Самостоятельная работа

Анализ спецификаций, верификация и аттестация программного обеспечения

Часть 1. Теоретическая часть:

Определения:

1. Спецификация программного обеспечения — это формальный документ, который описывает функциональные и нефункциональные требования к программному продукту. Она служит основой для разработки и тестирования программного обеспечения, которое показывает то, что должно быть создано.
2. Верификация — это процесс проверки того, что программное обеспечение соответствует заданным требованиям и спецификациям. Верификация включает в себя различные методы, такие как тестирование и анализ, чтобы убедиться, что план разработки продукта идет правильно.
3. Аттестация — это процесс формальной оценки и подтверждения того, что система или компонент соответствуют установленным стандартам и требованиям. Аттестация может включать в себя сертификацию безопасности или соответствия, чтобы гарантировать, что продукт готов к использованию в определенных условиях.
4. Задача анализа спецификаций — это процесс изучения и проверки спецификаций на предмет их корректности, полноты и непротиворечивости. Это важный этап в разработке ПО, который помогает выявить возможные ошибки или неопределенности до начала реализации.
5. Моделирование в процессе анализа спецификаций — это создание абстрактных представлений (моделей) системы для изучения ее поведения и свойств. Модели помогают визуализировать требования и взаимодействия, а также позволяют проводить симуляции и анализировать различные сценарии работы системы.

Верификация помогает убедиться, что разработанное программное обеспечение соответствует спецификациям и требованиям, установленным на начальных этапах проекта. Находит ошибки на ранних этапах создания продукта и помогает повысить его качество.

Примеры решаемых верификацией задач:

1. Оценивает полноту и непротиворечивость требований.
2. Проверяет, выполняет ли система все заложенные в нее функции.
3. Проверяет код на наличие ошибок
4. Создает модели систем для дальнейшего анализа их анализа.

Аттестация нужна для того, чтобы подтвердить, что программное обеспечение соответствует стандартам, особенно если оно работает в специфических отраслях, например, в медицине. Она минимизирует риски, что система может слететь, путем проверки и оценки системы.

Пример, когда она обязательна: аттестация обязательна в тех случаях, когда она проверяет медицинские системы или транспортные, т.е. в тех случаях, когда есть риск угрозы жизни в случае, если ПО выйдет из строя.

Пример, когда она добровольна: аттестация добровольна в тех случаях, когда система не навредит тем, что выйдет из строя. Это могут быть какие-то офисные ПО, для бизнеса или даже игры.

Часть 2. Практическая часть:

-Требование 1: «Система должна обеспечивать безопасность пользовательских данных.»

1. Полнота: не были указаны меры, которые будут предприниматься для защиты пользовательских данных.
2. Непротиворечивость: я думаю, что при такой формулировки тяжело обозначить противоречия.
3. Однозначность: требование «обеспечить безопасность» достаточно тяжело сузить, ведь это достаточно общее понятие.
4. Проверяемость: требование должно иметь больше критериев для его создания
5. Рекомендации для улучшения: я считаю, что в этом требовании не хватает деталей и конкретики: нужно обозначить, каким путем и с какими предложенными вариантами система будет осуществлять защиту данных пользователей.

- Требование 2: «Приложение должно загружаться быстро.»

1. Полнота: в требовании не указаны конкретные временные рамки для "быстрой" загрузки (например, в течение 2 секунд).
2. Непротиворечивость: я не думаю, что в этом требовании имеются противоречия.
3. Однозначность: требование «быстро» для всех является разным, нужно указать временной интервал загрузки.
4. Проверяемость: не хватает указанного интервала времени для проверки.
5. Рекомендации для улучшения: для этого требования нужно указать временной интервал, для которого и будет создаваться система.

- Требование 3: «Пользователь должен иметь возможность восстановить доступ к учетной записи через электронную почту.»

1. Полнота: требование вполне является полным, но не указано, как именно будет проводиться восстановление (например, через сброс пароля на почту или перехода по ссылке для сброса пароля).
2. Непротиворечивость: нет противоречий.
3. Однозначность: в требовании все однозначно, но может не хватать конкретных деталей.
4. Проверяемость: требование возможно проверить.
5. Рекомендация для улучшения: необходимо уточнить способы восстановления пароля.

Этапы проведения верификации функции «восстановление пароля» в веб-приложении:

1. Создание аккаунта: ввод электронной почти и пароля – нужно создать аккаунт на существующую рабочую почту.
2. Проверка аккаунта на правильность и работоспособность – убедиться, что данные введены корректно.
3. Сброс ссылки для восстановления пароля по эл. почте – проверить, что ссылка рабочая и отправляет нас на станицу для сброса пароля.
4. Переход по ссылке и сброс пароля – ввести корректные пароль.
5. Проверка работоспособности пароля при входе – повторить вход в аккаунт с новым паролем, убедиться, что данные написаны корректно.

