

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования «Саратовский государственный технический
университет имени Гагарина Ю.А.»

Энгельсский технологический институт (филиал)



УТВЕРЖДАЮ
Зам. директора по СПДО
О.Г. Коваленко

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

**ПМ.03 Сопровождение и обслуживание программного обеспечения
компьютерных систем**

по специальности:

09.02.07 Информационные системы и программирование

Методические указания
рассмотрены на заседании
предметной (цикловой) методической комиссии
специальности 09.02.07
«25» июня 2024 года, протокол № 11

Председатель ПЦМК  А.А. Сдобнова

Энгельс 2024

ОРГАНИЗАЦИЯ - РАЗРАБОТЧИК:

Энгельсский технологический институт (филиал) федерального государственного бюджетного образовательного учреждения высшего образования «Саратовский государственный технический университет имени Гагарина Ю.А.»

РАЗРАБОТЧИК: Зотов А.А преподаватель спецдисциплин ОСПДО

Пояснительная записка

В результате освоения ПМ.03 Сопровождение и обслуживание программного обеспечения компьютерных систем обучающийся должен обладать предусмотренными ФГОС по специальности следующими умениями, знаниями, профессиональными компетенциями, общими компетенциями:

В результате освоения профессионального модуля студент 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.

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.

Перечень профессиональных компетенций:

ВД 4 Сопровождение и обслуживание программного обеспечения компьютерных систем

ПК 4.1. Осуществлять инсталляцию, настройку и обслуживание программного обеспечения компьютерных систем.

ПК 4.2 Осуществлять измерения эксплуатационных характеристик программного обеспечения компьютерных систем

ПК 4.3 Выполнять работы по модификации отдельных компонент программного обеспечения в соответствии с потребностями заказчика

ПК 4.4 Обеспечивать защиту программного обеспечения компьютерных систем программными средствами.

Перечень общих компетенций:

Код	Наименование общих компетенций
ОК 01.	Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности;
ОК 02.	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по финансовой грамотности в различных жизненных ситуациях.
ОК 03.	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по финансовой грамотности в различных жизненных ситуациях
ОК 04.	Эффективно взаимодействовать и работать в коллективе и команде
ОК 05.	Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста.
ОК 06.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения
ОК 07.	Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях
ОК 08.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности
ОК 09.	Пользоваться профессиональной документацией на государственном и иностранном языках

В ФОС по профессиональному ПМ.03 Сопровождение и обслуживание программного обеспечения компьютерных систем, включены:

1) текущий контроль успеваемости:

- входной контроль знаний;
- рубежный контроль успеваемости;
- межсессионная аттестация.

2) промежуточная аттестация:

МДК. 03.01 Внедрение и поддержка компьютерных систем – экзамен

МДК. 03.02 Обеспечение качества функционирования компьютерных систем

– экзамен

- экзамен по модулю.

Информационное обеспечение

Перечень используемых учебных изданий, интернет-ресурсов, дополнительной литературы

Печатные издания

Электронные издания (электронные ресурсы)

1. Гниденко, И. Г. Технология разработки программного обеспечения : учебное пособие для среднего профессионального образования / И. Г. Гниденко, Ф. Ф. Павлов, Д. Ю. Федоров. — Москва : Издательство Юрайт, 2021. — 235 с. — (Профессиональное образование). — ISBN 978-5-534-05047-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/472502>

2. Черткова, Е. А. Программная инженерия. Визуальное моделирование программных систем : учебник для среднего профессионального образования / Е. А. Черткова. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2021. — 147 с. — (Профессиональное образование). — ISBN 978-5-534-09823-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/473307>

3. Сергеев, А. Г. Стандартизация и сертификация : учебник и практикум для среднего профессионального образования / А. Г. Сергеев, В. В. Терегеря. — Москва : Издательство Юрайт, 2021. — 323 с. — (Профессиональное образование). — ISBN 978-5-534-04315-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/469819>

4. Трофимов, В. В. Основы алгоритмизации и программирования : учебник для среднего профессионального образования / В. В. Трофимов, Т. А. Павловская ; под редакцией В. В. Трофимова. — Москва : Издательство Юрайт, 2021. — 137 с. — (Профессиональное образование). — ISBN 978-5-534-07321-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/473347>

5. Илюшечкин, В. М. Основы использования и проектирования баз данных : учебник для среднего профессионального образования / В. М. Илюшечкин. — испр. и доп. — Москва : Издательство Юрайт, 2021. — 213 с. — (Профессиональное образование). — ISBN 978-5-534-01283-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/471698>

Интернет-ресурсы

1. Образовательный портал INTUIT.RU <http://www.intuit.ru>
2. METANIT.COM. Сайт о программировании <https://metanit.com>
3. Журнал «Успехи современной науки» - Режим доступа: <https://www.elibrary.ru/item.asp?id=27712534>
4. Журнал «Известия Высших учебных заведений. Поволжский регион. Технические науки – Режим доступа: <https://www.elibrary.ru/item.asp?id=44291082>

Электронно-библиотечные системы:

1. «ЭБС IPRbooks», ООО «Ай Пи Эр Медиа»
2. ЭБС «Электронная библиотека технического вуза», ООО «Политехресурс»
3. ЭБС «Лань», ООО «Издательство Лань»
4. «ЭБС elibrary», ООО «РУНЭБ»
5. ЭБС «ЮРАЙТ»
6. ЭБС «Book.ru»

Входной контроль

Форма контроля: выполнение письменной работы

Время выполнения: 40 минут.

Вариантов вопросов:

1. Основные положения ГОСТ Р ИСО/МЭК 12207.
2. Основные процессы и взаимосвязь между документами в информационной системе согласно стандартам
3. Виды внедрения, план внедрения.
4. Стратегии, цели и сценарии внедрения.
5. Функции менеджера сопровождения и менеджера развертывания
6. Типовые функции инструментария для автоматизации процесса внедрения информационной системы
7. Оценка качества функционирования информационной системы.
8. CALS-технологии
9. Организация процесса обновления в информационной системе.
10. Регламенты обновления
11. Тестирование программного обеспечения в процессе внедрения и эксплуатации.
12. Эксплуатационная документация

Критерии оценивания:

Оценка 5 «отлично» теоретическое содержание курса освоено полностью, без пробелов, умения сформированы, все предусмотренные программой учебные задания выполнены, качество их выполнения оценено высоко.

Оценка 4 «хорошо» теоретическое содержание курса освоено полностью, без пробелов, некоторые умения сформированы недостаточно, все предусмотренные программой учебные задания выполнены, некоторые виды заданий выполнены с ошибками.

Оценка 3 «удовлетворительно» теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые умения работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий содержат ошибки.

Оценка 2 «неудовлетворительно» теоретическое содержание курса не освоено, необходимые умения не сформированы, выполненные учебные задания содержат грубые ошибки

МДК. 03.01 Внедрение и поддержка компьютерных систем

Тема 1.1 Основные методы внедрения и анализа функционирования программного обеспечения

Форма контроля: тестирование

Время выполнения: 60 минут

Задание: выполнить тест

1. Построение SADT-модели включает в себя выполнение следующих действий:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

- Написание программного обеспечения для разрабатываемой системы по требованиям заказчика
- + Сбор информации об объекте, определение его границ
- + Определение цели и точки зрения модели, построение, обобщение и декомпозиция диа-грамм
- Представление исследуемой системы в графическом виде
- Представление исследуемого объекта средствами системного моделирования
- + Критическая оценка, рецензирование и комментирование
- Разработка, отладка и тестирование программного обеспечения
- Использование графических пакетов для представления системы в виде модели

2. Моделирование основывается на принципах:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

- + Выбор модели оказывает определяющее влияние на подход к решению проблемы и то, как будет выглядеть это решение
- Декомпозиции системы на отдельные подзадачи
- Инкапсуляции и полиморфизма
- Децентрализации управления системой
- + Каждая модель может быть представлена с различной степенью точности; лучшие мо-дели – те, что ближе к реальности
- Открытой трансформируемой системы
- + Нельзя ограничиваться созданием только одной модели. Наилучший подход при разработке любой нетривиальной системы – использовать совокупность нескольких моделей, почти независимых друг от друга
- Анализа и синтеза проектирования систем

3. В бизнес-процессах выделяют классы процессов:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

