**1) ФАКТОРИ ЯКОСТІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ.**

1. Функциональность (Functionality)

* Совместимость в смысле алгоритма
* Точность (соответствие между функцией и требованиями)
* Взаимодействие
* Безопасность

1. Надежность (Reliability)

* Зрелость
* Толерантность к ошибке
* Самовосстановление

1. Удобство использования (Usability)

* Способность к пониманию (understandability)
* Способность к обучению (learnability)
* Работоспособность (operability)
* Привлекательность (attractiveness)

1. Эффективность (Efficiency)

* Временное поведение (time behavior)
* Использование ресурсов

1. Сопровождаемость (Maintainability)

- Анализируемость (Analysability)

- Изменяемость (Changeability)

- Стабильность (Stability)

- Тестируемость (Testability)

6. Мобильность (Portability)

- Адаптируемость (Adaptability)

- Настраиваемость (простота внедрения, Installability)

- Совместимость (Co-existence)

- Взаимозаменяемость (Replaceability)

**ФУНКЦИОНАЛЬНОСТЬ (FUNCTIONALITY)**

Способность программного продукта обеспечивать функции, удовлетворяющие установленные и подразумеваемые потребности при применении программного средства в заданных условиях. Эта характеристика определяет,*что*делает ПС в соответствии с потребностями. Другие характеристики определяют,*когда*и*как*эти потребности удовлетворяются.

***Пригодность (Suitability)***– способность программного продукта обеспечивать набор функций, соответствующий специфическим задачам и целям пользователей.

***Правильность (корректность, Accuracy)***– способность программного продукта обеспечивать правильные или приемлемые результаты или эффекты с необходимой степенью точности.

***Способность к взаимодействию(Interoperability)***– способность про-

граммного продукта взаимодействовать с одной или несколькими заданными системами.

***Защищенность (Security)***– способность программного продукта защищать информацию и данные так, чтобы несанкционированные пользователи или системы не могли прочитать или модифицировать их, а санкционированные пользователи или системы не могли получить отказа в доступе к ним.

**НАДЕЖНОСТЬ (RELIABILITY)**

Способность программного продукта поддерживать заданный уровень качества функционирования при его использовании в заданных условиях. Ограничения надежности в процессе эксплуатации вызваны ошибками в требованиях, проектировании и кодировании.

***Завершенность (Maturity)***– способность программного продукта избегать отказов вследствие ошибок в программах.

***Устойчивость к ошибке(Fault tolerance)***– способность программного продукта поддерживать заданный уровень качества функционирования в случаях ошибок в программах или нарушения заданного интерфейса ПП.

***Восстанавливаемость (Recoverability)***– способность программного продукта восстанавливать заданный уровень качества функционирования и -данные, поврежденные в случае отказа. Одним из показателей восстанавливаемости является длительность восстановления.

***Готовность (доступность, Availability)***– способность программного продукта быть в состоянии выполнять требуемую функцию в данный момент

**ПРАКТИЧНОСТЬ (USABILITY)**

Способность программного продукта быть понятным, изученным, использованным и привлекательным для пользователя при применении в заданных условиях. Очевидно, что практичность зависит от некоторых аспектов таких характеристик качества, как функциональность, надежность и эффективность. Подхарактеристики*Практичности*приведены нарис. 46.

***Понятность (Understandability)***– способность программного продукта, обеспечивающая понимание пользователем пригодности и способа использования программного средства для конкретных задач и условий применения.

***Обучаемость (Learnability)***– способность программного продукта, обеспечивающая изучение пользователем принципов его применения.

***Простота использования (Operability)***– способность программного продукта, позволяющая пользователю эксплуатировать его и управлять . имНа простоту использования влияют некоторые аспекты таких подхарактеристик, как пригодность, изменяемость, адаптируемость и простота внедрения. Простота использования зависит, например, от контролируемости и устойчивости к ошибке.

***Привлекательность (Attractiveness)***– способность программного продукта нравиться пользователю. Данная подхарактеристика связана со свойствами оформления ПП (например использование цветов, графики и т.п.).

