


Федеральное государственное образовательное бюджетное учреждение  
высшего образования  
«Финансовый университет при Правительстве Российской Федерации»  
(Финансовый университет)

**Красноярский филиал Финуниверситета**

---

(наименование структурного подразделения)

УТВЕРЖДАЮ  
Заместитель директора по  
учебно-методической работе  
Красноярского филиала  
Финуниверситета  
 О.С. Вергейчик  
« 04 » сентября 2025 г.

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ**

по профессиональному модулю

ПМ 04 Сопровождение и обслуживание программного обеспечения  
компьютерных систем

---

(код, наименование)

09.02.07 Информационные системы и программирование

---

(код, наименование специальности)

Красноярск – 2025 г.

Фонд оценочных средств по профессиональному модулю разработан на основании федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.07 «Информационные системы и программирование»

Составители:

Цирулькевич Алена Викторовна, преподаватель

(фамилия, имя, отчество, наименование должности, квалификационной категории)

Фонд оценочных средств по профессиональному модулю рассмотрен и рекомендован к утверждению на заседании предметной (цикловой) комиссии  
общепрофессиональных дисциплин

(наименование)

Протокол от «04» сентября 2025 г. № 1

Председатель предметной (цикловой)  
комиссии

  
\_\_\_\_\_  
(подпись)

О.А. Полтавец  
(инициалы, фамилия)

1. Паспорт фонда оценочных средств  
по профессиональному модулю «ПМ 04 Сопровождение и  
обслуживание программного обеспечения компьютерных систем»  
(код, наименование)

**09.02.07 Информационные системы и программирование**

(код, наименование специальности)

Результаты обучения (знания, умения)	Общие и профессиональные компетенции	Наименование элементов профессионального модуля, раздела, темы	Наименование оценочного средства	
			Текущий контроль	Промежуточная аттестация
<p>Знать:</p> <ul style="list-style-type: none"> <li>– основные методы и средства анализа функционирования ПО;</li> <li>– виды работ на этапе сопровождения ПО;</li> <li>– принципы контроля конфигурации и поддержки целостности конфигурации ПО;</li> <li>– средства защиты ПО в компьютерных системах.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– подбирать и настраивать конфигурацию ПО;</li> <li>– использовать методы защиты ПО;</li> <li>– проводить инсталляцию ПО;</li> <li>– производить настройку компонентов ПО;</li> </ul>	<p>Профессиональные компетенции: ПК 4.1 – ПК 4.4</p> <p>Общие компетенции: ОК 01 – ОК 09</p>	<p>МДК 04.01</p> <ul style="list-style-type: none"> <li>– Тема 1.1 «Основные методы внедрения и анализа функционирования ПО»</li> <li>– Тема 1.2 «Загрузка и установка программного обеспечения»</li> </ul> <p>МДК 04.02</p> <ul style="list-style-type: none"> <li>– Тема 2.1 «Основные методы обеспечения качества функционирования»</li> <li>– Тема 2.2 «Методы и средства защиты компьютерных систем»</li> </ul> <p>Учебная практика Производственная практика</p>	<ul style="list-style-type: none"> <li>– Защита практических и лабораторных работ</li> <li>– Выполнение индивидуальных заданий</li> <li>– Тестирование</li> <li>– Экспертное наблюдение за выполнением заданий</li> <li>– Оформление отчетов по практике</li> </ul>	<p>Дифференцированный зачёт по МДК 04.02</p> <p>Экзамен по МДК 04.01</p> <p>Квалификационный экзамен по ПМ.04</p>

–анализировать риски и характеристики качества ПО.				

## 2. Формы промежуточной аттестации по профессиональному модулю

Элементы профессионального модуля	Формы промежуточной аттестации				
МДК 04.01 «Внедрение и поддержка программного обеспечения компьютерных систем»	Экзамен				
МДК 04.02 «Обеспечение качества функционирования компьютерных систем»	Дифференцированный зачёт				
Учебная практика	Дифференцированный зачёт				
Производственная практика (по профилю специальности)	Дифференцированный зачёт				
ПМ	Экзамен по модулю (квалификационный экзамен)				

## 3. Комплект оценочных средств

### 1. Задание для текущего контроля успеваемости

Практическая работа №1 «Разработка сценария внедрения программного продукта для рабочего места»

Цель:

– Научиться планировать процесс внедрения ПО с учётом требований ГОСТ Р ИСО/МЭК 12207.

Задачи:

- Определить этапы внедрения.
- Учесть роли участников (менеджер сопровождения, администратор, пользователь).
- Составить план действий.

Инструкция:

- Выберите программный продукт (например, LibreOffice, 1С:Бухгалтерия, Kaspersky Endpoint Security).
- Опишите целевую аудиторию (один пользователь / группа / организация).