- Решающие бизнес-процессы
- Регламентирующие бизнес-процессы
- + Основные бизнес-процессы

- Бизнес-процессы поведения системы
- Программируемые бизнес-процессы
- Экономические бизнес-процессы
- + Обеспечивающие бизнес-процессы
- + Бизнес-процессы управления

4. CASE-средства классифицируются по следующим признакам:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

- + По применяемым методологиям и моделям систем и БД
- По используемому программному обеспечению
- По этапам жизненного цикла программного обеспечения
- + По степени интегрированности с СУБД
- По уровням детализации и декомпозиции проектируемой системы
- + По доступным платформам
- По используемым языкам программирования
- По степени сложности моделируемой системы

5. К малым интегрированным средствам моделирования относятся:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

- ARIS Toolset
- Design/IDEF
- + ERwin
- + BPwin
- Designer/2000
- Paradigm Plus
- + Model Mart
- Rational Rose

6. К средним интегрированным средствам моделирования относятся:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

- Rational Rose
- + Design/IDEF
- BPwin
- + Designer/2000
- + ARIS Toolset
- Model Mart
- Paradigm Plus
- ERwin

7. К инструментальным средствам объектно-ориентированного анализа и проектирования относятся:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

- + Rational Rose
- Model Mart
- + MS Visio
- + ARIS
- IDEF1X
- Erwin
- BPwin
- JAM

8. К инструментальным средствам представления функциональных моделей относятся:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

- JAM
- + Model Mart
- MS Visio
- ARIS
- IDEF0
- + Erwin
- + BPwin
- Rational Rose

9. Методологии, поддерживаемые в BPwin:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

- IDEF1X
- + IDEF0
- IDEF1
- + IDEF3
- IDEFX
- IDEF5
- + DFD
- DFD1X

10. Диаграмма IDEF0 может содержать следующие типы диаграмм:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

- Диаграмму классов
- + Контекстную диаграмму, диаграмму декомпозиции
- Диаграмму компонентов
- + Диаграмму дерева узлов
- Диаграмму взаимодействий
- + Диаграмму только для экспозиции (FEO)

- Диаграмму последовательности, диаграмму кооперации
- Диаграмму узлов

11. Уровни логической модели:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

- Диаграмма сущность
- Диаграмма связь
- Диаграмма пакетов
- + Диаграмма сущность-связь
- Модель данных, основанная на классах
- + Модель данных, основанная на ключах
- Полная операционная модель
- + Полная атрибутивная модель

12. Внутренние стрелки не входящие в состав диаграммы IDEF0:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

- + mechanism- output
- output-input
- + mechanism- input
- output-control
- output-input feedback
- output-control feedback
- output-mechanism
- + control feedback- mechanism

13. Типы стрелок не входящие в состав диаграммы IDEF0:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

- Input
- + Editor
- Control
- + Properties
- Output
- Mechanism
- Call
- + Dictionary

14. Quick Reports – создание простейших отчетов – позволяет создавать отчеты:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

- Group/Totals. Табличный отчет с автоматической группировкой и сортировкой данных
- Report Header. Печатается единожды в начале отчета
- + Columnar. Простой табличный отчет
- Page Header. Печатается в верхней части каждой страницы

- + Vertical. Простой вертикальный отчет
- Group Header. Печатается в начале каждой группы
- + Blank Report. Бланк. Создается пустой бланк отчета, в который не включаются данные
- Detail. Печатается для каждой строчки набора данных

15. BРwin допускает следующие переходы с одной нотации на другую:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

- IDEF3 → DFD
- DFD → IDEF0
- + IDEF0 → DFD
- DFD → DFD
- IDEF3 → IDEF0
- + IDEF0 → IDEF3
- IDEF3 → IDEF3
- + DFD → IDEF3

16. DFD описывает:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

- Функции обработки стрелок (arrow)
- + Функции обработки информации (работы)
- Внешние ссылки (external references), объекты, сотрудников или отделы, которые участвуют в обработке информации
- + Документы (стрелки, arrow), объекты, сотрудников или отделы, которые участвуют в обработке информации
- Функции обработки внешних ссылок
- + Внешние ссылки (external references), таблицы для хранения документов (хранилищ данных, data stor+ E)
- Функции обработки документов
- Документы (стрелки, arrow), объекты, сотрудников или отделы, которые участвуют в обработке внешних стрелок

17. BРwin позволяет создавать на диаграмме DFD типы граничных стрелок:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

- + Обычная граничная стрелка
- Специальная стрелка
- Внутренняя ссылка
- + Межграничная ссылка и тоннельная стрелка
- + Внешняя ссылка
- Страничная ссылка и теневая стрелка
- Контрольная стрелка
- Стрелка механизм

18. Создать отчет в BRwin возможно с помощью:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

+ Встроенных шаблонов

- Программных модулей, создаваемых разработчиком на языке Visual Basic
- Создать отчет в BRwin не возможно

+ Report Template Builder

- Отчет создается разработчиком
 - Отдельно поставляемых программ
 - Встроенных мастер-функций
- + RPTwin

19. В BRwin 4.0 отчеты могут быть экспортированы в распространенные форматы:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

+ Текстовый

- Символьный

+ MS Office

- Графический

+ HTML

- Internet Explorer
- Acrobat

20. Поддерживаемые в RPTwin типы операторов:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

+ Текстовый оператор конкатенации (&)

- Символ
- Текст
- Дата

+ Арифметические

- Графический оператор конкатенации (&)

+ Логические

- Номер

21. Инструментальное средство ERwin позволяет:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

- Редактировать и отлаживать программы

+ Проектировать на физическом и логическом уровне модели данных

- Управлять процессом конструирования ПО
- Проектировать диаграммы вариантов использования и взаимодействий

+ Проводить процессы прямого и обратного проектирования баз данных

- Управлять процессом трансляции и отладки программ

+ Выравнивать модель и содержимое системного каталога после редактирования

- Проектировать контекстные диаграммы и диаграммы декомпозиции

22. ERwin позволяет создавать модели следующих типов:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

- + Модель, имеющую только логический уровень
- Модель, имеющую абстрактный уровень
- Модель, имеющую абстрактный и физический уровни
- + Модель, имеющую только физический уровень
- Модель, имеющую абстрактный и логический уровни
- + Модель, имеющую как логический уровень, так и физический уровень
- Модель, имеющую концептуальный уровень
- Модель, имеющую контекстный уровень

23. Точки зрения организации в ARIS:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

- Структура внедрения и структура потоков
- + Организационная структура
- Управленческая структура
- Поведенческая структура
- + Функциональная структура
- Коммуникационная структура
- + Структура данных и структура процессов
- Обобщенная структура

24. Уровни точки зрения в ARIS:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

- Описание структуры
- + Описание требований
- Описание поведения
- Описание разработки
- + Описание спецификации
- + Описание внедрения
- Описание процессов
- Описание классов

25. Методы описания, используемые в ARIS:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

- EPT – метод описания потоков
- + EPC - метод описания процессов
- ERM - модель сущность-связь для описания структуры объектов
- + ERM - модель сущность-связь для описания структуры данных
- EPP – метод описания пакетов
- EPC – метод описания компонентов
- + UML - унифицированный язык моделирования
- EPT – метод описания нитей

26. К основным компонентам инструментов ARIS Toolset относятся:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

- Internet (интернет)
- WordPad (ввод текстовых данных)
- Media (средство для медиа описания моделей)
- + Explorer (проводник)
- Acrobat (чтение текстовых данных)
- + Designer (средство для графического описания моделей)
- Document (для ввода различных параметров и атрибутов) и выноски
- + Таблица (для ввода различных параметров и атрибутов) и мастер (Wizards)

27. ARIS Business Optimizer позволяет:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

- + Определять целевые затраты и рассчитывать стоимость продукта: во что компании об-ходится предоставление отдельных продуктов
 - Принимать решения о времени начала и окончания работы над проектом
- + Принимать решения по аутсорсингу: стоит ли поручить выполнение бизнес-процессоввнешнему поставщику услуг
 - Определять последовательность работ , выполняемых в ходе работы над проектом
 - Определять требования к персоналу компании, которая в дальнейшем будет эксплуати-ровать программное обеспечение
 - Рассчитывать заработную плату сотрудников компании после внедрения программногообеспечения
 - Планировать требования к обслуживающему персоналу, сопровождающему программ-ное обеспечение
- + Планировать требования к персоналу: сколько необходимо сотрудников для оптималь-ного выполнения работ