**ЭФФЕКТИВНОСТЬ (EFFICIENCY)**

Способность программного продукта обеспечить соответствующую производительность в зависимости от количества используемых вычислительных ресурсов в заданных условиях. Ресурсы могут включать другие программные продукты, конфигурацию программных и аппаратных средств системы и материалы.

***Поведение во времени (Time behaviour)***– способность программного продукта обеспечивать соответствующие времена отклика и обработки, также пропускную способность при выполнении своих функций в заданных условиях.

***Использование ресурсов (Resource utilisation)***– способность программно-го продукта использовать соответствующее количество всех типов ресурсов при выполнении своих функций в заданных условиях. В данной подхарактеристике человеческие ресурсы не учитываются. Они учитываются в такой характеристике качества в использовании, как продуктивность.

***Соответствие эффективности (Efficiency compliance)***– способность программного продукта соответствовать стандартам и соглашениям, связанным с эффективностью.

**СОПРОВОЖДАЕМОСТЬ (MAINTAINABILITY)**

Способность программного продукта к модификации. Модификации могут включать исправления, усовершенствования или адаптацию ПС к изменениям в среде применения, в требованиях и функциональных спецификациях.

***Анализируемость (Analysability)***– способность программного продукта к диагностике его недостатков или причин отказов или к идентификации его частей, которые должны быть модифицированы.

***Изменяемость (Changeability)***– способность программного продукта к реализации заданной модификации. Реализация включает проектирование, кодирование и изменение документации.

***Стабильность (Stability)***– способность программного средства предотвращать непредвиденные эффекты от его модификации.

***Тестируемость (Testability)***– способность программного продукта к проверке результата модификации.

**МОБИЛЬНОСТЬ (PORTABILITY)**

Способность программного продукта к переносу из одной среды в другую. Среда может включать организационное, аппаратное и программное окружение. Подхарактеристики*Мобильности*представлены нарис. 46.

***Адаптируемость (Adaptability)***– способность программного продукта к адаптации к различным окружающим средам без применения дополнительных действий или средств. Адаптируемость включает масштабируемость внутренних возможностей (например, областей экранов, таблиц, форматов отчетов).

***Настраиваемость (простота внедрения, Installability)***– способность программного продукта устанавливаться в заданной среде окружения.

***Совместимость (Co-existence)***– способность программного продукта к сосуществованию с другими независимыми программными средствами в общей среде, разделяя общие ресурсы.

***Взаимозаменяемость (Replaceability)***– способность программного продукта к использованию вместо другого(заданного) ПП с той же целью и в той же среде. Например, для пользователя важна взаимозаменяемость новой версии ПП с его старой версией. Взаимозаменяемость может включать атрибуты таких подхарактеристик, как настраиваемость и адаптируемость.

**2) МЕТРИКИ ЯКОСТІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ХОЛСТЕДА.**

*n1* – число уникальных операторов

*N1* – общее число всех операторов

*n2* – число уникальных операндов

*N2* – общее число всех операндов

*n2'* – кол-во входных и выходных параметров

*n = n1 + n2* – словарь программы

*N = N1 + N2* – длина реализации

*N' = n1 \* log2(n1) + n2 \* log2(n2)* – длина программы (для стилистически корректных программ отклонение *N* от *N'* не превышает 10%)

*V = N \* log2(n)* – объем программы

*V' = (n2' + 2) \* log2(n2' + 2)* – потенциальный объем программы

*L = V' / V* – уровень качества программы (для идеальной программы *L = 1*)

*λ = V'^2 / V = L / V'* – уровень языка программирования

*I = [(2 \* n2) / (n1 \* N2)] \* (N1 + N2) \* log2(n1 + n2) = V / D* – информационное содержание программы (умственные затраты на создание программы)

*E = V^2 / V' = V / L* – необходимые интеллектуальные усилия при разработке программы

*T = E / S* – время составления программы, (число Страуда *S = 18*)

*M = m – n + 2p, p = 1* – метрика Маккейба

*M = n2' / 6* – количество модулей

*B' = V / 3000* – оценка числа дефектов в программе

**Объем программы по Холстеду** определяет объем кода, запрограммированного алгоритма. Размер метрики должен быть от 20 до 1000 для одной функции и от 100 до 8000 для одного файла. Если размер метрики превышает верхнюю границу, то рекомендуется более детально изучить функциональную нагрузку на исследуемый элемент и разбить его на несколько составляющих либо провести оптимизацию алгоритма.

