преимущественное положение по сравнению с другими объектами.***

1. служебная информация
2. коммерческая тайна
3. банковская тайна

# конфиденциальная информация

***3. Гарантия того, что конкретная информация доступна только тому кругу лиц, для которых она предназначена***

# конфиденциальность

1. целостность
2. доступность
3. аутентичность
4. аппелеруемость

***4. Гарантия того, что АС ведет себя в нормальном и внештатном режиме так, как запланировано***

# надежность

1. точность
2. контролируемость
3. устойчивость
4. доступность

***5. Способность системы к целенаправленному приспособлению при изменении структуры, технологических схем или условий функционирования, которое спасает владельца АС от необходимости принятия кардинальных мер по полной замене средств защиты на новые.***

1. принцип системности
2. принцип комплексности
3. принцип непрерывной защиты
4. принцип разумной достаточности

# принцип гибкости системы

1. ***В классификацию вирусов по способу заражения входят***
2. опасные
3. файловые

# резидентные

1. загрузочные
2. файлово -загрузочные

# нерезидентные

1. ***Комплекс превентивных мер по защите конфиденциальных данных и информаци- онных процессов на предприятии это…***

# комплексное обеспечение ИБ

1. безопасность АС
2. угроза ИБ
3. атака на АС
4. политика безопасности

***8. Вирусы, не связывающие свои копии с файлами, а создающие свои копии на дисках, не изменяя других файлов, называются:***

1. компаньон - вирусами

# черви

1. паразитические
2. студенческие
3. призраки
4. стелс - вирусы
5. макровирусы

9. ***К видам системы обнаружения атак относятся :***

1. системы, обнаружения атаки на ОС
2. системы, обнаружения атаки на конкретные приложения
3. системы, обнаружения атаки на удаленных БД

# все варианты верны

10. ***Автоматизированная система должна обеспечивать***

1. надежность

# доступность

1. **целостность**
2. контролируемость

11. ***Основными компонентами парольной системы являются***

# интерфейс администратора

1. хранимая копия пароля

# база данных учетных записей

1. все варианты верны

***12. Некоторое секретное количество информации, известное только пользователю и парольной системе, которое может быть запомнено пользователем и предъявлено для прохождения процедуры аутентификации это ….***

1. идентификатор пользователя

# пароль пользователя

1. учетная запись пользователя
2. парольная система

***13. К принципам информационной безопасности относятся***

1. скрытость
2. масштабность

# системность

1. **законность**

# открытости алгоритмов

***14. К вирусам изменяющим среду обитания относятся:***

1. черви
2. студенческие

# полиморфные

1. спутники

***15. Охрана персональных данных, государственной служебной и других видов инфор- мации ограниченного доступа это…***

# Защита информации

1. Компьютерная безопасность
2. Защищенность информации
3. Безопасность данных

***16. Система физической безопасности включает в себя следующие подсистемы:***

# оценка обстановки

1. скрытность

# строительные препятствия

1. **аварийная и пожарная сигнализация**

***17. Какие степени сложности устройства Вам известны?***

1. упрощенные

# простые

1. **сложные**
2. оптические
3. встроенные

***18. К механическим системам защиты относятся:***

# проволока

1. **стена**
2. сигнализация

***19. Какие компоненты входят в комплекс защиты охраняемых объектов:***

# сигнализация

1. **охрана**

# датчики

1. **телевизионная система**

***20. К выполняемой функции защиты относится:***

1. внешняя защита
2. внутренняя защита

# все варианты верны

1. ***Набор аппаратных и программных средств для обеспечения сохранности, доступ ности и конфиденциальности данных:***
2. Защита информации

# Компьютерная безопасность

1. Защищенность информации
2. Безопасность данных

***22. Средства уничтожения, искажения или хищения информационных массивов, добывания из них необходимой информации после преодоления систем защиты, ограничения или воспрещения доступа к ним это:***

1. информационная война

# информационное оружие

1. информационное превосходство

***23. Информация, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличивать доходы, сохранить положение на рынке товаров, работ или услуг это:***

1. государственная тайна

# коммерческая тайна

1. банковская тайна
2. конфиденциальная информация

***24. Гарантия того, что при хранении или передаче информации не было произведено несанкционированных изменений:***

1. конфиденциальность

# целостность

1. доступность
2. аутентичность
3. аппелеруемость

***25. Гарантия точного и полного выполнения команд в АС:***

1. надежность

# точность

1. контролируемость
2. устойчивость
3. доступность

***26. Уровень защиты, при котором затраты, риск, размер возможного ущерба были бы приемлемыми:***

1. принцип системности
2. принцип комплексности
3. принцип непрерывности

# принцип разумной достаточности

1. принцип гибкости системы

***27. Совокупность норм, правил и практических рекомендаций, регламентирующих работу средств защиты АС от заданного множества угроз безопасности:***

1. Комплексное обеспечение информационной безопасности
2. Безопасность АС
3. Угроза информационной безопасности
4. атака на автоматизированную систему

# политика безопасности

***28. Особенностями информационного оружия являются:***

1. системность
2. открытость

# универсальность

1. **скрытность**

***29. К функциям информационной безопасности относятся:***

# совершенствование законодательства РФ в сфере обеспечения информационной безопасности

1. **выявление источников внутренних и внешних угроз**

# Страхование информационных ресурсов

1. **защита государственных информационных ресурсов**

# подготовка специалистов по обеспечению информационной безопасности

***30. К типам угроз безопасности парольных систем относятся***

1. словарная атака
2. тотальный перебор
3. атака на основе психологии
4. разглашение параметров учетной записи