28. «Взгляды» ARIS:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

- + Процессы
 - Потоки
- + Функции (с целями)
- + Данные и организация
 - Процедуры
 - Управление и внедрение
 - Нити
 - Память

29. MS Visio позволяет создавать схемы, чертежи, диаграммы с помощью:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

- + Встроенных шаблонов

- Панели инструментов
- + Трафаретов
- Графических редакторов
- Дополнительного программного обеспечения
- Панели рисования
- + Стандартных модулей
- Панели автофигур

30. Язык UML – это:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

- Язык программирования высокого уровня
- + Унифицированный язык моделирования
- Язык для разработки систем искусственного интеллекта
- + Unified Modeling Language
- Язык управления базами данных
- + Язык для визуализации, специфицирования, конструирования и документирования артефактов программных систем
- Язык создания запросов в базах данных
- Язык программирования низкого уровня

31. Моделирование в UML позволяет решать задачи:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

- Анализа и синтеза систем управления
- Разработать и отладить программное обеспечение
- + Визуализировать систему в ее текущем или желательном для нас состоянии
- Провести тестирование разработанного программного обеспечения
- + Описать структуру или поведение системы; получить шаблон, позволяющий сконструировать систему
- Смоделировать разрабатываемую информационную систему
- + Документировать принимаемые решения, используя полученные модели
- Рассчитать экономическую эффективность от внедрения программного обеспечения

32. UML, как язык документирования, помимо исполняемого кода производит и другие продукты, включающие:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

- + Требования, архитектуру, проектные решения
- Спецификацию технических средств
- + Дизайн, исходный код, проектные планы,
- Требования к уровню квалификации разработчиков
- Набор заданий для тестирования программного обеспечения
- Требования к уровню квалификации персонала сопровождения
- + Тесты, прототипы, релизы (версии)

- Требования к выбору языка программирования

33. UML включает синтаксические и семантические правила для:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

- Агрегации
- Тестирования
- + Имен, областей действия
- Сборки
- Сопровождения
- + Видимости, целостности
- Вывода из эксплуатации
- + Исполнения

34. Механизмы расширения UML включают:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

- Исключения
- + Стереотипы
- Дополнения
- Управления
- + Помеченные значения
- Слияния
- + Ограничения
- Объединения
-

35. Аппаратные инструментальные средства разработки ПО – это:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

- Система для разработки новых программ на конкретном языке программирования
- Средства создания и редактирования текстов программ
- + Микропроцессор и подключаемые (внешние) устройства
- + Устройства вычислительной системы, специально предназначенные для поддержки разработки ПО
- + Периферийные устройства, микропроцессор вычислительного комплекса, предназначенные для разработки нового ПО
- Программное обеспечение, написанное на языках программирования низкого уровня
- Программы, которые используются в ходе разработки, корректировки или развития других прикладных или системных программ
- Программы, используемые для корректировки и тестирования других прикладных или системных программ

36. Программные инструментальные средства разработки ПО – это:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

+ Программы, позволяющие выполнить все работы, определенные методологией проек-тирования ПО

- Системное программное обеспечение, позволяющее сопровождать офисные программ-ные пакеты

- Средства создания текстовых документов

+ Программное обеспечение, используемое на всех стадиях разработки нового ПО

- Программное обеспечение для настройки офисных приложений на условия конкретного применения

+ Программы, которые используются в ходе разработки, корректировки или развития других прикладных или системных программ

- Устройство компьютера, специально предназначенное для поддержки разработки про-граммных средств

- Средства создания и редактирования текстовых документов

37. К этапам развития технологии разработки программного обеспечения относятся:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

+ «Процедурное» программирование

- Программирование на алгоритмических языках высокого уровня

+ Структурный подход к программированию

- Программирование на языках низкого уровня

+ Компонентный подход и CASE-технологии

- Машинно-ориентированное программирование

- Машинно-независимое программирование

- Подход к разработке ПО, основанный на стратегии поиска

38. «Стихийное» программирование:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

- Разработка программного обеспечения без предварительного составления плана-гра- фики работ

+ Первый этап в истории развития технологии разработки программного обеспечения, когда программирование фактически было искусством

+ Период в истории разработки программного обеспечения, когда программа создавалась одним программистом, способным отслеживать последовательность выполняемых опе- раций и местонахождения данных в программе

- Разработка программ с использованием различных языков программирования низкого и высокого уровня

- Разработка программ с элементами случайного выбора алгоритмов решения задачи
- + Характеризуется тем, что типичная программа этого периода состояла из основной программы, области глобальных данных и набора подпрограмм (в основном библиотечных), выполняющих обработку всех данных или их части
- Разработка программного обеспечения для решения задач теории вероятностей и математической статистики
- Разработка программного обеспечения для решения задач, построенных на алгоритмах случайного поиска

39. Управление требованиями:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

- Задача выявления изначальных проблем заказчика и создание системы, удовлетворяющей этим требованиям
- + Процесс систематического выявления, организации и документирования требований сложной системе
- Выявление требований заказчика и управление ими
- + Задача, состоящая в том, чтобы понимать проблемы заказчиков в их предметной области и на их языке и создавать системы, удовлетворяющие их потребности
- Процесс создания программного обеспечения и адаптация его под требования заказчика
- Разработка требований к программному обеспечению и создание ПО на основе этих требований
- + Процесс, в ходе которого вырабатывается и обеспечивается соглашение между заказчиком и выполняющей проект группой по поводу меняющихся требований к системе
- Разработка программного обеспечения и выработка требований к изменению работы системы заказчика

40. К методам выявления требований относятся:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

- Беседы с первыми руководителями предприятия, для которого разрабатывается программное обеспечение
- Анализ научной и технической литературы, посвященной вопросам разработки программного обеспечения
- Личные встречи и беседы со всеми сотрудниками предприятия
- Анализ технической документации и на основе нее разработка требований к системе
- На начальном этапе требования не выявляются, а формируются по мере разработки программного обеспечения
- + Интервьюирование и анкетирование, мозговой штурм и отбор идей
- + Совещания, посвященные требованиям, создание прототипов

- + Раскадровки, прецеденты, обыгрывание ролей Требования – это:
 - Документ, регулирующий отношения между заказчиком информационной системы и проектировщиком
- + Некоторое свойство программного обеспечения, необходимое пользователю для решения проблемы при достижении поставленной цели
 - Оформленное заказчиком в виде документа задание на проектирование программного обеспечения
- + Возможность, которую должна обеспечивать система
 - Характеристика проектируемого программного обеспечения с точки зрения разработчика
- + Некоторое свойство программного обеспечения, которым должна обладать система или ее компонент, чтобы удовлетворить требования формальной документации
 - Оформленное разработчиком в виде документа задание на проектирование программного обеспечения
 - Характеристика проектируемого программного обеспечения с точки зрения заказчика

41. Типичная схема процесса анализа С-требований включает в себя:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

- + Идентификацию заказчика и проведение интервью с представителями заказчика
 - Разработку программного обеспечения в соответствии с требованиями заказчика
 - Изложение заказчику требований к системе на основе разработанного программного обеспечения
- + Написание С-Требований в форме стандартного документа
 - Верификацию разработанного программного обеспечения в соответствии с требованиями заказчика
 - Составление плана мероприятий по анализу С-требований
- + Проверку С-Требований и согласование их с заказчиком
 - Адаптацию разработанного программного обеспечения в соответствии с требованиями заказчика

42. В классификацию требований к программной системе входят:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

- Требования заказчика
- Требования, накладываемые условиями эксплуатации
- + Функциональные требования
 - Требования, накладываемые аппаратными средствами
- + Нефункциональные требования
- + Требования предметной области
 - Экономические требования
 - Требования разработчиков

43. Процесс определения и анализа требований включает в себя:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

- Анализ работы систем с аналогичной предметной областью
- + Анализ предметной области, сбор и классификацию требований
- Проведение совместных совещаний с представителями заказчика
- + Разрешение противоречий и определение приоритетов
- Адаптацию требований к разрабатываемому программному обеспечению
- Декомпозицию общей задачи на подзадачи
- + Проверку, специфицирование и документирование требований
- Верификацию требований в соответствии с разработанным программным обеспечением