**Операнды**

При расчете метрики Холстеда используются с

ледующие операнды:

*Идентификаторы* – все идентификаторы которые не являются зарезервированными словами;

*Идентификаторы типов* – зарезервированные слова обозначающие тип данных: bool, char, double, float, int, long, short, signed, unsigned, void;

*Константы* – числовые, символьные, строковые константы.

**Операторы**

Ключевые слова следующих категорий, которые интерпретируются как операторы:

Идентификаторы класса памяти: inline, register, static, typedef, virtual, mutable.

Квалификаторы типа: const, friend, volatile.

Зарезервированные слова: asm, break, case, class, continue, default, delete, do, else, enum, for, goto, if, new, operator, private, protected, public, return, sizeof, struct, switch, this, union, while, namespace, using, try, catch, throw, const\_cast, static\_cast, dynamic\_cast, reinterpret\_cast, typeid, template, explicit, true, false, typename

Операторы языка программирования:! != % %= &&& || &= ( ) \* \*= + ++ += , - -- -= -> . ... / /= : :: <<<<<= <= = == >>= >>>>= ? [ ] ^ ^= { } | |= ~

Следующие управляющие структуры for (...) if (...) switch (...) while for (...) and catch (...) интерпретируются как один оператор.

Холстед вводит *n'* – **теоретический словарь программы**, т.е. словарный запас, необходимый для написания программы с учетом того, что необходимая функция уже реализована в данном языке и, следовательно, программа сводится к вызову этой функции. Например, согласно Холстеду возможное осуществление процедуры выделения простого числа могло бы выглядеть так:

CALL SIMPLE (X, Y),

где Y – массив численных значений, содержащих искомое число X.

Теоретический словарь в этом случае будет состоять из

*n1'*: {CALL, SIMPLE (...)}, *n1'* =2;

*n2'*: {X,Y}, *n2'* =2;

а его длина, определяемая как *n' = n1' + n2'* будет равна 4.

Для вычисления цикломатического числа Маккейба Z(G) применяется формула

Z(G)=e-v+2p,

где e - число дуг ориентированного графа G;

v - число вершин;

p - число компонентов связности графа.

Число компонентов связности графа можно рассматривать как количество дуг, которые необходимо добавить для преобразования графа в сильно связный. Cильно связным называется граф, любые две вершины которого взаимно достижимы. Для графов корректных программ, т. е. графов, не имеющих недостижимых от точки входа участков и "висячих" точек входа и выхода, сильно связный граф, как правило, получается путем замыкания дугой вершины, обозначающей конец программы, на вершину, обозначающую точку входа в эту программу (p = 1).

**3) Визначення поняття верифікації програмного забезпечення**

Верифікацією й атестацією називаються процеси перевірки й аналізу, у ході яких перевіряється відповідність програмного забезпечення своєї специфікації і вимогам замовників. Верифікація й атестація охоплюють весь цикл життя ПЗ – вони починаються на етапі аналізу вимог і завершуються перевіркою програмного коду на етапі тестування програмної системи. Верифікація відповідає на запитання, чи правильно створена система, а атестація відповідає на запитання, чи правильно працює система. Верифікація перевіряє відповідність ПЗ системній специфікації, зокрема функціональним і нефункціональним вимогам.

У процесах верифікації й атестації використовуються дві основні методики перевірки й аналізу систем: інспектування ПЗ і тестування ПЗ. Інспектування ПЗ має на увазі аналіз і перевірку різних представлень системи, наприклад, документації. Інспектування відбувається на всіх етапах розробки програмної системи. Паралельно з інспектуванням може проводитися автоматичний аналіз вихідного коду програм і відповідних документів. Інспектування й автоматичний аналіз – це статичні методи верифікації й атестації, оскільки їм не потрібна виконуюча система. Тестування – динамічний метод верифікації й атестації, тому що застосовується до системи, що виконується.