Разработайте поэтапный сценарий:

1. Подготовка (анализ требований, совместимости, резервное копирование).
2. Установка (локальная или сетевая).
3. Тестирование (функциональность, производительность).
4. Обучение пользователей.
5. Передача в эксплуатацию.
6. Укажите используемые средства автоматизации (например, MSI-пакеты, групповые политики).

Отчёт должен содержать:

- Титульный лист.
- Введение (цель, актуальность).
- Сценарий внедрения (в виде таблицы или блок-схемы).
- Заключение.

Критерии оценки:

«Отлично» — все этапы учтены, обоснован выбор методов, соблюдены стандарты.

«Хорошо» — пропущен один второстепенный этап.

«Удовлетворительно» — есть основные этапы, но без детализации.

Практическая работа №2 «Разработка руководства оператора»

Цель:

- Создать понятную документацию для конечного пользователя без IT-образования.

Инструкция:

1. Используйте выбранный ПО из ПР №1.
2. Включите следующие разделы:
3. Назначение программы.
4. Минимальные системные требования.
5. Пошаговая инструкция запуска.
6. Основные функции (с пояснениями и скриншотами).
7. Типовые ошибки и способы их устранения.
8. Контакты службы поддержки.

Критерии оценки:

«Отлично» — полное, логичное, с примерами и скриншотами.

«Хорошо» — есть все разделы, но недостаточно иллюстраций.

«Удовлетворительно» — отсутствуют разделы по устранению ошибок или требованиям.

Практическая работа №3 «Разработка документации и отчётных форм для внедрения ПО»

Цель:

- Подготовить комплект служебной документации, используемой при внедрении.

Инструкция:

– Создайте три документа:

1. Отчёт об установке — дата, версия ПО, оборудование, выявленные проблемы.
2. Журнал изменений — фиксация всех обновлений и модификаций.
3. Форма заявки на техническую поддержку — поля: ФИО, отдел, описание проблемы, приоритет.

Формат: Word или PDF. Используйте шаблоны CALS-технологий (таблицы с рамками, нумерация).

Критерии оценки: наличие всех трёх документов, соответствие формату, читаемость.

Лабораторные работы по теме 1.2 «Загрузка и установка программного обеспечения»

Общие требования ко всем лабораторным работам:

Выполняются в изолированной виртуальной среде (VMware/VirtualBox).

Отчёт оформляется по шаблону: цель, ход работы, результаты, выводы.

Все действия фиксируются скриншотами.

Лабораторная работа №1 «Измерение и анализ эксплуатационных характеристик качества ПО»

Цель: Оценить производительность, стабильность и время отклика ПО.

Инструменты: Windows Performance Monitor, Task Manager, PassMark.

Инструкция:

- Установите тестовое ПО (например, VLC Media Player).
- Запустите мониторинг CPU, RAM, диска до и во время работы программы.
- Зафиксируйте:
- Время запуска.
- Пиковое потребление ресурсов.
- Наличие утечек памяти.
- Сравните с рекомендованными требованиями.

Вывод: Соответствует ли ПО заявленным характеристикам?

Лабораторная работа №2 «Выявление и документирование проблем установки ПО»

Инструкция:

– Попробуйте установить ПО на «чистую» ОС (Windows 10 без обновлений).

Зафиксируйте:

- Ошибки установщика.
- Отсутствующие зависимости (.NET Framework, Visual C++ Redistributable).
- Конфликты с антивирусом.

Составьте отчёт с рекомендациями (например: «обновить ОС до версии 22H2»).

### Лабораторная работа №3 «Устранение проблем совместимости ПО»

Инструкция:

- Возьмите устаревшее ПО (например, игру 2005 г.).
- Попробуйте запустить на Windows 11.

Примените:

- Режим совместимости (ПКМ → Свойства → Совместимость).
- «Мастер совместимости программ».
- Виртуальную машину с Windows XP/7.
- Зафиксируйте, какой метод сработал.

### Лабораторная работа №4–8

(Аналогично — кратко по инструкции)

№4 «Конфигурирование ПО и аппаратных средств»: Настройка BIOS (Secure Boot, TPM), драйверов (через Device Manager).

№5 «Настройка системы и обновлений»: Отключение/включение автообновлений, настройка WSUS-зеркала.

№6 «Создание образа системы»: Использовать Macrium Reflect Free → создать полный образ → проверить восстановление.

№7 «Разработка модулей ПО»: Написать PowerShell-скрипт, который делает резервную копию папки раз в день.

№8 «Настройка сетевого доступа»: Создать общую папку → назначить права → подключиться с другого ПК.

### МДК 04.02 «Обеспечение качества функционирования компьютерных систем»

#### Лабораторная работа №9 «Тестирование программных продуктов»

Инструкция:

- Выберите ПО с известным ТЗ (например, учебный калькулятор).