44. Опорные точки зрения конечных пользователей системы программного обеспечения можно трактовать как:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

- + Источник информации о системных данных
- Структуру требований
- Источник событий
- Структуру событий
- + Структуру представлений
- Получателей требований
- Источник сценариев
- + Получателей системных сервисов

45. При аттестации требований выполняются следующие типы проверок документации требований:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

- Проверка на совместимость
- Проверка на управляемость
- + Проверка правильности требований
- + Проверка на непротиворечивость
- Проверка на соответствие
- Проверка на обратимость
- + Проверка на полноту и на выполнимость
- Проверка на заменяемость

46. К методам аттестации требований относится:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

- Тестирование
- + Обзор требований
- Верификация
- Сравнительный анализ
- + Прототипирование
- Генерация случайных данных
- + Генерация тестовых сценариев
- Декомпозиция

47. Уровни организационного управления при планировании разработки системы:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

- + Стратегический
- + Тактический
- + Оперативный
- Основной
- Вспомогательный
- Дополнительный
- Системный
- Аналитический

48. Классификация бизнес-процессов включает следующие классы процессов:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

- Вспомогательные бизнес-процессы
- + Основные бизнес-процессы
- Дополнительные бизнес-процессы
- + Обеспечивающие бизнес-процессы
- Обслуживающие бизнес-процессы

- Бизнес-процессы согласования
- + Бизнес-процессы управления
- Руководящие бизнес-процессы

49. Типы D-требований:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

- + Функциональные требования
- Интерфейсные требования
- + Нефункциональные требования
- Программные требования
- + Обратные требования
- Ограниченные требования
- Производительные требования
- Надежность

50. Возможные способы организации D-требований:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

- По атрибутам, по компонентам
- По взаимоотношениям сущности
- По пакетам и по иерархии компонентов
- + По свойствам, по классам
- + По вариантам использования
- По узлам и по использованным процессам
- + По состояниям и по иерархии функции
- По прецедентам, по кооперациям

51. Принципы разработки эффективного пользовательского интерфейса:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

- Сложность, графика
- + Структура, простота
- Связь, обработка
- + Видимость, обратная связь
- Невидимость, сложность
- + Толерантность, повторное использование
- Первое использование, итерация
- Интеграция, повторение
-

52. Типы интерфейсных требований:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

- + Пользовательские требования
- + Аппаратные требования
- Административные требования
- Требования к производительности
- + Программные и коммуникационные требования

- Требования к надежности
- Требования к устойчивости
- Атрибуты программной системы и другие требования

53. Технология проектирования определяется как совокупность составляющих:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

- Поэтапная процедура
- + Пошаговая процедура
- Модели и правила
- + Критерий и правила
- Тестирование
- + Нотаций
- Прецеденты
- Классы

54. Разработка и сопровождение ИС в конкретной организации и конкретном проекте должна поддерживаться стандартами:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

- Стандарт организации
- Стандарт конкретного проекта
- + Стандарт проектирования
- Стандарт оценки
- + Стандарт оформления проектной документации
- Стандарт аудита
- Стандарт оформления разработки
- + Стандарт пользовательского интерфейса

55. Результатами проектирования архитектуры являются:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

- Модель административного интерфейса
- + Модель процессов
- Модель потоков
- Модель классов
- + Модель данных
- + Модель пользовательского интерфейса
- Модель компонентов
- Модель узлов

56. Какие работы включает процесс разработки программного обеспечения:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

- Документирование, управление конфигурацией
- Управление, создание инфраструктуры

- Структура из процессов, работ, задач
- Обеспечение качества, верификация
- + Анализ требований, проектирование
- + Программирование, сборка, тестирование
- + Ввод в действие, приемка
- Совместный анализ, аудит

57. Объектно-ориентированное проектирование использует инструментальные средства:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

- Model mart
- + Rational Rose
- Bpwin
- + ARIS
- Idef1X
- Erwin
- + MS Visio
- Jam

58. Проектирование функциональных моделей поддерживается инструментальными средствами:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

- Jam
- + Model Mart
- MS visio
- + ERwin
- Idef0
- Aris
- Rational rose
- + BPwin

59. IEEE – это:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

- Коммерческая организация ученых и исследователей
- Просто принятое обозначение, расшифровки не имеет
- Обозначение всемирной компьютерной сети
- + Всемирная некоммерческая техническая профессиональная ассоциация ученых и исследователей
- Такая аббревиатура нигде не используется
- + Institute Of Electrical and Electronic Engineers, Inc
- Американская организация ученых-экономистов
- + Институт инженеров радиоэлектроники и электротехники

60. Ядро знаний SWEBOOK – это:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

- ГОСТ на разработку программного обеспечения
- + Нормативный документ, разработанный IEEE
- ГОСТ на разработку информационных систем
- Документ, устанавливающий правовые отношения между заказчиком и разработчиком программного обеспечения
- + Основополагающий научно-технический документ, который отображает мнение специалистов в области программной инженерии
- Документ, устанавливающий методику тестирования и испытания программного обеспечения
- + Документ, который согласуется с современными регламентированными процессами жизненного цикла ПО стандарта ISO/IEC 12207
- ГОСТ на разработку и комплектацию сопровождающей документации

61. Каждая область ядра знаний SWEBOOK представляется:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 9

- Структурной схемой
- + Общей схемой описания
- Диаграммой UML
- Описанием и комментариями
- + Определением понятийного аппарата, методов и средств инженерной деятельности
- Определением языка программирования
- + Определением инструментов поддержки инженерной деятельности
- Иерархической диаграммой

62. К основным областям знаний SWEBOOK относятся:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

- + Инженерия требований, проектирование ПО
- Анализ деятельности системы
- Управление проектами
- + Конструирование ПО
- Управление персоналом
- + Тестирование ПО, сопровождение ПО
- Управление конфигурацией
- Инженерия качества программных средств

63. К организационным областям знаний SWEBOOK относятся:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

- Инженерия требований
- + Управление конфигурацией, управление проектами
- Конструирование ПО

+ Процесс инженерии программных средств, методы и средства программной инженерии

- Проектирование ПО
- Сопровождение ПО
- Тестирование ПО

+ Инженерия качества программных средств

64. В рамках Rational Unified Process (RUP) набор действий по разработке программ включает этапы:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

- Создание структурных схем
- Определения входных, выходных данных
- Согласование стоимости проекта
- Согласования требований с заказчиком
- Создания бизнес-моделей

+ Определение требований

+ Проектирование, программирование

+ Тестирование, внедрение

Критерии оценивания:

Отметка	Объем выполнения работы в %
«5» (отлично)	90 – 100
«4» (хорошо)	70 – 89
«3» (удовлетворительно)	50 – 69
«2» (неудовлетворительно)	менее 50

Тема 1.2 Загрузка и установка программного обеспечения

Форма контроля: тестирование

Время выполнения: 20 минут.

Задание: выполнить тест

1. Какие программы можно отнести к системному программному обеспечению:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

Варианты ответа:

- 1. операционные системы;**
2. прикладные программы;
3. игровые программы.

2. Какие программы можно отнести к системному ПО:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

Варианты ответа:

- 1. драйверы;**
2. текстовые редакторы;
3. электронные таблицы;
4. графические редакторы.

3. Специфические особенности ПО как продукта:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

- 1. продажа по ценам ниже себестоимости (лицензирование);**
2. низкие материальные затраты при создании программ;
3. возможность создание программ небольшие коллективом или даже одним человеком;
- 4. разнообразие решаемых задач с помощью программных средств.**

4. Какие программы можно отнести к системному ПО:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

Варианты ответа:

1. программа расчета заработной платы;
2. электронные таблицы;
3. **СУБД (системы управления базами данных).**

5. Какие программы нельзя отнести к системному ПО:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

Варианты ответа:

1. **игровые программы;**
2. компиляторы языков программирования;
3. операционные системы;
4. системы управления базами данных.

6. Какие программы можно отнести к прикладному программному обеспечению:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

Варианты ответа:

1. **электронные таблицы;**
2. таблицы решений;
3. **СУБД (системы управления базами данных).**

7. Какие программы можно отнести к прикладному ПО:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

Варианты ответа:

- 1) **программа расчета заработной платы;**
- 2) диспетчер программ;
- 3) программа «Проводник» (Explorer).