У процесі планування верифікації й атестації необхідно визначити співвідношення між статичними і динамічними методами перевірки системи, визначити стандарти і процедури інспектування, скласти план тестування програм. Від типу розроблювальної системи залежить те, чому варто приділити більше уваги – інспектуванню або тестуванню. Чим більше критична система, тим більше уваги варто приділяти статичним методам верифікації. Отже, процеси верифікації й атестації інспектування і тестування варто використовувати спільно.

**4. Метрики якості програмного забезпечення маккейба**

Основанная на анализе передачи управления от 1-го операнда к 2-ому.

Она также была разработана для структурного программирования. Маккейб предельно описал программный код в виде графа где вершины являются операторами, а дугами – переходы между ними.

М = m-n+2 , где m- кол-во ребр, n – к-во вершин.

Цикломатическое число Маккейба: z = m-n+2p, p=1

Ц. число показывает его полносвязность (сколько цыклов)

Р – кол-во ребр, необходимых чтобы граф был полносвязным.

Ц. число Маккейба показывает сколько тестов надо запустить. Чтобы полностью протестировать программный код по одному з критериев покрытия. Если z>10, программа обладает излишней сложностью, и его следует разбить на модули.

Существует упрощённая формула расчета z:

М = u+1, u – к-во операторов условий

**5) Обнаружение ошибок**

Большинство методов направлено по возможности на неза­медлительное обнаружение сбоев. Немедленное обнаружение имеет два преимущества: можно минимизировать влияние ошиб­ки и последующие затруднения для человека, которому придется извлекать информацию о ней, находить ее и исправлять.

{SITELINK-S405}Меры по обнаружению ошибок {/SITELINK}можно разбить на две под­группы: ***пассивные***попытки обнаружить симптомы ошибки в про­цессе «обычной» работы программного обеспечения и ***активные***попытки программной системы периодически обследовать свое состояние в поисках признаков ошибок.

***Пассивное обнаружение****.*Меры по обнаружению ошибок могут быть приняты на нескольких структурных уровнях программной системы. Здесь мы будем рассматривать уровень подсистем, или ком­понентов, т.е. нас будут интересовать меры по обнаружению симп­томов ошибок, предпринимаемые при переходе от одного компо­нента к другому, а также внутри компонента. Все это, конечно, при­менимо также к отдельным модулям внутри компонента.

Разрабатывая эти меры, мы будем опираться на следующее.

1. *Взаимное недоверие.*Каждый из компонентов должен пред­полагать, что все другие содержат ошибки. Когда он получает какие-нибудь данные от другого компонента или из источника вне системы, он должен предполагать, что данные могут быть неправильными, и пытаться найти в них ошибки.

*2. Немедленное обнаружение.*Ошибки необходимо обнаружить как можно раньше. Это не только ограничивает наносимый ими ущерб, но и значительно упрощает задачу отладки.

3. *Избыточность.*Все средства обнаружения ошибок основаны на некоторой форме избыточности (явной или неявной).

*Активное обнаружение ошибок.*Не все ошибки можно выя­вить пассивными методами, поскольку эти методы обнаружива­ют ошибку лишь тогда, когда ее симптомы подвергаются соот­ветствующей проверке. Можно делать и дополнительные провер­ки, если спроектировать специальные программные средства для активного поиска признаков ошибок в системе. Такие средства называются *средствами активного обнаружения ошибок.*

Активные средства обнаружения ошибок обычно объединя­ются в *диагностический монитор:*параллельный процесс, кото­рый периодически анализирует состояние системы с целью обна­ружить ошибку. Большие программные системы, управляющие ресурсами, часто содержат ошибки, приводящие к потере ресур­сов на длительное время. Например, управление памятью опера­ционной системы сдает блоки памяти «в аренду» программам пользователей и другим частям операционной системы. Ошибка в этих самых «других частях» системы может иногда вести к не­правильной работе блока управления памятью, занимающегося возвратом сданной ранее в аренду памяти, что вызывает медлен­ное вырождение системы.

**6) Концепция тестирования**

*Программа* – это аналог формулы в обычной математике.