Составьте 5 тест-кейсов:

1. Ввод корректных данных.
2. Ввод некорректных данных.
3. Граничные значения.
4. Обработка исключений.
5. Выполните тестирование → зафиксируйте результаты в таблице (Ожидаемый / Фактический результат).

#### Лабораторная работа №10 «Сравнение результатов тестирования с ТЗ»

Сопоставьте фактические результаты с требованиями.

Если расхождения — составьте баг-репорт (описание, шаги воспроизведения, скриншот).

Лабораторная работа №11 «Анализ рисков»  
Проведите SWOT-анализ для выбранного ПО.  
Оцените:  
Вероятность сбоя.  
Последствия (потеря данных, простои).  
Возможные меры снижения риска.

Лабораторная работа №12 «Выявление первичных и вторичных ошибок»

Пример: ошибка в коде → сбой службы → повреждение БД.  
Постройте диаграмму «причина → следствие».

Лабораторные работы №13–18 (защита ПО)

№13: Заразите виртуальную машину EICAR-тестовым файлом → просканируйте → удалите.

№14: Установите Dr.Web → настройте локальное зеркало обновлений через HTTP-сервер.

№15: Через gpedit.msc запретите запуск .exe из %AppData%.

№16: В Chrome/Firefox отключите JavaScript, очистите кэш, включите DoH.

№17: Через regedit измените параметр автозагрузки → создайте резервную копию ветки.

№18: Удалите файл → восстановите через Recuva → очистите диск через CCleaner.

2. Вопросы и задание для промежуточной аттестации

Вопросы к экзамену по МДК 04.01:

- 1) Стандарты в области информационных систем
- 2) Первичные, вторичные ошибки и их проявления
- 3) Международный стандарт ISO/IEC 12207: 1995-08-01. 5 основных процессов ЖЦ ПО.
- 4) Методы предотвращения угроз надежности
- 5) Стандарты комплекса ГОСТ 34. Особенности стандарта
- 6) Методы тестирования ПО. Различные типы тестов
- 7) Настройка сетевого доступа к дискам (папкам) в системе Windows
- 8) Внедрение системы. Стратегии внедрения. Цели внедрения информационной системы.
- 9) Этапы процесса внедрения информационной системы.
- 10) Разработка модулей программного средства
- 11) Сценарии внедрения
- 12) Создание образа системы. Восстановление системы
- 13) Ошибки планирования внедрения систем для управления проектами
- 14) Настройка системы обновлений операционной системы Windows



15) Методология внедрения ИС. Бизнес-моделирование. Пилотное тестирование

16) Конфигурирование программных и аппаратных средств. Последовательность действий при управлении конфигурацией всех стадиях жизненного цикла ПО.

17) Типовые функции инструментария для автоматизации процесса внедрения информационной системы. CASE-технологии. CASE-средства.

18) Устранение проблем совместимости программного обеспечения. Программное обеспечение. Совместимость. Виды совместимости.

19) Оценка качества функционирования информационной системы. Дефектологические свойства.

20) Выявление и документирование проблем установки программного обеспечения.

21) Характеристики качества. Показатели качества. Критерии показателей качества.

22) Функциональная пригодность программного средства. Оценка корректности, способности к взаимодействию, защищенности, надежности, практичности, мобильности программных средств.

23) Метрики. Типы метрик.

24) Качество программного обеспечения. Схема процессов оценки характеристик качества программ.

25) Модель классификации критериев качества информационных систем

26) Измерение и анализ эксплуатационных характеристик качества программного обеспечения

27) Стратегия CALS в создании единого информационного пространства. Методы CALS.

28) Регламент внедрения программного продукта. Состав Регламента внедрения программного продукта

29) Организация процесса обновления в информационной системе. Обновление. Типы обновлений.

30) Что включает в себя технологическая, проектная, пользовательская документация, документация тестирования, испытаний и сопровождения?

31) Этапы простого обновления и миграции.

32) Документирование пакета прикладных программ. Классификация документации пакета прикладных программ.

33) Тестирование программного обеспечения в процессе внедрения и эксплуатации. Согласование изменений в процессе внедрения информационной системы.

34) Комплекты документации, входящие в состав программного средства. Состав этих комплектов

35) Этапы внедрения информационной системы. Доработка информационной системы по итогам опытной эксплуатации. Передача информационной системы в промышленную эксплуатацию.

36) Документация и отчетные формы внедрения программных средств. Группы и типы документации.

37) Типы и состав технической документации на программный продукт согласно ЕСПД.

