**1. Теоретическая часть:**

**Определения:**

* **Спецификация программного обеспечения** — это документ, в котором описаны все требования к ПО. Он включает функциональные и нефункциональные требования, которые должны быть выполнены. Спецификация —это документ, в котором содержится информация о функциональных и нефункциональных требованиях к программному продукту. Она является основой для разработки, тестирования и верификации
* **Верификация** — это процесс проверки, соответствует ли разработанный продукт требованиям и спецификациям. Основной целью верификации является выявление ошибок в коде, проекте и документации на ранних этапах разработки, что позволяет сократить затраты на исправление ошибок
* **Аттестация** — это процедура оценки соответствия ПО установленным стандартам качества и требованиям. Это как "сертификация" программы, чтобы убедиться, что она безопасна, надежна и готова к использованию
* **Задача анализа спецификаций** — это проверка спецификации на полноту, наличие непротиворечивостей, однозначности и проверяемость. Мы должны убедиться, что все требования понятны, не конфликтуют друг с другом и могут быть проверены
* **Моделирование в процессе анализа спецификаций** — это создание моделей или прототипов программного продукта для проверки корректности требований. Например, мы можем создать схему взаимодействия пользователя с системой, чтобы убедиться, что все работает как задумано

**Цели верификации:**

Верификация важна, потому что она помогает выявить ошибки на ранних этапах разработки. Чем раньше мы найдем ошибку, тем дешевле и проще будет ее исправить. Верификация решает такие задачи, как:

* Проверка, что программа делает то, что должна
* Обеспечение качества кода и документации
* Снижение рисков появления серьезных ошибок в будущем

**Роль аттестации:**

Аттестация необходима для определенных типов ПО, особенно для тех, которые работают в критических областях (медицина, инженерия, атомная энергетика, сапёр). Аттестация подтверждает, что программа безопасна и надежна. Например, медицинское ПО должно пройти аттестацию, чтобы гарантировать безопасность пациентов. Аттестация может быть обязательной, например, для ПО, используемого в госструктурах

**2. Практическая часть:**

**Анализ требований:**

* **Первое требование:** Система должна обеспечивать безопасность пользовательских данных
  + **Анализ:** Требование не однозначное, потому что не указано, какие именно меры безопасности должны быть применены.
  + **Рекомендация:** Система должна обеспечивать безопасность пользовательских данных с использованием шифрования данных и двухфакторной аутентификации
* **Второе требование:** Приложение должно загружаться быстро
  + **Анализ:** средняя скорость загрузки ПО должна варьироваться от 1 до 3 секунд
  + **Рекомендация:** Сделать оптимизацию ПО, чтобы система работала быстро даже на слабых системах
* **Третье требование:** Пользователь должен иметь возможность восстановить доступ к учетной записи через электронную почту
  + **Анализ:** Требование полное, непротиворечивое и проверяемое.
  + **Рекомендация:** Пользователь должен получить письмо с инструкцией по восстановлению доступа в течение 5 минут после запроса

**Процедура верификации функции "восстановление пароля":**

1. **Проверка документации:** убедиться, что в документации описаны все шаги по восстановлению пароля
2. **Тестирование функциональности:**
   * Проверить, что пользователь может запросить восстановление пароля
   * Убедиться, что письмо с инструкцией приходит на указанный адрес
   * Проверить, что ссылка в письме действительна и позволяет сменить пароль
3. **Тестирование безопасности:**
   * Убедиться, что ссылка на восстановление пароля действительна только один раз
   * Проверить, что пароль меняется только после подтверждения по электронной почте
4. **Тестирование граничных условий:**
   * Проверить, что система корректно обрабатывает неправильные адреса электронной почты
   * Убедиться, что письма не приходят, если пользователь не запрашивал восстановление

**Оценка требований к аттестации медицинского приложения:**

* **Основные требования к безопасности и надежности:**
  + Защита данных пациентов (шифрование, доступ только авторизованным пользователям)
  + Надежность работы (отсутствие сбоев, резервное копирование данных)
  + Соответствие медицинским стандартам
* **Документация для аттестации:**
  + Документация по безопасности: политики безопасности, процедуры доступа
  + Техническая документация: архитектура системы, описание модулей).
  + Результаты тестирования, например, как: тесты на безопасность и надёжность
  + Должны быть сертификаты соответствия

**3. Аналитическая часть:**

**Сравнение анализа спецификаций и верификации:**

Анализ спецификаций проводится на этапе проектирования, чтобы убедиться, что требования корректны. Верификация проводится на этапе разработки, чтобы убедиться, что программа соответствует этим требованиям. Важно разделять эти процессы, потому что анализ спецификаций помогает избежать ошибок на начальных этапах, а верификация — на этапе реализации.

**Риски недостаточной аттестации:**

Недостаточная аттестация может привести к серьезным проблемам, особенно в критических областях. Например, в медицине некачественная аттестация может привести к утечке данных пациентов или сбоям в работе программы, что может навредить здоровью людей. В атомной энергетике — к сбоям в работе компьютеров или датчикам отслеживания, что может привести к авариям.

**Влияние на затраты:**

Регулярная верификация и аттестация могут увеличить затраты на начальных этапах, но в долгосрочной перспективе они помогают сэкономить деньги. Пренебрежение этими процессами может привести к дорогостоящим исправлениям ошибок на поздних этапах разработки или даже к отзыву продукта.

**Анализ времени на тестирование:**

Анализ спецификаций и грамотное распределение времени на верификацию и аттестацию помогают сократить общий срок разработки. Если мы закладываем время на эти процессы с самого начала, то можем избежать доработок и переделок на поздних этапах.

**Роль внешних аудитов:**

Внешние аудиты и независимая аттестация повышают доверие к программному продукту, потому что они подтверждают, что продукт соответствует стандартам. Плюсы: объективность и независимость. Минусы: дополнительные затраты и время.

**4. Заключение:**

Анализ спецификаций, верификация и аттестация — это важные этапы в создании качественного и безопасного программного обеспечения. Они помогают убедиться, что программа делает то, что должна, и готова к использованию. Без этих процессов можно столкнуться с серьезными проблемами, которые могут привести к потерям времени и денег.