8. Какие программы нельзя отнести к прикладному ПО:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

Варианты ответа:

- 1) **компиляторы и (или) интерпретаторы;**
- 2) текстовые и (или) графические редакторы;
- 3) **электронные таблицы.**

9. Можно ли отнести операционную систему к программному обеспечению:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

Варианты ответа:

1. да;
2. нет.

10. Можно ли отнести операционную систему к прикладному программному обеспечению:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

Варианты ответа:

1. да;
2. нет.

11. Специфические особенности ПО как продукта:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

Варианты ответа:

1. низкие затраты при дублировании;
2. универсальность;
3. простота эксплуатации;
4. наличие поддержки (сопровождения) со стороны разработчика.

12. Какие программы можно отнести к системному ПО:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

Варианты ответа:

1. утилиты;
2. экономические программы;
3. статистические программы;
4. мультимедийные программы.

13. Для решения инженерных задач характерно применение:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

Варианты ответа:

1. САПР (систем автоматизированного проектирования);
2. СУБД (систем управления базами данных);
3. ОС (операционных систем).

14. Ошибки компоновки заключаются в том, что:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

Варианты ответа:

1. указано внешнее имя, но не объявлено;
2. неправильно использовано зарезервированное слово;
3. составлено неверное выражение;

4. указан неверный тип переменной.

15. Могут ли проявиться ошибки при изменении условий эксплуатации:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

Варианты ответа:

1. да;
2. нет.

16. Могут ли проявиться ошибки при изменении в предметной области:

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

Варианты ответа:

1. да;
2. нет.

Критерии оценивания:

Отметка	Объем выполнения работы в %
«5» (отлично)	90 – 100
«4» (хорошо)	70 – 89
«3» (удовлетворительно)	50 – 69
«2» (неудовлетворительно)	менее 50

Раздел 2 Обеспечение качества компьютерных систем в процессе эксплуатации

МДК. 03.02 Обеспечение качества функционирования компьютерных систем

Тема 2.1 Основные методы обеспечения качества функционирования

Форма контроля: выполнение письменной работы

Время: 40 минут

Задание: письменно ответить на вопросы

Варианты вопросов:

1. Как называется совокупность технических средств, необходимых для технической поддержки решения всех тех задач защиты информации, решение которых может потребоваться в процессе функционирования СЗИ?
2. Что включает в себя организационная защита
3. Какова конечная цель идентификации и установления подлинности объекта в вычислительной системе?
4. Как называется комплекс мероприятий, исключающих или уменьшающих возможность выхода конфиденциальной информации за пределы контролируемой зоны за счет акустических полей?
5. Что обозначает такой общеметодологический принцип, как концептуальное единство?
6. В чем заключается ограничение доступа?
7. 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?
8. Согласно каким методам шифрования информации, шифрование выполняется путем сложения символов исходного текста и ключа по модулю, равному числу букв в алфавите?
9. Как называется комплекс мероприятий, исключающих или ослабляющих возможность неконтролируемого выхода конфиденциальной информации за пределы контролируемой зоны за счет электромагнитных полей побочного характера и наводок?
10. Что такое система защиты информации?

Критерии оценивания:

Оценка 5 «отлично» теоретическое содержание курса освоено полностью, без пробелов, умения сформированы, все предусмотренные программой учебные задания выполнены, качество их выполнения оценено высоко.

Оценка 4 «хорошо» теоретическое содержание курса освоено полностью, без пробелов, некоторые умения сформированы недостаточно, все предусмотренные программой учебные задания выполнены, некоторые виды заданий выполнены с ошибками.

Оценка 3 «удовлетворительно» теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые умения работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий содержат ошибки.

Оценка 2 «неудовлетворительно» теоретическое содержание курса не освоено, необходимые умения не сформированы, выполненные учебные задания содержат грубые ошибки

Тема 2.2 Методы и средства защиты компьютерных систем

Форма контроля: тестирование

Время: 40 минут

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

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

Варианты ответа

2. **информационная война**
3. информационное оружие
4. информационное превосходство

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

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

1. служебная информация
2. коммерческая тайна
3. банковская тайна
4. **конфиденциальная информация**

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

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

1. **конфиденциальность**
2. целостность
3. доступность
4. аутентичность
5. апеллируемость

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

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

1. **надежность**
2. точность
3. контролируемость
4. устойчивость
5. доступность

6. В классификацию вирусов по способу заражения входят
Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

1. опасные
2. файловые
3. **резидентные**
4. загрузочные
5. файлово -загрузочные
6. **нерезидентные**

7. Комплекс превентивных мер по защите конфиденциальных данных и информационных процессов на предприятии это...

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

1. **комплексное обеспечение ИБ**
2. безопасность АС
3. угроза ИБ
4. атака на АС
5. политика безопасности

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

Проверяемые компетенции: ВД 4, ПК 4.1. ОК 1-ОК 09

1. компаньон - вирусами
2. **черви**
3. паразитические
4. студенческие
5. призраки
6. стелс - вирусы
7. 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
4. **все варианты верны**

10. Автоматизированная система должна обеспечивать

1. надежность
2. **доступность**
3. **целостность**
4. контролируемость

11. Основными компонентами парольной системы являются

1. **интерфейс администратора**
2. хранимая копия пароля
3. **база данных учетных записей**
4. 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
2. **пароль пользователя**
3. учетная запись пользователя
4. парольная система

13. К принципам информационной безопасности относятся

1. скрытость
2. масштабность
3. **системность**
4. **законность**
5. **открытости алгоритмов**

14. К вирусам изменяющим среду обитания относятся:

1. черви
2. студенческие
3. **полиморфные**
4. спутники

15. Охрана персональных данных, государственной служебной и других видов информации ограниченного доступа это...

1. **Защита информации**
2. Компьютерная безопасность
3. Защищенность информации
4. Безопасность данных

16. Система физической безопасности включает в себя следующие подсистемы:

1. **оценка обстановки**
2. скрытность
3. **строительные препятствия**
4. **аварийная и пожарная сигнализация**

17. Какие степени сложности устройства Вам известны

1. упрощенные
2. **простые**
3. **сложные**
4. оптические
5. встроенные

18. К механическим системам защиты относятся:

1. **проволока**
2. **стена**
3. сигнализация
4. **вы**

19. Какие компоненты входят в комплекс защиты охраняемых объектов:

1. **сигнализация**
2. **охрана**
3. **датчики**
4. **телевизионная система**

20. К выполняемой функции защиты относится:

1. внешняя защита
2. внутренняя защита
3. **все варианты верны**

21. Набор аппаратных и программных средств для обеспечения сохранности, доступности и конфиденциальности данных:

1. Защита информации
2. **Компьютерная безопасность**
3. Защищенность информации
4. Безопасность данных

22. Средства уничтожения, искажения или хищения информационных массивов, добы- вания из них необходимой информации после преодоления систем защиты, огра- ничения или воспреещения доступа к ним это:

1. информационная война
2. **информационное оружие**
3. информационное превосходство

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

1. государственная тайна
2. **коммерческая тайна**
3. банковская тайна
4. конфиденциальная информация

24. Гарантия того, что при хранении или передаче информации не было произведенонесанкционированных изменений:

1. конфиденциальность
2. **целостность**
3. доступность
4. аутентичность
5. аппелеруемость

25. Гарантия точного и полного выполнения команд в АС:

1. надежность
2. **точность**
3. контролируемость
4. устойчивость
5. доступность

26. Уровень защиты, при котором затраты, риск, размер возможного ущерба были быприемлемыми:

1. принцип системности
2. принцип комплексности
3. принцип непрерывности
4. **принцип разумной достаточности**
5. принцип гибкости системы

27. Совокупность норм, правил и практических рекомендаций, регламентирующих ра- боту 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
5. **политика безопасности**

28. Особенности информационного оружия являются:

1. системность
2. открытость
3. **универсальность**
4. **скрытность**

29. К функциям информационной безопасности относятся:

1. **совершенствование законодательства РФ в сфере обеспечения информацион-ной безопасности**
2. **выявление источников внутренних и внешних угроз**
3. **Страхование информационных ресурсов**
4. **защита государственных информационных ресурсов**
5. **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
5. **все варианты ответа верны**