# все варианты ответа верны

***31. К вирусам не изменяющим среду обитания относятся:***

# черви

1. студенческие
2. полиморфные

# спутники

***32. Хранение паролей может осуществляться***

# в виде сверток

1. **в открытом виде**
2. в закрытом виде

# в зашифрованном виде

1. все варианты ответа верны

***33. Антивирусная программа принцип работы, которой основан на проверке файлов, секторов и системной памяти и поиске в них известных и новых вирусов называется:***

1. ревизором
2. иммунизатором

# сканером

1. доктора и фаги

***34. Выбрать недостатки имеющиеся у антивирусной программы ревизор:***

# неспособность поймать вирус в момент его появления в системе

1. **небольшая скорость поиска вирусов**

# невозможность определить вирус в новых файлах (в электронной почте, на дискете)

***35. В соответствии с особенностями алгоритма вирусы можно разделить на два класса:***

1. вирусы изменяющие среду обитания, но не распространяющиеся

# вирусы изменяющие среду обитания при распространении

1. **вирусы не изменяющие среду обитания при распространении**
2. вирусы не изменяющие среду обитания и не способные к распространению в даль- нейшем

36. К достоинствам технических средств защиты относятся:

1. регулярный контроль

# создание комплексных систем защиты

1. степень сложности устройства
2. Все варианты верны

***37. К тщательно контролируемым зонам относятся:***

# рабочее место администратора

1. **архив**

# рабочее место пользователя

***38. К системам оповещения относятся:***

# инфракрасные датчики

1. **электрические датчики**
2. электромеханические датчики
3. электрохимические датчики

***39. К оборонительным системам защиты относятся:***

# проволочные ограждения

1. **звуковые установки**
2. датчики

# световые установки

***40. Охранное освещение бывает:***

# дежурное

1. световое

# тревожное

***41. К национальным интересам РФ в информационной сфере относятся:***

# Реализация конституционных прав на доступ к информации

1. Защита информации, обеспечивающей личную безопасность
2. Защита независимости, суверенитета, государственной и территориальной целостности
3. Политическая экономическая и социальная стабильность
4. Сохранение и оздоровлении окружающей среды

***42. Информационная безопасность это:***

1. Состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз

# Состояние защищенности жизненно важных интересов личности, общества и государства в информационной сфере от внутренних и внешних угроз

1. Состояние, когда не угрожает опасность информационным системам
2. Политика национальной безопасности России

***43. Наиболее распространенные угрозы информационной безопасности:***

# угрозы целостности

1. угрозы защищенности
2. угрозы безопасности

# угрозы доступности

1. **угрозы конфиденциальности**

***44. Что относится к классу информационных ресурсов:***

# Документы

1. **Персонал**

# Организационные единицы

1. **Промышленные образцы, рецептуры и технологии**

# Научный инструментарий

***45. Гарантия того, что конкретная информация доступна только тому кругу лиц, для кого она предназначена:***

# конфиденциальность

1. доступность
2. аутентичность
3. целостность

***46. Устройства осуществляющие воздействие на человека путем передачи информации через внечувственное восприятие:***

1. Средства массовой информации
2. Психотропные препараты
3. Психотронные генераторы

# Средства специального программно-технического воздействия

***47. Злонамеренные действия в нематериальной сфере могут быть подразделены на два класса, какие?***

# Информационный саботаж

1. **Физический саботаж**
2. Информационные инфекции

***48. Что не относится к информационной инфекции:***

1. Троянский конь

# Фальсификация данных

1. Черви
2. Вирусы
3. Логическая бомба

***49. Деятельность по предотвращению неконтролируемого распространения защищаемой информации от ее разглашения и несанкционированного доступа к защищаемой информации и от получения защищаемой информации:***

1. защита информации от непреднамеренного воздействия
2. защита информации от несанкционированного воздействия
3. защита информации от несанкционированного доступа

# защита от утечки информации

***50. Идентификатор субъекта доступа, который является его секретом:***

# пароль

1. ключ
2. электронно-цифровая подпись
3. сертификат ключа подписи

***51. Исследование возможности расшифрования информации без знания ключей:***

1. криптология

# криптоанализ

1. взлом
2. несанкционированный доступ

***52. Состояние защищенности национальных интересов страны в информационной сфере от внутренних и внешних угроз это:***

# Информационная безопасность

1. Безопасность
2. Национальная безопасность
3. Защита информации

***53. Охрана персональных данных, государственной, служебной и других видов информации ограниченного доступа это:***

1. Защита информации
2. Компьютерная безопасность
3. Защищенность информации
4. Защищенность потребителей информации

# Безопасность данных

***54. Создание и использование средств опасного воздействия на информационные сферы других стран мира и нарушение нормального функционирования информационных и телекоммуникационных систем это:***

1. Информационная война

# Информационное оружие

1. Информационное превосходство

***55. Реализация конституционных прав и свобод человека, обеспечение личной безопас ности, повышение качества и уровня жизни это:***

1. Интересы государства
2. Интересы государства в информационной сфере

# Интересы личности

1. Интересы личности в информационной сфере
2. Интересы общества в информационной сфере

***56. Информация, не являющаяся общедоступной, которая ставит лиц, обладающих ею в силу своего служебного положения, в преимущественное положение по сравнению с другими объектами:***