38) Что должно содержать Руководство оператора? Для чего разрабатывается руководство оператора? Почему руководство оператора входит в состав комплекта эксплуатационной документации на программное обеспечение

39) Эксплуатационная документация на программный продукт

40) Внедрение программного обеспечения. Цели внедрения программного продукта. Коллективная разработка. Модели разбиения коллектива на рабочие группы

41) Совместимость программного обеспечения. Поддержка рабочей среды (совместимость приложений)

42) Безопасность компьютерной системы. Три составляющие безопасности. Обязательные и не обязательные категории модели безопасности.

43) Виртуализация ОС и её применение. Преимущества виртуализации.

44) Решение проблем конфигурации с помощью групповых политик. Компоненты GPO. Оснастка Управление групповыми политиками

45) Архивация системных данных и программ. Классификация типов резервного копирования.

46) Особенности эксплуатации различных видов серверного программного обеспечения.

47) Производительность ПК. Проблемы производительности. признаками медленной работы компьютера. Десять методов улучшения работы ПК

48) Средства диагностики оборудования. Разрешение проблем аппаратного сбоя

49) Функции менеджера сопровождения и менеджера развертывания

50) Процесс оптимизации работы ПК

51) Модели внедрения ПО

52) Развертывание ПО

1. Какой из перечисленных факторов НЕ относится к дестабилизирующим при эксплуатации ПО?

a) Сбои питания

b) Обновление операционной системы

c) Корректная установка драйверов

d) Вредоносное ПО

2. Что такое первичная ошибка в программном обеспечении?

a) Ошибка, вызванная пользователем

b) Исходный дефект в коде или логике программы

- c) Следствие сбоя оборудования
  - d) Ошибка, возникшая после обновления
3. Какой метод повышения надёжности ПО предполагает дублирование критических компонентов?
- a) Информационная избыточность
  - b) Программная избыточность
  - c) Временная избыточность
  - d) Аппаратная резервация
4. Какая модель качества ПО определяет иерархию характеристик и подхарактеристик?
- a) CMMI
  - b) ISO/IEC 25010
  - c) COBIT
  - d) ITIL
5. Какой из перечисленных инструментов используется для анализа журналов событий Windows?
- a) Regedit
  - b) Event Viewer
  - c) Task Manager
  - d) PerfMon
6. Что такое вторичная ошибка?
- a) Ошибка, исправленная разработчиком
  - b) Последствие первичной ошибки
  - c) Опечатка в документации
  - d) Ошибка в требованиях заказчика
7. Какой из перечисленных типов вредоносных программ шифрует файлы пользователя и требует выкуп?
- a) Троян
  - b) Червь
  - c) Рекламное ПО (adware)
  - d) Вымогатель (ransomware)
8. Какой протокол обеспечивает защищённую передачу данных в браузере?
- a) HTTP
  - b) FTP
  - c) HTTPS
  - d) SMTP
9. Что позволяет настроить «Локальная политика безопасности» в Windows?
- a) Автоматическое обновление драйверов
  - b) Правила блокировки USB-устройств
  - c) Установку антивируса
  - d) Создание резервных копий
10. Какой из перечисленных методов НЕ относится к защите от вредоносного ПО?

- a) Регулярное обновление ОС
- b) Отключение брандмауэра
- c) Использование антивируса
- d) Ограничение прав пользователей

11. Какой компонент Windows отвечает за централизованное управление политиками безопасности в домене?

- a) BIOS
- b) PowerShell
- c) Групповые политики (GPO)
- d) Диспетчер задач

12. Какой из перечисленных инструментов НЕ предназначен для восстановления удалённых файлов?

- a) Recuva
- b) CCleaner
- c) PhotoRec
- d) TestDisk

13. Что такое CALS-технологии?

- a) Средства автоматизации тестирования
- b) Стандарты создания и управления технической документацией
- c) Методы шифрования данных
- d) Протоколы сетевой безопасности

14. Какой из перечисленных подходов используется при анализе рисков внедрения ПО?

- a) SWOT-анализ
- b) Метод «мозгового штурма»
- c) FMEA (анализ видов отказов)
- d) Все перечисленные

15. Какой параметр НЕ входит в эксплуатационные характеристики ПО?

- a) Время отклика
- b) Цвет интерфейса
- c) Стабильность работы
- d) Потребление оперативной памяти

16. Какой из перечисленных элементов реестра Windows хранит настройки текущего пользователя?

- a) HKEY\_LOCAL\_MACHINE
- b) HKEY\_CURRENT\_USER
- c) HKEY\_CLASSES\_ROOT
- d) HKEY\_USERS

17. Что происходит при «чистой загрузке» Windows?

- a) Загружается только ядро ОС без сторонних служб и автозагрузки
- b) Удаляются все пользовательские файлы
- c) Выполняется полное форматирование диска
- d) Обновляется BIOS

18. Какой из перечисленных методов защиты ПО относится к «превентивным»?