31. К вирусам не изменяющим среду обитания относятся:

1. **черви**
2. студенческие
3. полиморфные
4. **спутники**

32. Хранение паролей может осуществляться

1. **в виде сверток**
2. **в открытом виде**
3. в закрытом виде
4. **в зашифрованном виде**
5. **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
3. **сканером**
4. доктора и фаги

34. Выбрать недостатки имеющиеся у антивирусной программы ревизор:

1. **неспособность поймать вирус в момент его появления в системе**
2. **небольшая скорость поиска вирусов**
3. **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
2. **вирусы изменяющие среду обитания при распространении**
3. **вирусы не изменяющие среду обитания при распространении**
4. вирусы не изменяющие среду обитания и не способные к распространению в дальнейшем

36. К достоинствам технических средств защиты относятся:

1. регулярный контроль
2. **создание комплексных систем защиты**
3. степень сложности устройства
4. Все варианты верны

37. К тщательно контролируемым зонам относятся:

1. **рабочее место администратора**
2. **архив**
3. **рабочее место пользователя**

38. К системам оповещения относятся:

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

39. Наиболее распространенные угрозы информационной безопасности:

1. угрозы целостности
2. угрозы защищенности
3. угрозы безопасности
4. угрозы доступности
5. угрозы конфиденциальности

40. Что относится к классу информационных ресурсов:

1. Документы
2. Персонал
3. Организационные единицы
4. Промышленные образцы, рецепты и технологии
5. Научный инструментарий

41. Гарантия того, что конкретная информация доступна только тому кругу лиц, для которого она предназначена:

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

42. К какому уровню доступа информации относится следующая информация: «Информация в области работ по хранению, перевозке, уничтожению химического оружия – сведения о состоянии здоровья граждан и объектов окружающей среды в районах размещения объектов по уничтожению химического оружия...»

1. Информация без ограничения права доступа
2. **Информация с ограниченным доступом**
3. Информация, распространение которой наносит вред интересам общества
4. Объект интеллектуальной собственности
5. Иная общедоступная информация

43. Соотнесите интересы в области информационной безопасности:

1. Национальные интересы
 2. Интересы личности
 3. Интересы государства
 4. Интересы общества
1. 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
2. обеспечиваются институтами государственной власти, осуществляющими свои функции, в том числе во взаимодействии с действующими на основе Конституции РФ и законодательства РФ общественными организациями
3. состоят в незыблемости конституционного строя, суверенитета и

территориальной целостности России, в политической, экономической и социальной стабильности, в безусловном обеспечении законности и поддержании правопорядка, в развитии равноправного и взаимовыгодного международного сотрудничества.

4. состоят в упрочении демократии, в создании правового, социального государства, в достижении и поддержании общенационального согласия, в духовном обновлении России.

ОТВЕТ: 1-2; 2-1; 3-3; 4-4.

44. Соотнесите основные методы получения паролей:

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

ОТВЕТ: 1-3; 2-1; 3-2; 4-4;

45. Соотнесите принципы информационной безопасности, определенные Гостехкомиссией

1. Принцип системности
 2. Принцип комплексности
 3. Принцип непрерывности защиты
 4. Гибкость системы защиты
 5. Разумная достаточность
1. правильно выбрать тот достаточный уровень защиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми
 2. непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла АС
 3. 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
 4. освобождает владельца АС от необходимости принятия кардинальных мер по полной замене средств защиты на новые.
 5. 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;

46. Соотнесите основные понятия в области информационной безопасности:

1. Атака
2. Уязвимость АС
3. Угроза безопасности АС
4. Защищенная система

1. некоторое неудачное свойство системы, которое делает возможным возникновение реализации угрозы
2. система со средствами защиты, которые успешно и эффективно противостоят угрозам безопасности
3. возможные воздействия на АС, которые прямо или косвенно могут нанести ущерб безопасности
4. действие, предпринимаемое злоумышленником, которое заключается в поиске и использовании той или иной уязвимости системы

ОТВЕТ: 1-4; 2-1; 3-3; 4-2;

46. Соотнесите функции, выполняемые техническими средствами защиты:

1. внешняя защита
2. опознавание
3. внутренняя защита

1. защита от воздействия дестабилизирующих факторов, проявляющихся непосредственно в средствах обработки информации
2. защита от воздействия дестабилизирующих факторов, проявляющихся за пределами основных средств АСОД
3. специфическая группа средств, предназначенных для опознавания людей по различным индивидуальным характеристикам

ОТВЕТ: 1-2; 2-3; 3-1

47. Соотнесите степени сложности устройств:

1. простые устройства
2. системы
3. сложные устройства

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

ОТВЕТ: 1-2; 2-3; 3-1;

48. Соотнесите основные виды угроз для АС:

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

ОТВЕТ: 1-3; 2-2; 3-1

49. 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
1. пассивные и активные
 2. направленные на использование прямого стандартного пути доступа к ресурсам и направленные на использование скрытого нестандартного доступа к ресурсам АС
 3. естественные или искусственные
 4. природная среда, человек, санкционированные программные средства и несанкционированные программные средства

ОТВЕТ: 1-3; 2-4; 3-3; 4-1

Критерии оценивания:

Отметка	Объем выполнения работы в %
«5» (отлично)	90 – 100
«4» (хорошо)	70 – 89
«3» (удовлетворительно)	50 – 69
«2» (неудовлетворительно)	менее 50

МЕЖСЕССИОННАЯ АТТЕСТАЦИЯ
Межсессионная аттестация
проводится в форме тестирования (7 семестр)
3. КОНТРОЛЬНО-ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ
ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

3.1 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.

2 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. +

3 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 функционирование ПК, несмотря на неправильные (ошибочные) входные данные;
- б) свойство, способно противостоять преднамеренным или непреднамеренным деструктивным действиям пользователя; +
- в) свойство, характеризующее способность ПС продолжать корректное функционирование, несмотря на неправильные (ошибочные) входные данные.

5 UML — это:

- а) язык программирования, имеющий синтаксис схож с C ;

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

6 При конструировании программного обеспечения процесс решения задачи составляет) 90 — 95%;

б) 50%;

в) 5 — 10%.

7 При конструировании программного обеспечения на этапе разработки или выбора алгоритма решения реализуется следующее:

а) архитектурное обработки программы;

в) алгебраическое программирования. +

7 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.

8 Интерфейс-это

а) прежде всего, набор правил;

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

9 Техническое задание — это

а) документ объяснений для заказчика;

б) исходный документ для сдачи ПО в эксплуатацию;

в) выходной документ для проектирования, разработки автоматизированной системы. +

10 Анализ требований —

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

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

в) отображение частей программ, которые будут модифицироваться. 17
Архитектура программной системы —

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

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

в) соответствующие вариации состава выделенных компонент.

11 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»). +

11 Ассоциация —

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

б) объединение нескольких понятий в новое понятие, 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. +

12 Валидация —

а) обеспечение соответствия разработки требованиям ее заказчиков. +

б) проверка правильности трансформации проекта в код реализации;

в) выявление всех ошибок.

12 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.

13 К процессу разработки ПО включает следующие процессы:

а) сопровождения;

б) проектирование; + в) эксплуатация.