1. Служебная информация
2. Коммерческая тайна
3. Банковская тайна

# Конфиденциальная информация

***57. Действие, предпринимаемое злоумышленником, которое заключается в поиске и использовании той или иной уязвимости системы.***

1. Комплексное обеспечение информационной безопасности
2. Безопасность АС
3. Угроза информационной безопасности

# Атака на автоматизированную систему

1. Политика безопасности

***58. Вся накопленная информация об окружающей нас действительности, зафиксированная на материальных носителях или в любой другой форме, обеспечивающая ее передачу во времени и пространстве между различными потребителями для решения научных, производственных, управленческих и других задач***

# Информационные ресурсы

1. Информационная система
2. Информационная сфера
3. Информационные услуги
4. Информационные продукты

***59. К какому уровню доступа информации относится следующая информация: «Ин- формация, содержащая сведения об обстоятельствах и фактах, предоставляющих угрозу жизни, здоровью граждан …»***

# Информация без ограничения права доступа

1. Информация с ограниченным доступом
2. Информация, распространение которой наносит вред интересам общества
3. Объект интеллектуальной собственности
4. Иная общедоступная информация

***60. Состояние защищенности при котором не угрожает опасность это:***

1. Информационная безопасность

# Безопасность

1. Защита информации
2. Национальная безопасность

***61. Набор аппаратных и программных средств для обеспечения сохранности, доступ ности и конфиденциальности данных:***

# Защита информации

1. Компьютерная безопасность
2. Защищенность информации
3. Защищенность потребителей информации

***62. Особый вид отношений между государствами, при котором для разрешения существующих межгосударственных противоречий используются методы, средства и технологии силового воздействия на информационную сферу этих государств:***

# Информационная война

1. Информационное оружие
2. Информационное превосходство

***63. Создание условий для гармоничного развития российской информационной инфра- структуры, для реализации конституционных прав и свобод человека в области по- лучения информации и пользования ею в целях обеспечения незыблемости конституционного строя , суверенитета и территориальной целостности это:***

1. Интересы государства

# Интересы государства в информационной сфере

1. Интересы личности
2. Интересы личности в информационной сфере
3. Интересы общества в информационной сфере

***64. Информационно упорядоченная совокупность документов и информационных технологий, реализующая информационные процессы***

1. Информационные ресурсы

# Информационная система

1. Информационная сфера
2. Информационные услуги
3. Информационные продукты

***65. К какому уровню доступа информации относится следующая информация: «Автор- ское право, патентное право…»***

1. Информация без ограничения права доступа
2. Информация с ограниченным доступом
3. Информация, распространение которой наносит вред интересам общества

# Объект интеллектуальной собственности

1. Иная общедоступная информация

***66. Состояние защищенности многонационального народа как носителя суверенитета и единственного источника власти:***

1. Информационная безопасность
2. Безопасность
3. Защита информации

# Национальная безопасность

***67. Защита от случайных и преднамеренных воздействий, чреватых нанесением ущерба владельцам или пользователям информации это:***

1. Защита информации
2. Компьютерная безопасность
3. Защищенность информации

# Защищенность потребителей информации

***68. Средства уничтожения, искажения, или хищения информационных массивов, добывания из них необходимой информации после преодоления систем защиты, ограничения или воспрещения доступа к ним это:***

1. Информационная война

# Информационное оружие

1. Информационное превосходство

***69. Документированная информация, доступ к которой ограничивается в соответствии с законодательством РФ:***

# Государственная тайна

1. Коммерческая тайна
2. Банковская тайна
3. Конфиденциальная информация

***70. Свойство данных быть доступными для санкционированного пользования в произвольный момент времени, когда в обращении к ним возникает необходимость:***

1. Конфиденциальность
2. Целостность

# Доступность

1. Аутентичность
2. Аппелируемость

***71. Гарантия того, что в любой момент времени может быть произведена полноценная проверка любого компонента программного комплекса АС:***

1. Надежность
2. Точность

# Контролируемость

1. Устойчивость
2. Доступность

***72. Непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла АС:***

1. Принцип системности
2. Принцип комплексности

# Принцип непрерывной защиты

1. Принцип разумной достаточности
2. Принцип гибкости системы

***73. Возможные воздействия на АС, которые прямо или косвенно могут нанести ущерб ее безопасности:***

1. Комплексное обеспечение информационной безопасности
2. Безопасность АС

# Угрозы информационной безопасности

1. Атака на автоматизированную систему
2. Политика безопасности

***74. Совокупность информации, информационной структуры субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений***

1. Информационные ресурсы
2. Информационная система

# Информационная сфера

1. Информационные услуги
2. Информационные продукты

***75. К какому уровню доступа информации относится следующая информация: «Лож- ная реклама, реклама со скрытыми вставками…»***

1. Информация без ограничения права доступа
2. Информация с ограниченным доступом

# Информация, распространение которой наносит вред интересам общества

1. Объект интеллектуальной собственности
2. Иная общедоступная информация

***76. Защищенность страны от нападения извне, шпионажа, покушения на государствен- ный и общественный строй:***

1. Информационная безопасность
2. Безопасность

# Национальная безопасность

1. Защита информации

77. Защищенность от негативных информационно-психологических и информаци- онно- технических воздействий:

1. Компьютерная безопасность
2. Защищенность информации

# Защищенность потребителей информации

***78. Возможность сбора, обработки и распространения непрерывного потока информации при воспрещении использования информации противником это:***