- a) Восстановление из резервной копии
- b) Установка файрвола
- c) Анализ логов после атаки
- d) Удаление вируса

19. Какой из перечисленных документов регламентирует жизненный цикл ПО?

- a) ГОСТ Р ИСО/МЭК 12207
- b) ГОСТ 19.101–77
- c) ФЗ-152
- d) RFC 791

20. Какой из перечисленных факторов может вызвать проблему совместимости ПО?

- a) Отсутствие .NET Framework нужной версии
- b) Наличие лицензионного ключа
- c) Использование SSD вместо HDD
- d) Подключение монитора через HDMI

21. Какой из перечисленных инструментов позволяет настроить «зеркало обновлений» антивируса?

- a) Kaspersky Security Center
- b) Microsoft Word
- c) Notepad++
- d) Paint

22. Что рекомендуется делать при подозрении на заражение системы вирусом?

- a) Немедленно отключить компьютер от сети
- b) Перезагрузить в обычном режиме
- c) Удалить все файлы на рабочем столе
- d) Обновить обои рабочего стола

23. Какой из перечисленных методов НЕ относится к тестированию ПО?

- a) Функциональное тестирование
- b) Регрессионное тестирование
- c) Социальная инженерия
- d) Нагрузочное тестирование

24. Какой из перечисленных параметров безопасности можно настроить в браузере?

- a) Блокировка всплывающих окон
- b) Автоматическая очистка кэша при закрытии
- c) Отключение JavaScript
- d) Все перечисленные

25. Какой из перечисленных действий НЕ рекомендуется при работе с реестром Windows?

- a) Создавать резервную копию перед изменениями
- b) Удалять произвольные ключи без понимания их назначения
- c) Использовать поиск по ключевым словам
- d) Экспортировать ветку в .reg-файл

26. Какой из перечисленных показателей качества ПО связан с «безотказностью»?

- a) Производительность
- b) Надёжность
- c) Портативность
- d) Удобство использования

27. Какой из перечисленных инструментов позволяет создать образ системы в Windows?

- a) Acronis True Image
- b) CCleaner
- c) WinRAR
- d) VLC Media Player

28. Что такое «групповая политика» в Windows?

- a) Инструмент централизованного управления настройками ОС и ПО
- b) Антивирусная программа
- c) Служба обновления Windows
- d) Утилита для очистки диска

29. Какой из перечисленных методов позволяет повысить производительность ПО?

- a) Оптимизация запросов к базе данных
- b) Увеличение объёма оперативной памяти
- c) Дефрагментация диска (для HDD)
- d) Все перечисленные

30. Какой из перечисленных документов должен быть подготовлен при выявлении несоответствия ПО требованиям ТЗ?

- a) Баг-репорт
- b) Руководство пользователя
- c) Лицензионное соглашение
- d) Счёт на оплату

Время выполнения теста: 45 минут.

Оценка:

- 26–30 правильных ответов — «отлично»
- 20–25 — «хорошо»
- 15–19 — «удовлетворительно»
- менее 15 — «неудовлетворительно»

Ответы:

1	c) Корректная установка драйверов
2	b) Исходный дефект в коде или логике программы
3	d) Аппаратная резервация
4	b) ISO/IEC 25010
5	b) Event Viewer
6	b) Последствие первичной ошибки
7	d) Вымогатель (ransomware)
8	c) HTTPS
9	b) Правила блокировки USB-устройств

10	b) Отключение брандмауэра
11	c) Групповые политики (GPO)
12	b) CCleaner
13	b) Стандарты создания и управления технической документацией
14	d) Все перечисленные
15	b) Цвет интерфейса
16	b) HKEY_CURRENT_USER
17	a) Загружается только ядро ОС без сторонних служб и автозагрузки
18	b) Установка файрвола
19	a) ГОСТ Р ИСО/МЭК 12207
20	a) Отсутствие .NET Framework нужной версии
21	a) Kaspersky Security Center
22	a) Немедленно отключить компьютер от сети
23	c) Социальная инженерия
24	d) Все перечисленные
25	b) Удалять произвольные ключи без понимания их назначения
26	b) Надёжность
27	a) Acronis True Image
28	a) Инструмент централизованного управления настройками ОС и ПО
29	d) Все перечисленные
30	a) Баг-репорт

Вопросы открытого типа:

- 1) Что понимается под «качеством функционирования программного обеспечения»? Назовите ключевые характеристики.
- 2) В чём разница между первичной и вторичной ошибкой в программном обеспечении? Приведите пример.
- 3) Какие дестабилизирующие факторы могут повлиять на надёжность ПО в процессе эксплуатации?
- 4) Опишите методы повышения надёжности ПО: временная, информационная и программная избыточность.
- 5) Как проводится анализ рисков при внедрении нового программного продукта?
- 6) Какие математические модели используются для описания статистических характеристик ошибок в программах?
- 7) Что такое многоуровневая модель качества ПО? Как она применяется на практике?
- 8) В каких случаях целесообразна разработка модулей адаптации для существующего ПО?
- 9) Какие инструментальные средства вы используете для измерения эксплуатационных характеристик ПО?
- 10) Как организуется процесс тестирования ПО на соответствие требованиям технического задания?
- 11) Дайте классификацию вредоносных программ. Приведите примеры каждой категории.
- 12) Какие антивирусные технологии вы знаете? В чём их преимущества и недостатки?