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 системы 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 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 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: базопасность информации

Вопрос 38. Процесс определения риска, применения средств защиты для сокращения риска с последующим определением приемлемости остаточного риска, называется:

- Ответ: управлением риском

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

- Ответ: принцип минимизации привилегий

Вопрос 40. Проверка подлинности субъекта по предъявленному им идентификатору для принятия решения о предоставлении ему доступа к ресурсам системы — это:

- Ответ: аутентификация

Вопрос 41. Получение и анализ информации о состоянии ресурсов системы с помощью специальных средств контроля называется:

- Ответ: мониторингом

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

- 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 системы является:

- Ответ: числовая вероятностная оценка надежности

Вопрос 48. Присвоение субъектам и объектам доступа уникального номера, шифра, кода и т.п. с целью получения доступа к информации — это:

- Ответ: идентификация

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

- Ответ: электронной подписью

Вопрос 50. Обеспечением скрытности информации в информационных массивах занимается:

- Ответ: стеганография

Вопрос 51. Достоинством дискретных моделей политики безопасности является:

- Ответ: простой механизм реализации

Вопрос 52. Трояские программы — это:

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

Вопрос 53. Достоинствами аппаратной реализации криптографического закрытия данных являются:

- Ответ: высокая производительность и простота

Вопрос 54. Недостатком модели конечных состояний политики безопасности является:

- Ответ: сложность реализации

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

- Ответ: качеством информации

Вопрос 56. Гарантия сохранности данными правильных значений, которая обеспечивается запретом для неавторизованных пользователей каким-либо образом модифицировать, разрушать или создавать данные — это:

- Ответ: целостность

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

- Ответ: криптография

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

- Ответ: прикладном

Вопрос 59. "Уполномоченные серверы" фильтруют пакеты на уровне

- Ответ: приложений

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

- Ответ: алфавитом

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

• Ответ: гарантировать правильность реализации средств защиты

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

- Ответ: системный

Вопрос 63. Присвоение субъектам и объектам доступа уникального номера, шифра, кода и т.п. с целью получения доступа к информации — это:

- Ответ: идентификация

Вопрос 64. Недостатком матричных моделей безопасности является:

- Ответ: отсутствие контроля за потоками информации

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

- Ответ: мандатным

Вопрос 66. Политика информационной безопасности — это:

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

ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

1.1. Цели и задачи промежуточной аттестации

Главной задачей промежуточной аттестации обучающихся является установление соответствия результата освоения знаний и умений, сформированности общих и профессиональных компетенций требованиям Федерального государственного образовательного стандарта среднего профессионального образования по специальности 27.02.07 Управление качеством продукции, процессов и услуг (по отраслям).

1.2. Форма промежуточной аттестации

МДК. 03.01 Внедрение и поддержка компьютерных систем –

экзамен

МДК. 03.02 Обеспечение качества функционирования

компьютерных систем – экзамен

Экзамен по модулю

1.3 Система оценивания результатов выполнения заданий

Оценивание результатов выполнения заданий промежуточной аттестации осуществляется на основе следующих принципов:

достоверности оценки – оценивается уровень сформированности знаний, умений, практического опыта, общих и профессиональных компетенций, продемонстрированных обучающимися в ходе выполнения задания;

адекватности оценки – оценка выполнения заданий должна проводиться в отношении тех компетенций, которые необходимы для эффективного выполнения задания; надежности оценки – система оценивания выполнения заданий должна обладать высокой степенью устойчивости при неоднократных оценках уровня сформированности знаний, умений, практического опыта, общих и профессиональных компетенций обучающихся;

комплексности оценки – система оценивания выполнения заданий должна позволять интегративно оценивать общие и профессиональные компетенции обучающихся;

объективности оценки – оценка выполнения конкурсных заданий должна быть независимой от особенностей профессиональной ориентации или предпочтений преподавателей, осуществляющих контроль или аттестацию.

При выполнении процедур оценки заданий используются следующие основные методы:

метод расчета первичных баллов;

метод расчета сводных баллов.

Результаты выполнения заданий оцениваются в соответствии с разработанными критериями оценки. Используется пятибалльная шкала для оценивания результатов обучения.

Перевод пятибалльной шкалы учета результатов в пятибалльную оценочную шкалу:

Оценка	Количество баллов, набранных за выполнение теоретического и практического задания, средний балл по итогам аттестации
Оценка 5 «отлично»	4,6-5
Оценка 4 «хорошо»	3,6-4,5
Оценка 3 «удовлетворительно»	3-3,5
Оценка 2 «неудовлетворительно»	≤ 2,9

1.4 Материально-техническое обеспечение для проведения промежуточной аттестации

Аттестация проводится в кабинете Кабинет информатики, информационных технологий в профессиональной деятельности и Лаборатория информатики и информационных технологий в профессиональной деятельности

1.5 КОС МДК. 03.01 Внедрение и поддержка компьютерных систем

Условия выполнения задания:

- 1) теоретическое задание выполняется на бумажном носителе;
- 2) время, отводимое на выполнение задания – 2 часа;
- 3) максимальный балл за задание- 5 баллов.

Типовые задания

Виды теоретических вопросов:

1. Анализ приложений с проблемами совместимости. Использование динамически загружаемых библиотек. Механизм решения проблем совместимости на основе «системных заплаток». Разработка модулей обеспечения совместимости
 2. Аппаратно-программные платформы серверов и рабочих станций.
 3. Виды внедрения, план внедрения. Стратегии, цели и сценарии внедрения.
 4. Виды клиентского программного обеспечения. Установка, адаптация и сопровождение клиентского программного обеспечения.
 5. Выполнение чистой загрузки. Выявление причин возникновения проблем совместимости ПО. Выбор методов выявления совместимости.
 6. ГОСТ Р ИСО/МЭК 12207. Основные процессы и взаимосвязь между документами в информационной системе согласно стандартам
 7. Изменение настроек по умолчанию в образе. Подключение к сетевому ресурсу. Настройка обновлений программ. Обновление драйверов.
 8. Настройка управления питанием. Оптимизация использования процессора.
 9. Оптимизация использования памяти. Оптимизация использования жесткого диска. Оптимизация использования сети. Инструменты повышения производительности программного обеспечения.
 10. Организация процесса обновления в информационной системе.
- #### Регламенты обновления
11. Особенности эксплуатации различных видов серверного программного обеспечения.
 12. Оценка качества функционирования информационной системы.
- #### CAKS- технологии

13. Понятие совместимости программного обеспечения. Аппаратная и программная совместимость. Совместимость драйверов.
14. Причины возникновения проблем совместимости. Методы выявления проблем совместимости ПО.
15. Проблемы перехода на новые версии программ. Мастер совместимости программ. Инструментарий учета аппаратных компонентов.
16. Производительность ПК. Проблемы производительности. Анализ журналов событий.
17. Решение проблем конфигурации с помощью групповых политик.
18. Создание в системе виртуальной машины для исполнения приложений.
19. Средства диагностики оборудования. Разрешение проблем аппаратного сбоя
20. Тестирование на совместимость в безопасном режиме. Восстановление системы.
21. Тестирование программного обеспечения в процессе внедрения и эксплуатации
22. Типовые функции инструментария для автоматизации процесса внедрения информационной системы
23. Установка серверной части. Виды серверного программного обеспечения.
24. Функции менеджера сопровождения и менеджера развертывания
25. Эксплуатационная документация

Виды практических заданий:

1. «Выявление и документирование проблем установки программного обеспечения»
2. «Измерение и анализ эксплуатационных характеристик качества программного обеспечения».
3. «Конфигурирование программных и аппаратных средств»
4. «Настройка сетевого доступа»
5. «Настройки системы и обновлений»
6. «Разработка (подготовка) документации и отчетных форм для внедрения программных средств»
7. «Разработка модулей программного средства»
8. «Разработка руководства оператора»

9. «Разработка сценария внедрения программного продукта для рабочего места»
10. «Создание образа системы. Восстановление системы»
11. «Устранение проблем совместимости программного обеспечения»

1.6 КОС МДК. 03.02 Обеспечение качества функционирования компьютерных систем

Условия выполнения задания:

- 1) Теоретическое задание выполняется на бумажном носителе;
- 2) время, отводимое на выполнение задания – 2 часа;
- 3) максимальный балл за задание- 5 баллов.

Типовые задания

Виды теоретических вопросов:

1. Анализ рисков и характеристик качества программного обеспечения при внедрении.
2. Антивирусные программы: классификация, сравнительный анализ
3. Вредоносные программы: классификация, методы обнаружения
4. Групповые политики. Аутентификация. Учетные записи
5. Дестабилизирующие факторы и угрозы надежности
6. Математические модели описания статистических характеристик ошибок в программах
7. Методы предотвращения угроз надежности
8. Многоуровневая модель качества программного обеспечения
9. Объекты уязвимости
10. Оперативные методы повышения надежности: временная, информационная, программная избыточность
11. Первичные ошибки, вторичные ошибки и их проявления
12. Средства и протоколы шифрования сообщений
13. Тестирование защиты программного обеспечения
14. Файрвол: задачи, сравнительный анализ, настройка
15. Целесообразность разработки модулей адаптации

Виды практических заданий:

1. «Анализ рисков»

2. «Выявление первичных и вторичных ошибок»
3. «Настройка браузера»
4. «Настройка политики безопасности»
5. «Обнаружение вируса и устранение последствий его влияния»
6. «Работа с программой восстановления файлов и очистки дисков»
7. «Работа с реестром»
8. «Сравнение результатов тестирования с требованиями технического задания и/или спецификацией».
9. «Тестирование программных продуктов»
10. «Установка и настройка антивируса. Настройка обновлений с помощью зеркал

1.7 КОС Экзамен по модулю

Условия выполнения задания:

- 1) Теоретическое задание выполняется на бумажном носителе;
- 2) время, отводимое на выполнение задания – 2 часа;
- 3) максимальный балл за задание- 5 баллов.