Формула для функции f, полученной *суперпозицией* функций f1, f2, ... fn – *выражение*, описывающее эту *суперпозицию*.

f = f1\* f2\* f3\*... \* fn

Если аналог f1,f2,... fn – *операторы* языка программирования, то их формула – *программа*.

Существует два метода обоснования *истинности формул*:

1. **Формальный подход** или **доказательство** применяется, когда из исходных формул-аксиом с помощью формальных процедур (правил вывода) выводятся искомые формулы и утверждения (теоремы). Вывод осуществляется путем перехода от одних формул к другим по строгим правилам, которые позволяют свести процедуру перехода от формулы к формуле к последовательности текстовых подстановок:
2. A\*\*3 = A\*A\*A

A\*A\*A = A -> R, A\*R -> R, A\*R -> R

Преимущество формального подхода заключается в том, что с его помощью удается избегать обращений к бесконечной области значений и на каждом шаге доказательства оперировать только конечным множеством символов.

1. **Интерпретационный подход** применяется, когда осуществляется подстановка констант в формулы, а затем интерпретация формул как осмысленных утверждений в элементах множеств конкретных значений. *Истинность* интерпретируемых формул проверяется на конечных множествах возможных значений. Сложность подхода состоит в том, что на конечных множествах комбинации возможных значений для реализации исчерпывающей проверки могут оказаться достаточно велики.

Интерпретационный подход используется при экспериментальной проверке соответствия программы своей спецификации

Применение интерпретационного подхода в форме экспериментов над исполняемой программой составляет суть *отладки* и *тестирования*.

**Основная терминология**

***Отладка (debug, debugging)*** – процесс поиска, локализации и исправления ошибок в программе [[ 9 ]](https://www.intuit.ru/studies/courses/48/48/literature#literature.9)[IEEE Std.610-12.1990].

Термин " *отладка* " в отечественной литературе используется двояко: для обозначения активности по поиску ошибок (собственно *тестирование*), по нахождению причин их появления и исправлению, или активности по локализации и исправлению ошибок.

***Тестирование*** обеспечивает выявление (констатацию наличия) фактов расхождений с требованиями (ошибок).

Как правило, на ***фазе тестирования*** осуществляется и исправление идентифицированных ошибок, включающее локализацию ошибок, нахождение причин ошибок и соответствующую корректировку программы тестируемого приложения (Application Under Testing (AUT) или Implementation Under Testing (IUT)).

Если *программа* не содержит синтаксических ошибок (прошла трансляцию) и может быть выполнена на компьютере, она обязательно вычисляет какую-либо функцию, осуществляющую *отображение* входных данных в выходные. Это означает, что *компьютер* на своих ресурсах доопределяет частично определенную программой функцию до тотальной определенности. Следовательно, судить о правильности или неправильности результатов выполнения программы можно, только сравнивая спецификацию желаемой функции с результатами ее вычисления, что и осуществляется в процессе *тестирования*.

7. **Зв’язок задач валідації, верифікації та тестування с життевим циклом програмного забезпечення.**

**Валідація програмного забезпечення** ([англ.](https://uk.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0_%D0%BC%D0%BE%D0%B2%D0%B0) *Validation Software*) — процес визначення відповідності розроблюваного [програмного забезпечення](https://uk.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BD%D0%B5_%D0%B7%D0%B0%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%BD%D1%8F) між очікуваннями і потребами користувача, вимогам до системи. Валідація є одним із основних етапів [тестування програмного забезпечення](https://uk.wikipedia.org/wiki/%D0%A2%D0%B5%D1%81%D1%82%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BD%D0%BE%D0%B3%D0%BE_%D0%B7%D0%B0%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%BD%D1%8F).

Мета процесу валідації — переконатися, що специфічні вимоги для програмного продукту виконано, і здійснюється це за допомогою:

* розробленої стратегії і критеріїв перевірки всіх робочих продуктів;
* обговорених дій з проведення валідації;
* демонстрації відповідності розроблених програмних продуктів вимогам замовника і правилам їхнього використання;
* узгодження із замовником отриманих результатів валідації продукту.