- 13) Объясните принцип работы файрвола. Как он защищает компьютерную систему?
- 14) Какие задачи решают групповые политики безопасности в Windows?
- 15) Как правильно настроить зеркало обновлений антивирусной базы в корпоративной сети?
- 16) Какие меры защиты следует применить при работе с конфиденциальной информацией в браузере?
- 17) Какие риски связаны с неправильной работой с реестром Windows? Как их минимизировать?
- 18) Опишите процедуру обнаружения и устранения последствий вирусной атаки.
- 19) Какие протоколы и средства шифрования применяются для защиты передаваемых данных?
- 20) Какие действия необходимо выполнить при подозрении на компрометацию системы?
- 21) Как связана защита ПО с обеспечением его качества? Приведите пример взаимосвязи.
- 22) Какие документы согласно ГОСТ Р ИСО/МЭК 12207 регламентируют процессы обеспечения качества ПО?
- 23) Как вы будете действовать, если после установки ПО система стала нестабильно работать?
- 24) Какие шаги включает план восстановления системы после кибератаки?
- 25) Какие метрики качества ПО вы будете использовать при приёмке системы заказчиком?
- 26) Почему важно проводить сравнение результатов тестирования с требованиями ТЗ?
- 27) Какие средства диагностики помогут выявить аппаратные причины снижения производительности ПО?
- 28) Как организовать безопасное обновление ПО в условиях ограниченного доступа к интернету?
- 29) Какие права пользователей следует ограничить для повышения уровня защиты ПО?
- 30) Как CALS-технологии способствуют обеспечению качества документации при сопровождении ПО?

Ответы на вопросы:

- 1) Качество функционирования ПО — совокупность свойств, определяющих его пригодность к использованию в заданных условиях. Ключевые характеристики: надёжность, производительность, безопасность, удобство использования, сопровождаемость (по ISO/IEC 25010).
- 2) Первичная ошибка — исходный дефект в коде или логике (например, деление на ноль). Вторичная ошибка — следствие первичной



(например, сбой службы → потеря данных). Пример: ошибка в модуле авторизации → несанкционированный доступ → удаление БД.

3) Дестабилизирующие факторы: сбои питания, несовместимость ПО/драйверов, вредоносные программы, человеческий фактор, устаревшее оборудование, сетевые атаки.

4) Временная избыточность: повторное выполнение операции при сбое.

5) Информационная: контрольные суммы, резервное копирование.

6) Программная: дублирование модулей, использование альтернативных алгоритмов.

7) Анализ рисков включает: идентификацию угроз, оценку вероятности и последствий, выбор мер снижения риска (например, FMEA или SWOT-анализ).

8) Модели: модель Джелина–Моранды, модель Шумана, модель Гоэла–Окамото — описывают интенсивность отказов и распределение ошибок во времени.

9) Многоуровневая модель (например, ISO/IEC 25010) включает уровни: качество в использовании → внешнее качество → внутреннее качество → качество процесса.

10) Модули адаптации целесообразны при: миграции на новую ОС, интеграции устаревших систем, изменении требований заказчика без переписывания всего ПО.

11) PerfMon, Task Manager, PassMark, журналы событий Windows, специализированные профайлеры (например, Visual Studio Profiler).

12) На основе ТЗ формируются тест-кейсы → выполняется тестирование → фиксируются отклонения → составляется баг-репорт → проводится повторное тестирование после исправлений.

13) Вирусы — внедряются в файлы.

14) Черви — самораспространяются по сети.

15) Трояны — маскируются под легитимное ПО.

16) Ransomware — шифрует данные.

17) Spyware — собирает информацию.

18) Adware — показывает рекламу.

19) Сигнатурный анализ — быстро, но не ловит новые угрозы.

20) Эвристический — обнаруживает подозрительное поведение.

21) Песочница — изолирует запуск.

22) Облачные базы — актуальны, но требуют интернет.

23) Файрвол контролирует входящий/исходящий трафик по правилам. Блокирует несанкционированные подключения, предотвращает эксплуатацию уязвимостей.