1. Информационная война
2. Информационное оружие

# Информационное превосходство

***79. Обобщение интересов личности в этой сфере, упрочнение демократии, создание правового государства это:***

1. Интересы государства
2. Интересы государства в информационной сфере
3. Интересы личности в информационной сфере

# Интересы общества

1. Интересы общества в информационной сфере

***80. Защищаемые государством сведения в области военной, внешнеполитической и внешнеэкономической деятельности, распространение которых может нанести ущерб безопасности РФ.***

# Государственная тайна

1. Коммерческая тайна
2. Банковская тайна
3. Конфиденциальная информация

***81. Гарантия того, что источником информации является именно то лицо, которое заявлено как ее автор:***

1. Конфиденциальность
2. Целостность
3. Доступность

# Аутентичность

1. Аппелируемость

***82. Гарантия того, что при умышленном внесении ошибок в пределах заранее оговоренных норм АС будет вести себя так, как оговорено заранее:***

1. Надежность
2. Точность
3. Контролируемость

# Устойчивость

1. Доступность

***83. Согласование разнородных средств при построении целостной системы защиты, перекрывающий все существенные каналы реализации угроз и не содержащий слабых мест на стыках отдельных компонентов:***

1. Принцип системности

# Принцип комплексности

1. Принцип непрерывной защиты
2. Принцип разумной достаточности
3. Принцип гибкости системы

***84. Защищенность АС от случайного или преднамеренного вмешательства в нормальный процесс ее функционирования, а также от попыток хищения, изменения или разрушения ее компонентов:***

1. Комплексное обеспечение информационной безопасности

# Безопасность АС

1. Угроза информационной безопасности
2. Атака на автоматизированную систему
3. Политика безопасности

***85. Действие субъектов по обеспечению пользователей информационными продуктами:***

1. Информационные ресурсы
2. Информационная система
3. Информационная сфера

# Информационные услуги

1. Информационные продукты

***86. К какому уровню доступа информации относится следующая информация: «Библиографические и опознавательные данные, личные характеристики , сведения о семейном положении, сведения об имущественном или финансовом состоянии…»***

1. Информация без ограничения права доступа

# Информация с ограниченным доступом

1. Информация, распространение которой наносит вред интересам общества
2. Объект интеллектуальной собственности
3. Иная общедоступная информация

***87. Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов и требований:***

1. Защищенность информации

# Защищаемая информация

1. Защищенность потребителей информации
2. Защита информации

***88. Действия, предпринимаемые для достижения информационного превосходства в поддержке национальной информационной стратегии посредством воздействия на информацию и информационные системы противника:***

# Информационная война

1. Информационное оружие
2. Информационное превосходство

***89. Гарантия неразглашения банковского счета, операций по счету и сведений о клиенте:***

1. Государственная тайна
2. Коммерческая тайна

# Банковская тайна

1. Конфиденциальная информация

***90. Гарантия того, что при необходимости можно будет доказать, что автором сообщения является именно тот человек, который заявлен как ее автор и никто другой:***

1. Конфиденциальность
2. Целостность
3. Доступность
4. Аутентичность

# Аппелируемость

***91. Системный подход к защите компьютерных систем предполагающий необходимость учета всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов:***

# Принцип системности

1. Принцип комплексности
2. Принцип непрерывной защиты
3. Принцип разумной достаточности
4. Принцип гибкости системы

***92. Область науки и техники, охватывающая совокупность криптографических, про граммно-аппаратных, технических, правовых, организационных методов и средств обеспечения безопасности информации при ее обработке, хранении и передаче с использованием современных информационных технологий:***

# Комплексное обеспечение информационной безопасности

1. Безопасность АС
2. Угроза безопасности
3. Атака на автоматизированную систему
4. Политика безопасности

***93. Документированная информация, подготовленная в соответствии с потребностями пользователей и предназначенная или применяемая для удовлетворения потребностей пользователей:***

1. Информационные ресурсы
2. Информационная система
3. Информационная сфера
4. Информационные услуги

# Информационные продукты

***94. К какому уровню доступа информации относится следующая информация: «Ин- формация в области работ по хранению, перевозке, уничтожению химического оружия – сведения о состоянии здоровья граждан и объектов окружающей среды в рай- онах размещения объектов по уничтожению химического оружия…»***

1. Информация без ограничения права доступа

# Информация с ограниченным доступом

1. Информация, распространение которой наносит вред интересам общества
2. Объект интеллектуальной собственности
3. Иная общедоступная информация

***95. Соотнесите интересы в области информационной безопасности:***

1. Национальные интересы
2. Интересы личности
3. Интересы государства
4. Интересы общества
5. состоят в реализации конституционных прав и свобод [2], в обеспечении личной безопасности, в повышении качества и уровня жизни, в физическом, духовном и интеллектуальном развитии человека и гражданина
6. обеспечиваются институтами государственной власти, осуществляющими свои функции, в том числе во взаимодей твии с действующими на основе Конституции РФ и законодательства РФ общественными организациями
7. состоят в незыблемости конституционного строя, суверенитета и территориальной целостности России, в политиче ской, экономической и социальной стабильности, в безусловном обеспе чении законности и поддержании правопорядка, в развитии равноправно го и взаимовыгодного международного сотрудничества.
8. состоят в упрочении демократии, в создании правового, социального государства, в достижении и поддержании обще ственного согласия, в духовном обновлении России.