Процес валідації може проводитися самим виконавцем або іншою особою, наприклад, замовником, що здійснює дії з впровадженню і проведенню цього процесу за планом, у якому відбиті елементи і задачі перевірки. При цьому використовуються методи, інструментальні засоби і процедури виконання задач процесу для встановлення відповідності тестових вимог і особливостей використання програмних продуктів проекту на правильність реалізації вимог.

[Верифікація](https://uk.wikipedia.org/wiki/%D0%92%D0%B5%D1%80%D0%B8%D1%84%D1%96%D0%BA%D0%B0%D1%86%D1%96%D1%8F_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BD%D0%BE%D0%B3%D0%BE_%D0%B7%D0%B0%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%BD%D1%8F) і валідація полягає в перевірці специфікацій і правильності виконання програм відповідно до заданих вимог і формального опису програми.

Верифікація програмного коду допомагає зробити висновок про коректність створеної програмної системи при її проектуванні і після завершення її розроблення. Валідація дозволяє встановити здійснимість заданих вимог шляхом їх перегляду, інспекції і оцінки результатів проектування на процесах [життєвого циклу](https://uk.wikipedia.org/wiki/%D0%96%D0%B8%D1%82%D1%82%D1%94%D0%B2%D0%B8%D0%B9_%D1%86%D0%B8%D0%BA%D0%BB_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BD%D0%BE%D0%B3%D0%BE_%D0%B7%D0%B0%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%BD%D1%8F) для підтвердження того, що здійснюється коректна реалізація вимог, дотримання заданих умов і обмежень до системи. Верифікація і валідація забезпечують перевірку повноти, несуперечності і однозначності специфікації і правильності виконання функцій системи.

[Верифікації](https://uk.wikipedia.org/wiki/%D0%92%D0%B5%D1%80%D0%B8%D1%84%D1%96%D0%BA%D0%B0%D1%86%D1%96%D1%8F_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BD%D0%BE%D0%B3%D0%BE_%D0%B7%D0%B0%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%BD%D1%8F) і валідації піддаються:

* компоненти системи, їх інтерфейси (програмні, технічні і інформаційні) і взаємодія об'єктів (протоколи, повідомлення) у розподілених середовищах;
* описи доступу до [баз даних](https://uk.wikipedia.org/wiki/%D0%91%D0%B0%D0%B7%D0%B8_%D0%B4%D0%B0%D0%BD%D0%B8%D1%85), засоби захисту від несанкціонованого доступу до даних різних користувачів;
* документація до системи;
* тести, тестові процедури і вхідні набори даних.

На інших процесах [життєвого циклу](https://uk.wikipedia.org/wiki/%D0%96%D0%B8%D1%82%D1%82%D1%94%D0%B2%D0%B8%D0%B9_%D1%86%D0%B8%D0%BA%D0%BB_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BD%D0%BE%D0%B3%D0%BE_%D0%B7%D0%B0%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%BD%D1%8F) виконуються додаткові дії:

* перевірка і контроль проектних рішень за допомогою методик і процедур перегляду ходу розроблення;<
* звернення до CASE-систем , що містять у собі процедури перевірки вимог до продукту;
* перегляди й інспекції проміжних результатів на відповідність вимогам для підтвердження того, що програмна система має коректну

реалізацію вимог і задовольняє умови виконання.

Таким чином, основні задачі процесів верифікації і валідації полягають у тому, щоб перевірити і підтвердити, що кінцевий програмний продукт відповідає призначенню і задовольняє вимогам замовника. Ці процеси взаємозалежні і визначаються, як правило, одним загальним терміном «верифікація і валідація» або «Verification and Validation» (V&V).

V&V засновані на плануванні їх як процесів, так і перевірки для найбільш критичних елементів проекту: компонентів, інтерфейсів (програмних, технічних і інформаційних), взаємодій об'єктів (протоколів і повідомлень), передачі даних між компонентами і їхнього захисту, а також створення тестів і тестових процедур.

Після перевірки окремих компонентів системи проводяться їхня інтеграція, повторна верифікація і валідація інтегрованої системи, створюється комплект документації, що відображає правильність виконання вимог за результатами інспекцій і [тестування тестування](https://uk.wikipedia.org/wiki/%D0%A2%D0%B5%D1%81%D1%82%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BD%D0%BE%D0%B3%D0%BE_%D0%B7%D0%B0%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%BD%D1%8F).