24) Групповые политики позволяют централизованно: запретить автозагрузку, ограничить доступ к реестру, настроить парольную политику, отключить USB-накопители.

25) Установить антивирусный сервер (например, Kaspersky Security Center) → настроить HTTP-репозиторий → клиенты получают обновления с локального зеркала.

26) Отключить JavaScript/cookies от третьих лиц, включить DoH, использовать режим инкогнито, регулярно очищать кэш, установить расширения приватности (uBlock Origin).

27) Риск: повреждение системы, невозможность загрузки. Минимизация: резервная копия веток (.reg), работа только с известными ключами, использование PowerShell вместо прямого редактирования.

28) Отключить от сети.

29) Запустить антивирус (в безопасном режиме).

30) Восстановить файлы из резервной копии.

31) Проанализировать логи.

32) Обновить ПО и ОС.

33) Изменить пароли.

34) TLS/SSL для передачи, BitLocker/FileVault для хранения, PGP/GPG для электронной почты, AES-256 как стандарт шифрования.

35) Изолировать систему, сохранить логи, провести диагностику, уведомить администратора, восстановить из резервной копии, проанализировать вектор атаки.

36) Безопасность — часть качества. Например, уязвимость в ПО снижает его надёжность и доверие пользователей, что нарушает критерий «безопасность» в модели ISO 25010.

37) ГОСТ Р ИСО/МЭК 12207 регламентирует процессы: сопровождения, верификации, валидации, управления качеством.

38) Проверить журналы событий → выполнить чистую загрузку → откатить обновления → восстановить систему → проверить совместимость → переустановить ПО.

39) Изоляция → диагностика → устранение угрозы → восстановление данных → усиление защиты → аудит безопасности.

40) Время отклика, потребление CPU/RAM, частота сбоев, процент пройденных тест-кейсов, соответствие требованиям безопасности.

41) Чтобы убедиться, что ПО реализует все заявленные функции и не содержит критических отклонений от ожидаемого поведения.

42) HWiNFO, CrystalDiskInfo (для дисков), MemTest86 (память), диагностические утилиты BIOS/UEFI.

43) Настроить локальное зеркало обновлений (WSUS для Windows, репозиторий APT/YUM для Linux), обновлять через изолированный ПК с интернетом.

44) Запретить установку ПО, изменение системных настроек, доступ к панели управления, использование командной строки без одобрения.

45) CALS-технологии обеспечивают стандартизацию, структурирование, многократное использование и контроль версий технической документации, что повышает её качество и актуальность.

### 3. Задание к экзамену по модулю (квалификационному экзамену)

Теоретические вопросы:

- 1) Назовите основные этапы жизненного цикла программного обеспечения согласно ГОСТ Р ИСО/МЭК 12207. Какие процессы происходят на этапе сопровождения?
- 2) В чём заключается роль менеджера сопровождения при внедрении ПО? Какие документы он должен подготовить?
- 3) Опишите стратегии внедрения программного продукта (параллельное, поэтапное, «большой взрыв»). Приведите примеры применения каждой.
- 4) Что такое эксплуатационная документация? Какие виды документов в неё входят?
- 5) Объясните понятие «совместимость ПО». Какие типы совместимости вы знаете (аппаратная, программная, драйверная)?
- 6) Какие методы используются для решения проблем совместимости устаревших приложений в современных ОС?
- 7) Что такое «чистая загрузка»? В каких случаях она применяется?
- 8) Какие инструменты Windows позволяют диагностировать проблемы установки и запуска ПО?
- 9) Опишите процесс создания и восстановления системы из образа. Какие программы вы используете?
- 10) Что такое CALS-технологии? Как они применяются при оформлении технической документации?
- 11) Дайте определение качества функционирования ПО. Перечислите характеристики по модели ISO/IEC 25010.
- 12) В чём разница между первичной и вторичной ошибкой? Приведите пример из практики.
- 13) Какие дестабилизирующие факторы влияют на надёжность ПО в процессе эксплуатации?
- 14) Опишите методы повышения надёжности: временная, информационная и программная избыточность.
- 15) Как проводится анализ рисков при внедрении нового ПО? Какие методы вы используете (FMEA, SWOT)?
- 16) Какие метрики вы применяете для измерения эксплуатационных характеристик ПО (время отклика, потребление CPU и т.д.)?
- 17) Дайте классификацию вредоносных программ. Чем отличается троян от червя? Что такое ransomware?
- 18) Какие антивирусные технологии вы знаете? В чём их преимущества и недостатки?
- 19) Как настроить локальное зеркало обновлений антивирусных баз в корпоративной сети?
- 20) Что такое групповые политики (GPO)? Как с их помощью ограничить установку ПО пользователями?