# ОТВЕТ: 1-2; 2-1; 3-3; 4-4.

***96. Соотнесите основные методы получения паролей:***

1. метод тотального перебора
2. словарная атака
3. получение паролей из самой системы на основе программной и аппаратной реали- зации конкретной системы
4. проверка паролей, устанавливаемых в системах по умолчанию
5. для перебора используется словарь наиболее вероятных ключей
6. двумя возможностями выяснения пароля являются: несанкционированный доступ к носителю, содержащему пароли, либо использование уязвимостей
7. опробываются все ключи последовательно, один за другим
8. пароль, установленный фирмой-разработчиком по умолчанию, остается основным паролем в системе

# ОТВЕТ: 1-3; 2-1; 3-2; 4-4;

***97. Соотнесите принципы информационной безопасности, определенные ФСТЭК (Гостехкомиссией)***

1. Принцип системности
2. Принцип комплексности
3. Принцип непрерывности защиты
4. Гибкость системы защиты
5. Разумная достаточность
6. правильно выбрать тот достаточный уровень защиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми
7. непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла АС
8. предполагает согласование разнородных средств при построении целостной системы защиты, перекрывающей все существенные каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов
9. освобождает владельца АС от необходимости принятия кардинальных мер по полной замене средств защиты на новые.
10. предполагает необходимость учета всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов

# ОТВЕТ: 1-5; 2-3; 3-2; 4-4; 5-1;

***98. Соотнесите основные понятия в области информационной безопасности:***

1. Атака
2. Уязвимость AC
3. Угроза безопасности АС
4. Защищенная система
5. некоторое неудачное свойство системы, которое делает возможным возникновение и реализацию угрозы
6. система со средствами защиты, которые успешно и эффективно противостоят угро зам безопасности
7. возможные воздействия на АС, которые прямо или косвенно могут нанести ущерб ее безопасности
8. действие, предпринимаемое злоумышленником, которое заключается в поиске и использовании той или иной уязвимости системы

# ОТВЕТ: 1-4; 2-1; 3-3; 4-2;

***99. Соотнесите функции, выполняемые техническими средствами защиты:***

1. внешняя защита
2. опознавание
3. внутренняя защита
4. защита от воздействия дестабилизирующих факторов, проявляющихся непосредственно в средствах обработки информации
5. защита от воздействия дестабилизирующих факторов, проявляющихся за пределами основных средств АСОД
6. специфическая группа средств, предназначенных для опознавания людей по раз личным индивидуальным характеристикам

# ОТВЕТ: 1-2; 2-3; 3-1

***100. Соотнесите степени сложности устройств:***

1. простые устройства
2. системы
3. сложные устройства
4. комбинированные агрегаты, состоящие из некоторого количества простых устройств, способные к осуществлению сложных процедур защиты;
5. несложные приборы и приспособления, выполняющие отдельные процедуры защиты;
6. законченные технические комплексы, способные осуществлять некоторую комбинированную процедуру защиты, имеющую самостоятельное значение;

# ОТВЕТ: 1-2; 2-3; 3-1;

***101. Соотнесите основные виды угроз для АС:***

1. Угроза нарушения конфиденциальности
2. Угроза отказа служб
3. Угроза нарушения целостности
4. Любое умышленное изменение информации, хранящейся в ВС или передаваемой от одной системы в другую
5. Возникает всякий раз, когда в результате преднамеренных действий, предпринимаемых другим пользователем или злоумышленником, блокируется доступ к некоторому ресурсу АС
6. Заключается в том, что информация становится известной тому, кто не располагает полномочиями доступа к ней

# ОТВЕТ: 1-3; 2-2; 3-1

***102. Соотнесите классификацию угроз по ряду признаков:***

1. по природе возникновения
2. по непосредственному источнику
3. по степени воздействия на АС
4. по способу доступа к ресурсам АС
5. пассивные и активные
6. направленные на использование прямого стандартного пути доступа к ресурсам и направленные на использование скрытого нестандартного доступа к ресурсам АС
7. естественные или искусственные
8. природная среда, человек, санкционированные программные средства и несанкционированные программные средства

# ОТВЕТ: 1-3; 2-4; 3-3;4-1

# ПРАВИЛА ВЫПОЛНЕНИЯ ПРАКТИЧЕСКИХ РАБОТ

**Подготовка к выполнению практических работ**. Практические работы в группах проводятся в соответствии с расписанием учебных занятий в колледже в течение определенного времени. Поэтому для выполнения практических работ обучающийся должен руководствоваться следующими положениями:

* Предварительно ознакомиться с графиком выполнения практических работ;
* Внимательно ознакомиться с описанием соответствующей практической работе и установить, в чем состоит основная цель и задача этой работы;
* По лекционному курсу и соответствующим литературным источникам изучить теоретическую часть, относящуюся к данной практической работе;
* Неподготовленные к работе обучающиеся к выполнению практической работы не допускаются.

После окончания работы рабочее место должно быть приведено в порядок.

В течение всего времени занятий обучающиеся обязаны находиться на своих рабочих местах. Выходить из помещения во время занятий можно только с разрешения преподавателя.