Основные требования к безопасности и надежности медицинского приложения перед началом аттестации:

1. Конфиденциальность – данные зашифрованы и не разглашаются третьим лицам.
2. Доступность – пресечение кибер атак и присутствие резервного копирования.
3. Двойная аутентификация.
4. Соответствует стандартам и нормам.
5. Патчи безопасности.

Документации и данные перед началом аттестации:

1. Тестирование на ошибки и сбои.
2. Тестирование на онлайн пользователей.
3. Предоставление данных о нагрузке.
4. Описание конкретных компонентов системы.

Часть 3. Аналитическая часть:

Анализ спецификаций — это процесс изучения и оценки требований и спецификаций системы, чтобы убедиться, что они полные, ясные, непротиворечивые и выполнимые. Этот процесс может включать в себя проверку на наличие неясностей или пробелов в документации.

Верификация — это процесс проверки того, что продукт или система соответствует заданным требованиям и спецификациям. Это может включать тестирование, проверку кода и другие методы, чтобы убедиться, что система работает так, как задумано.

Этапы жизненного цикла: анализ спецификаций выполняется на ранних этапах жизненного цикла программного обеспечения, обычно во время фазы сбора требований и проектирования, а верификация выполняется на более поздних этапах жизненного цикла, таких как тестирование и интеграция, когда уже создан прототип или готовый продукт.

Недостаточная аттестация программного обеспечения может привести к серьезным последствиям, особенно в критических областях, таких как медицина и авиация. В медицине это могут быть ситуации, когда какие-либо программы, связанные с анализом данных об состоянии пациента, могут вывести неправильный результат. В таком случае врач может выписать неправильное лечение, что может усугубить состояние человека.

Регулярное выполнение верификации и аттестации может повлиять на общие затраты компании на разработку ПО данными способами:

1. Снижение дефектов: Раннее выявление ошибок уменьшает стоимость их исправления.
2. Улучшение качества: Высокое качество снижает обращения в поддержку и возвраты.
3. Сокращение времени на доработки: Четкие процессы помогают избежать значительных переработок.
4. Соответствие стандартам: это снижает риски юридических последствий и штрафов.

Пренебрежение этими процессами может привести к потере клиентов, увеличению затрат на обслуживание и потере одобрения со стороны общества.

Анализ спецификаций и грамотное распределение времени на верификацию и аттестацию может сократить общий срок разработки ПО в данных аспектах:

1. Раннее выявление проблем, в котором анализ требований на начальных этапах помогает обнаружить ошибки раньше, что снижает затраты на их исправление.
2. Эффективное планирование. Заблаговременное выделение времени на тестирование позволяет команде лучше организовать работу.
3. Улучшение качества продукта - систематическое тестирование повышает уверенность в продукте.
4. Сокращение рисков. Закладывание времени на тестирование помогает управлять рисками и более точно прогнозировать сроки завершения проекта.

Именно поэтому важно закладывать время на эти процессы, чтобы избежать рисков и привести работу в стабильное состояние.

Роль внешних аудитов и независимой аттестации:

1. Стандартизация, где внешние организации часто следуют установленным стандартам и методологиям, что обеспечивает единообразие в оценке качества программного продукта.
2. Повышение доверия, в которой сертификация или положительный результат аудита от уважаемой независимой компании могут повысить доверие со стороны клиентов, партнеров и инвесторов.
3. Выявление уязвимостей. Внешние эксперты могут обнаружить уязвимости и недостатки, которые могли быть упущены внутренней командой, благодаря своему опыту и свежему взгляду.
4. Соблюдение нормативных требований, где внешние аудиты помогают убедиться, что продукт соответствует требованиям законодательства и стандартам отрасли.

Плюсы, возникающие при привлечении сторонних компаний для проведения верификации и аттестации – экономия ресурсов, при которых команды смогут сосредоточиться на своих задачах; улучшение процессов; независимость, при которых можно получить более высокую оценку работы.

Минусы, возникающие при привлечении сторонних компаний для проведения верификации и аттестации – появляется зависимость от внешних экспертов; стоимость услуг может быть дорогой; процесс согласования на работу иногда затягивается.

Часть 4. Заключение:

Я считаю, что анализ спецификации, верификации и аттестации для создания качественного и безопасного программного обеспечения – это очень важный процесс в работе, потому что он помогает структурировать и проверить проект на наличие каких-либо недочетов. Эти аспекты могут выявить, что конечный продукт может не совпадать требованиям или нормам его осуществления. В таком случае у компании будут точные данные, что именно им нужно исправить. Подтверждение качества позволяет Благодаря качественной работе, компания получает не только хорошие отзывы от постоянных клиентов, но и новых потенциальных покупателей, что отлично сказывается на бюджете и репутации организации.