21) Какие меры безопасности следует применить при работе с браузером для защиты конфиденциальных данных?

22) Как правильно работать с реестром Windows? Какие риски связаны с его редактированием?

23) Какие протоколы и средства шифрования обеспечивают защиту передаваемых и хранимых данных?

24) Опишите действия администратора при подозрении на вирусную атаку.

25) Какие права пользователей необходимо ограничить для повышения уровня безопасности ПО?

26) Как организуется безопасное обновление ПО в условиях ограниченного доступа к интернету?

27) Какие задачи решает фаервол? Как его настроить для блокировки нежелательного трафика?

28) Какие средства диагностики оборудования вы используете для выявления причин снижения производительности ПО?

Практико-ориентированные задания:

Задание №1 Вам необходимо внедрить офисный пакет (например, LibreOffice) на 10 рабочих станций малого предприятия.

Требуется:

- Разработать сценарий внедрения.
- Подготовить руководство оператора.
- Установить и настроить ПО.
- Проверить совместимость с существующими программами.
- Настроить антивирусную защиту и политики безопасности.
- Подготовить отчёт об установке и тестировании.

Задание №2 После обновления Windows пользователи жалуются, что старое приложение больше не запускается.

Требуется:

- Выявить причину несовместимости.
- Предложить и реализовать не менее двух способов решения (режим совместимости, виртуальная машина и др.).
- Зафиксировать результаты в отчёте.

Задание №3 Система стала работать медленно, наблюдаются частые сбои.

Требуется:

- Провести диагностику (анализ журналов, мониторинг ресурсов).
- Измерить эксплуатационные характеристики ПО.
- Выявить возможные угрозы (вирусы, перегрузка диска и т.д.).

– Выполнить оптимизацию и восстановление системы при необходимости.

Задание №4 Заказчик требует модифицировать функционал учётной программы (например, добавить экспорт в Excel).

Требуется:

- Проанализировать текущую версию ПО.
- Разработать модуль расширения (скрипт или плагин).
- Протестировать изменения.
- Подготовить документацию по новой функции.

Задание №5 Организация переходит с Microsoft Office на LibreOffice.

Требуется:

- Разработать план миграции для 20 рабочих станций.
- Выявить возможные проблемы совместимости форматов (.docx → .odt).
- Настроить шаблоны документов и макросы (если возможно).
- Подготовить руководство пользователя по основным операциям.
- Обеспечить защиту конфигурации через групповые политики (ограничение установки сторонних расширений).

Задание №6 На одном из рабочих мест обнаружено зашифрованное содержимое папки «Документы».

Требуется:

- Изолировать заражённую систему от сети.
- Идентифицировать тип вредоносной программы (с использованием ESET Online Scanner или аналога).
- Удалить угрозу и очистить автозагрузку.
- Восстановить файлы из резервной копии (предварительно созданной в рамках ЛР №6).
- Настроить антивирус с локальным зеркалом обновлений и политику безопасности.

Задание №7 Требуется подготовить ПК для сотрудника, работающего с конфиденциальной финансовой информацией.

Требуется:

- Установить и настроить 1С:Бухгалтерию.
- Отключить ненужные службы и USB-порты через групповые политики.
- Настроить браузер (режим приватности, блокировка скриптов, HTTPS-only).
- Создать образ системы после настройки.
- Разработать чек-лист ежедневной проверки безопасности.

Задание №8 Пользователь жалуется на медленную работу ПО и частые зависания.

Требуется:

- Проанализировать журналы событий Windows (Event Viewer).
- Измерить эксплуатационные характеристики (загрузка CPU, RAM, диска — через PerfMon).
- Выполнить чистую загрузку для выявления конфликтующих служб.
- Очистить диск и восстановить повреждённые системные файлы (sfc /scannow).
- Предложить рекомендации по оптимизации (дефрагментация, отключение визуальных эффектов и т.д.).

Задание №9 Заказчик хочет ежедневно архивировать папку «Проекты» на сетевой диск.

Требуется:

- Написать скрипт на PowerShell или Bash (в зависимости от ОС), который:
  - создаёт архив с датой в имени;
  - копирует его на сетевой ресурс;
  - удаляет архивы старше 30 дней.
- Настроить задачу в Планировщике заданий.
- Протестировать работу модуля.
- Подготовить документацию по установке и использованию.

Задание №10 В организации используется внутреннее клиентское приложение для учёта заявок.

Требуется:

- Проверить, передаётся ли трафик по защищённому протоколу (HTTPS/TLS).
- Проанализировать права доступа к исполняемому файлу и конфигурационным файлам.
- Проверить, сохраняются ли пароли в открытом виде.
- Настроить фаервол для ограничения исходящих подключений только к серверу приложения.
- Составить отчёт с рекомендациями по повышению уровня защиты.