# Оформление отчета по практическим работам.

Составление отчета о проведенных исследованиях является важнейшим этапом выполнения практической работы. По каждой выполненной работе в рабочей тетради составляют отчет, руководствуясь следующими положениями:

* Указать название и порядковый номер лабораторной работы, а также краткое сформулировать цель работы;
* Схемы и графики чертить с соблюдением принятых стандартных условий обозначений;
* Отчет по каждой практической работе должен содержать основные выводы. В за-

головке отчета указывают номер работы и ее полное наименование. При составлении отчета нужно кратко описать цель работы, ее содержание, указать использованные аппаратуру и оборудование.

* При выполнении практической работ необходимо строго следовать правилам техники безопасности.

# Критерии оценки работ

**Оценка «отлично»** ставится, если обучающийся выполнил работу в полном объеме с соблюдением необходимой последовательности действий; в «Отчете к практическим работам» правильно выполняет все записи, таблицы, рисунки, чертежи, графики, вычисления; правильно выполняет анализ ошибок.

**Оценка «хорошо»** ставится, если обучающийся выполнил требования к оценке "5", но допущены 2-3 недочета.

**Оценка «удовлетворительно»** ставится, если обучающийся выполнил работу не полностью, но объем выполненной части таков, что позволяет получить правильные результаты и выводы; в ходе проведения работы были допущены ошибки. Оценка «неудовлетворительно» ставится, если обучающийся выполнил работу не полностью или объем выполненной части работы не позволяет сделать правильных выводов.

***Раздел 1. Основные методы обеспечения качества функционирования***

**Практическая работа № 1. «Тестирование программных продуктов»**

СОДЕРЖАНИЕ РАБОТЫ

Тестирование программных продуктов, анализ работоспособности и жизненного цикла. Выявление ошибок. Исправление ошибок, отладка программного средства с учетом выявленных проблем.

**Практическая работа № 2. «Сравнение результатов тестирования с требованиями технического задания и/или спецификацией»**

СОДЕРЖАНИЕ РАБОТЫ

Сравнение результатов тестирования с требованиями технического задания и/или спецификацией Исправление ошибок, отладка программного средства с учетом выявленных проблем.

**Практическая работа № 3. «Анализ рисков»**

СОДЕРЖАНИЕ РАБОТЫ

Анализ рисков работоспособности программного продукта, рекомендации по устранению и предотвращению рисков.

**Практическая работа № 4. «Выявление первичных и вторичных ошибок»**

СОДЕРЖАНИЕ РАБОТЫ

Выявление первичных и вторичных ошибок, Исправление ошибок, отладка программного продукта с учетом выявленных ошибок

# *Раздел 2. Методы и средства защиты компьютерных систем*

**Практическая работа №5. «Обнаружение вируса и устранение последствий его**

**влияния»**

СОДЕРЖАНИЕ РАБОТЫ

Обнаружение вируса и устранение последствий его влияния. Созданий рекомендаций или алгоритма зашиты системы от вирусов.

**Практическая работа № 6«Установка и настройка антивируса. Настройка обновлений с помощью зеркала»**

СОДЕРЖАНИЕ РАБОТЫ

Установка и настройка антивируса. Настройка обновлений с помощью зеркала. Созданий алгоритма по настройке антивирусной зашиты, ее постоянного обновления.

**Практическая работа № 7. «Настройка политики безопасности»**

СОДЕРЖАНИЕ РАБОТЫ

Настройка политики безопасности компьютерной системы с учетом специфика объекта

**Практическая работа № 8. «Настройка браузера»**

СОДЕРЖАНИЕ РАБОТЫ

Настройка браузера, его эксплуатация, способы настройки с учетом использования на объекте

**Практическая работа № 9. «Работа с реестром»**

СОДЕРЖАНИЕ РАБОТЫ

Работа с реестром, его настройка, исправление ошибок

**Практическая работа № 10. «Работа с программой восстановления файлов и очистки дисков»**

СОДЕРЖАНИЕ РАБОТЫ

Работа с программой восстановления файлов, резервное копирование, сохранение и восстановление информации, очистки дисков.

**4.КОНТРОЛЬНО-ОЦЕНОСНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ**

Формой промежуточной аттестации по учебной дисциплине МДК 04.02 в соответствии с учебным планом специальности 09.02.07 Информационные системы и программирование является экзамен.

Условием допуска к экзамену является положительный результат в ходе текущего контроля в процессе изучения дисциплины и выполнения всех практических занятий, предусмотренных рабочей программой.

Экзамен проводится в форме устного опроса обучающегося по билету, включающему 2 теоретических вопроса и решение ситуационной задачи. Вопросы к экзамену охватывают наиболее значимые из тем, предусмотренных рабочей программой.

Критерии оценки для промежуточной аттестации:

Промежуточная аттестация предназначена для определения уровня освоения всего объема учебной дисциплины. Для оценивания результатов обучения при проведении промежуточной аттестации используется 4-балльная шкала.

|  |  |
| --- | --- |
| ***4-балльная*** | |
| 5 | Отлично |
| 4 | Хорошо |
| 3 | Удовлетворительно |
| 2 | Неудовлетворительно |

При определении уровня достижений, обучающих на экзамене, обращается особое внимание на следующее:

* + - * дан полный, развернутый ответ на поставленный вопрос;
      * показана совокупность осознанных знаний об объекте, проявляющаяся в свободном оперировании понятиями, умении выделить существенные и несущественные признаки, причинно-следственные связи;
      * знание об объекте демонстрируются на фоне понимания его в системе данной дисциплины и междисциплинарных связей;
      * ответ формулируется в терминах дисциплины, изложен литературным языком, логичен, доказателен, демонстрирует авторскую позицию обучающегося;
      * теоретические постулаты подтверждаются примерами из практики.