Задание:

Ответить на два вопроса

Выполнить практическое задание

Вопросы к экзамену по модулю

1. Какие виды угроз для ПК в сети вы знаете?
2. Какие меры для защиты ПК вы знаете?
3. Что такое вирус?
4. Что такое и какие виды хакерских атак вы знаете?
5. Основные понятия защиты информации.
6. Способы обеспечения ИБ сетей
7. Аппаратные и программные средства резервного копирования данных.
8. Классификация программ резервного копирования.
9. Краткий обзор наиболее популярных программ резервного копирования.
10. Сравнение программ резервного копирования.
11. Стратегия предотвращения несанкционированного доступа в информационную систему (ИС).
12. Модели безопасности по разграничению доступа в систему.

13. Модели контроля целостности информации в системе.
14. Модели защиты при отказе в обслуживании.
15. Модели анализа безопасности ПО.
16. Модель безопасности объектов ВС.
17. Понятия политики безопасности.
18. Обеспечение ИБ в нормальных ситуациях.
19. Обеспечение ИБ в чрезвычайных ситуациях.
20. Классификация компьютерных вирусов.
21. Жизненный цикл вирусов.
22. Классические способы распространения Электронная почта.
23. Троянские Web-сайты
24. Методы обнаружения вирусов.
25. Антивирусные программы.
26. Антивирусные комплексы.
27. Встраивание антивирусов в BIOS компьютеров.
28. Виды антивирусных программ.
29. Профилактические меры защиты.
30. Построение системы антивирусной защиты корпоративной сети.
31. Состав мероприятий по защите персональных данных.
32. Основные мероприятия обеспечения безопасности персональных данных.
33. Мероприятия по техническому обеспечению безопасности персональных данных
34. Приведите примеры и опишите аппаратные средства резервного копирования данных.
35. Классификация программ резервного копирования.
36. Опишите наиболее популярные программы резервного копирования.
37. проведите сравнение программ.
38. Приведите примеры и опишите программные средства резервного копирования данных.
39. Классификация программ резервного копирования
40. Опишите наиболее популярные программы резервного копирования. проведите сравнение программ.
41. ГОСТ Р ИСО/МЭК 12207.
42. Основные процессы и взаимосвязь между документами в информационной системе согласно стандартам
43. Виды внедрения, план внедрения.
44. Стратегии, цели и сценарии внедрения.
45. Функции менеджера сопровождения и менеджера развертывания

46. Типовые функции инструментария для автоматизации процесса внедрения информационной системы
47. Оценка качества функционирования информационной системы.
48. CALS-технологии
49. Организация процесса обновления в информационной системе.
50. Регламенты обновления
51. Тестирование программного обеспечения в процессе внедрения и эксплуатации.
52. Эксплуатационная документация
53. Понятие совместимости программного обеспечения.
54. Аппаратная и программная совместимость.
55. Совместимость драйверов.
56. Причины возникновения проблем совместимости.
57. Методы выявления проблем совместимости ПО.
58. Выполнение чистой загрузки.
59. Выявление причин возникновения проблем совместимости ПО.
60. Выбор методов выявления совместимости.
61. Проблемы перехода на новые версии программ.
62. Мастер совместимости программ.
63. Инструментарий учета аппаратных компонентов.
64. Анализ приложений с проблемами совместимости.
65. Использование динамически загружаемых библиотек.
66. Механизм решения проблем совместимости на основе «системных заплаток».
67. Разработка модулей обеспечения совместимости
68. Создание в системе виртуальной машины для исполнения приложений.
69. Изменение настроек по умолчанию в образе.
70. Подключение к сетевому ресурсу.
71. Настройка обновлений программ.
72. Обновление драйверов.
73. Решение проблем конфигурации с помощью групповых политик.
74. Тестирование на совместимость в безопасном режиме.
75. Восстановление системы.
76. Производительность ПК.
77. Проблемы производительности.
78. Анализ журналов событий.
79. Настройка управления питанием.
80. Оптимизация использования процессора.
81. Оптимизация использования памяти.
82. Оптимизация использования жесткого диска.

83. Оптимизация использования сети.
84. Инструменты повышения производительности программного обеспечения.
85. Средства диагностики оборудования.
86. Разрешение проблем аппаратного сбоя
87. Аппаратно-программные платформы серверов и рабочих станций.
88. Установка серверной части.
89. Виды серверного программного обеспечения.
90. Особенности эксплуатации различных видов серверного программного обеспечения.
91. Виды клиентского программного обеспечения.
92. Установка, адаптация и сопровождение клиентского программного обеспечения.
93. Многоуровневая модель качества программного обеспечения
94. Объекты уязвимости
95. Дестабилизирующие факторы и угрозы надежности
96. Методы предотвращения угроз надежности
97. Оперативные методы повышения надежности: временная, информационная, программная избыточность
98. Первичные ошибки, вторичные ошибки и их проявления
99. Математические модели описания статистических характеристик ошибок в программах
100. Анализ рисков и характеристик качества программного обеспечения при внедрении.
101. Целесообразность разработки модулей адаптации
102. Вредоносные программы: классификация, методы обнаружения
103. Антивирусные программы: классификация, сравнительный анализ
104. Файрвол: задачи, сравнительный анализ, настройка
105. Групповые политики. Аутентификация. Учетные записи
106. Тестирование защиты программного обеспечения
107. Средства и протоколы шифрования сообщений.

Практическое задание

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. Проведите очистку системного реестра.

1.8 Критерии оценки:

Критерии оценки результатов выполнения теоретического задания		Баллы в соответствии с критериями оценки
		Максимальный балл -
1	Демонстрирует глубокое, полное знание и понимание программного материала. Последовательно, самостоятельно раскрывает основное содержание вопроса. Выводы аргументированы, основаны на самостоятельно выполненном анализе, обобщении данных.	2,0
2	Демонстрирует недостаточно глубокое, полное знание и понимание программного материала. Недостаточно последовательно, но самостоятельно раскрывает основное содержание вопроса. Выводы основаны на самостоятельно выполненном анализе, обобщении данных, но в отдельных случаях недостаточно аргументированы. Недостаточно четко и верно даны определения понятий и научных терминов.	1,6
3	Демонстрирует в отдельных вопросах, неглубокое владение знаниями программного материала. Излагает программный материал фрагментарно, не всегда последовательно. Допущены ошибки и неточности в использовании научной терминологии.	1,3
4	Студент демонстрирует незнание и непонимание программного материала. Основное содержание учебного материала не раскрыто; допущены грубые ошибки в определении понятий, при использовании терминологии. Затрудняется отвечать на вопросы, при ответе	0
Итого		2

Критерии оценки практического задания

Задание	Показатель оценки результата
Назначение программы определено правильно	макс. – 0,5 балла.
Устранение проблемы выполнено правильно	макс. – 0,5 балла.
Пример создан - программа функционирует	макс. – 0,5 балла.
Правильно описаны сценария тестирования	макс. – 0,5 балла.
Настройки определены правильно	макс. – 0,5 балла.
Обновление произведено правильно	макс. – 0,5 балла.
Всего баллов:	

Результаты выполнения заданий оцениваются в соответствии с разработанными критериями оценки. Используется пятибалльная шкала для оценивания результатов обучения.

Перевод пятибалльной шкалы учета результатов в пятибалльную оценочную шкалу:

Оценка	Количество баллов, набранных за выполнение теоретического и практического задания, средний балл по итогам аттестации
Оценка 5 «отлично»	4,6-5
Оценка 4 «хорошо»	3,6-4,5
Оценка 3 «удовлетворительно»	3-3,5
Оценка 2 «неудовлетворительно»	≤ 2,9