# Контрольные вопросы (тестовые задания) для проведения промежуточной аттестации

1. ***Легкость применения программного обеспечения это:***

а) характеристики ПО, позволяющие минимизировать усилия пользователя по подготовке исходных данных, применению ПО; +

б) отношение уровня услуг, предоставляемых ПО пользователю при заданных условиях, к объему используемых ресурсов;

в) характеристики ПО, позволяющие минимизировать усилия по внесению изменений для устранения в нем ошибок и по его модификации.

1. ***Мобильность программного обеспечения это:***

а) способность ПО выполнять набор функций, которые удовлетворяют потребности пользователей;

б) способность ПС безотказно выполнять определенные функции при заданных условиях в течение заданного периода времени;

в) способность ПО быть перенесенным из одной среды (аппаратного / программного) в другое. +

1. ***Укажите правильную последовательность этапов при каскадной модели жизненного цикла:***

а) Определение требований -> Тестирование -> Реализация; б) Проектирование -> Реализация -> Тестирование;

в) Проектирование -> Определение требований -> Реализация. ***4 Устойчивость программного обеспечения — это:***

а) свойство, характеризующее способность ПС завершать автоматически корректное функ ционирование ПК, несмотря на неправильные (ошибочные) входные данные;

б) свойство, способна противостоять преднамеренным или непреднамеренным деструктивным действиям пользователя; +

в) свойство, характеризующее способность ПС продолжать корректное функционирова ние, несмотря на неправильные (ошибочные) входные данные.

1. ***UML — это:***

а) язык программирования, имеющий синтаксис схож с С ++;

б) унифицированный язык визуального моделирования, использует нотацию диаграмм; + в) набор стандартов и спецификаций качества программного обеспечения.

1. ***При конструировании программного обеспечения процесс решения задачи составляет***

а) 90 — 95%;

б) 50%;

в) 5 — 10%.

1. ***При конструировании программного обеспечения на этапе разработки или выбора алгоритма решения реализуется следующее:***

а) архитектурное обработки программы; в) алгебраическое программирования. +

1. ***Как называется процесс разбиения одной сложной задачи на несколько простых подза- дач?***

а) абстракция;

б) декомпозиция; + в) реинжиниринг.

1. ***Что из приведенного является критериями оценки удобства интерфейсов?***

а) скорость обучения;

б) адаптация к стилю работы пользователя;

в) все ответы правильные. +

1. ***Интерфейс пользователя — это***

а) набор методов взаимодействия компьютерной программы и пользователя этой про- граммы; +

б) набор методов для взаимодействия между программами; в) способ взаимодействия между объектами.

1. ***Интерфейс - это***

а) прежде всего, набор правил;

б) набор задач пользователя, которые он решает с помощью системы; в) способ взаимодействия между объектами. +

1. ***Техническое задание — это***

а) документ объяснений для заказчика;

б) исходный документ для сдачи ПО в эксплуатацию;

в) выходной документ для проектирования, разработки автоматизированной системы. + ***13 Анализ требований —***

а) отображение функций системы и ее ограничений в модели проблемы; +

б) показатель, который определяет необходимые усилия для диагно стики случаев отказов;

в) отображение частей программ, которые будут модифицироваться. ***14 Архитектура программной системы —***

а) декомпозиция решения для выделенного спектра задач домена на подсистемы или иерархию подсистем;

б) определение системы в терминах вычислительных составляющих (подсистем) и интерфейсов между ними, которое отражает правила декомпозиции проблемы на составляющие;

+

в) соответствующие вариации состава выделенных компонент. ***15 Агрегация —***

а) отношения, утверждает наличие связи между понятиями, не уточняя зависимости их со держания и объемов;

б) возможность для некоторого класса находиться одновременно в связи с одним элемен том из определенного множества классов;

в) объединение нескольких понятий в новое понятие, существенные признаки нового понятия при этом могут быть либо суммой компонент или существенно новыми (отношение

«доля — целое»). + ***16 Ассоциация —***

а) возможность для некоторого класса находиться одновременно в связи с одним элементом из определенного множества классов;

б) объединение нескольких понятий в новее понятия, существенные признаки нового понятия о этом могут быть либо суммой компонент или существенно новыми (отношение

«доля — целое»);

в) самое общее отношение, утверждает наличие связи между понятиями, не уточняя зависимости их содержания и объемов. +

***17 Валидация —***

а) обеспечение соответствия разработки требованиям ее заказчиков. + б) проверка правильности трансформации проекта в код реализации; в) выявление всех ошибок.

***18 Верификация —***

а) обеспечение соответствия разработки требованиям ее заказчиков; б) проверка правильности трансформации проекта в программу; +

в) действия на каждой стадии жизненного цикла с проверки и подтверждения соответствия стандартам.

***19 Внутренние метрики продукта:***

а) метрики сопровождения; б) метрики годности;

в) метрики стиля. +

***20 Продукты инженерии требований по методу С.Шлеер и С.Меллора:***

а) информационная модель системы; +

б) описание интерфейсов сценариев и актеров; в) неформальное описание сценариев и актеров.

1. ***К процессу разработки ПО включает следующие процессы:***

а) сопровождения;

б) проектирование; + в) эксплуатация.

1. ***Последовательность работ по каскадной моделью:***

а) требования, проектирование, реализация; +

б) проектирование, сопровождение, тестирование; в) требования, сопровождение, тестирование.

1. ***Проектирование —***

а) преобразование требований в последовательность проектных решений по системе; + б) определение главных структурных особенностей системы;

в) определение подробностей функционирования и связей для всех компонент системы. ***24 Модель жизненного цикла —***

а) определение определенных действий, которые сопровождают изменения состояний объ ектов;

б) типичная схема последовательности работ на этапах разработки программного продукта; +

в) отражение динамики изменений состояния каждого класса объектов. ***25 Понятность — это***

а) атрибут функциональности, указывающий на возможность предотвращать НСД;

б) атрибут надежности, который указывает на способность программы к перезапуску для повторного выполнения;

в) атрибут удобства, определяющий усилия, необходимые для распознавания логических концепций и условий их применения. +

# Контрольные вопросы для проведения промежуточной аттестации 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 защиты

**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:

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 минимазации 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:

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 функцичми, 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, обусловливающих пригодность информации удовле- творять определенные потребности в соответствии с ее назначением, называется:

* + Ответ: качеством информации

**Вопрос 56.** Гарнтия 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.

# Практическое задание для проведение промежуточной аттестации (пример)

|  |  |  |
| --- | --- | --- |
| Задание | Показатель оценки  результатов | Кол-во  баллов |
| **Задание 1.** На своем персональном рабочем месте установите соответствующую программу, скачав её из интернета. При этом выполните следующие виды работ:   1. Определите назначение программного обеспечения (опишите основные направления деятельности). 2. Выявите и устраните проблемы, связанные с установкой программного обеспечения наиболее удобным способом (специальные программы, системные средства устранения проблем, учетной записи и т. д.). 3. Проведите обновление версии программного продукта. 4. Проведите настройку программного обеспечения под соответствующую операционную систему. 5. Провести очистку системного реестра. | Назначение программы определено правильно – макс. – 3  балла. |  |
| Устранение проблемы выполнено правильно – макс. – 5  балла. |  |
| Пример создан, про грамма функционирует –макс. – 4 балла. |  |
| Правильно описаны сценария тестирования – макс. – 3 балла. |  |
|  | Настройки  определены правильно –  макс. – 5 балла. |  |
|  | Обновление  произведено правильно – макс. – 4 балла. |  |
| **Задание 2.** На основе ГОСТ 19.505-79 разработать сборник рекомендаций по обучению персонала правилам эксплуатации отраслевого программного обеспечения | Слайды разработаны и оформлены – макс.  – 3 балла |  |
|  | Требования  Определены  правильно –  макс. – 3 балла. |  |
|  | Правильно  разработан опросник – макс.  – 6 балла. |  |
|  | Требования определены  правильно – макс. – 3  балла. |  |
| **Всего баллов:** | |  |

ВСЕГО – 39 баллов

**Оценка «5»** ставится при выполнении заданий на **35-39 баллов Оценка «4»** ставится при выполнении заданий на **31-34 баллов Оценка «3»** ставится при выполнении заданий на **27-30 баллов**

**Оценка «2»** ставится при выполнении заданий на **менее 27 баллов.**

# Устное обоснование (защита выполненной работы):

1. Грамотно построена речь (да - 1 балл, нет – 0 баллов). Количество баллов - \_\_\_.
2. Использование терминологии (да – 1 балл, нет – 0 баллов). Количество баллов - \_\_\_.

1. **ПЕРЕЧНЬ ПЕЧАТНЫХ ИЗДАНИЙ, ЭЛЕКТРОННЫХ ИЗДАНИЙ**

**(ЭЛЕКТРОННЫХ РЕСУРСОВ), ДОПОЛНИТЕЛЬНЫХ ИСТОЧНИКОВ**

Для реализации программы библиотечный фонд образовательной организации должен иметь печатные и/или электронные образовательные и информационные ресурсы, рекомендуемых для использования в образовательном процессе.

*Основные источники:*

1. Федорова Г.И. Разработка, внедрение и адаптация программного обеспечения отраслевой направленности. Учебное пособие. Изд.: КУРС, Инфра-М. Среднее профессиональное образование. 2016 г. 336 стр.
2. Рудаков А. Технология разработки программных продуктов: учебник. . –М.: Издательство Academia. Среднее профессиональное образование. 2019 г. - 208 с.
3. Федорова Г., Рудаков А. Технология разработки программных продуктов. Практикум: учебное пособие. . – М.: Издательство Academia. Среднее профессиональное образование. 2017 г. - 192 с.

*Дополнительные источники:*

1. Гвоздева, В. А. Основы построения автоматизированных информационных систем: учебник / В. А. Гвоздева, И. Ю. Лаврентьева. -М.: ФОРУМ-ИНФРА-М, 2007.-256 с.
2. Орлов С.А., Цилькер Б.Я. Технологии разработки программного обеспечения: учебник.– Издательство Инфра-М.: 2016, - 609 с.
3. Проектирование и реализация прикладного программного обеспечения: учебное пособие. Влацкая И. В., Заельская Н. А., Надточий Н. С. – М.: ОГУ. 2015 г. - 119 с

*Интернет-ресурсы:*

1. От модели объектов - к модели классов. Единое окно доступа к образовательным ресурсам. <http://real.tepkom.ru/Real_OM-CM_A.asp>
2. 2. Технология разработки программного обеспечения: - http://window.edu.ru/catalog/pdf2txt/195/19195/1551