**8) Стадії тестування в процесі розробки програмного забезпечення.**





**9) Модель управління якістю програмного забезпечення - CMMI.**

Capability Maturity Model Integration (CMMI) — це підхід для вдосконалення процесів, який забезпечує організації суттєвими елементами ефективних процесів. Він може використовуватись для покращення процесу як на рівні проекту чи відділу, так і на рівні цілої організації. CMMI дозволяє інтегрувати традиційно відокремлені організаційні функції.

CMMI визначає 22 процесні області . Для кожної із процесних областей існує ряд цілей (goals), які повинні бути досягнуті при впровадженні CMMI в даній конкретній процесній області. Деякі цілі є унікальними — вони називаються спеціальними. Загальні цілі застосовуються одразу до декількох процесних областей. Цілі досягаються за допомогою практик; так само, як і цілі, практики діляться на спеціальні та загальні.

Існує два представлення CMMI — поетапне і неперервне .Поетапне представлення групує процесні області у п'ять рівнів *зрілості*. Неперервне представлення визначає рівні *можливостей*.

5 рівнів : **1. Початковий** . Якщо організаця знаходиться на цьому рівні то ключові області процесів для неї не передбачено

**2. Повторюваний .** Управління програмними конфігураціями . Забезпечення якості програмних продуктів . Управління контрактами підрядчиків.Контроль за ходом проектів. Планування програмних проектів . Управління вимогами

**3.Визначений .** Експертні оцінки. Координація взаємодії проектних груп. Інженерія програмного продукту. Комплексний менеджмент ПЗ. Програма навчання персоналу. Визначення організаційного процесу.

**4 Керований .** Менеджмент якості ПЗ. Управління процессом на основі кількісних методів.

**5 Опитмізований.** Управління змінами в процесі . Управління технологічними змінами . Запобігання дефектів

10) Основні проблеми процесу тестування програмного забезпечення.

Тестирование – процесс выполнения действий программы с целью обнаружения в ней ошибок.

Тестовая ситуация – входы для проверки системы и соответственно существ выходы (спецификации требования).

Ошибка – действие программного кода на этапе разработки, приводящее к тому, что ПО работает неправильно, т.е. не соответствует требованиям.

Отказ – непредсказуемое поведение ПО, как правило является ошибкой аналитика, но программист так же может быть причастен.

**11. Модульне тестування**

Тестирование програмного кода на уровне отдельно взятого модуля , функции или классы. Основная цель – найти ошибку в алгоритме. Модульное тестирование проводится по принципе «Белого ящика» . Чтобы реализовать , необходимо создать соответсвующее окружение . Окружение включает в себя заглушки всех интерфейсов из одного модуля. Заглушка – генератор случаных чисел либо набор констант выхода или входа . Стратегия тестирования формируется с направлением входных данных либо выходных. Чтобы реализовать модульное тестирование необходимо реализовать цикл предотвращения дефектов.У нас есть база ошибок и контроль версий данного модуля , на практике это две системы контроль версий и back tracking . Благодаря наличию базы есть возможность анализировать ошибки и источники их возникновения. Это важно для поиска . Модульное тестирование в 99 случаях это структурное тестирование следовательно мы приминяем структурный критерий тестирования . Дополнением к структурному тестированию выступает анализ метрик третей фазей модульного тестирования может быть полуавтоматическое тестирование.

Вторая фаза модульного тестирования ориентирована на тесты алгоритмов. На первом этапе вычисляется количество тестовых путей необходимо выбрать необходимое количество тестовых путей .

**12. Тестирование методом „белій ящик”**

Тестирование методом белого ящика (также: прозрачного, открытого, стеклянного ящика; основанное на коде или структурное тестирование) – метод тестирования программного обеспечения, который предполагает, что внутренняя структура/устройство/реализация системы известны тестировщику. Мы выбираем входные значения, основываясь на знании кода, который будет их обрабатывать. Точно так же мы знаем, каким должен быть результат этой обработки. Знание всех особенностей тестируемой программы и ее реализации – обязательны для этой техники. Тестирование белого ящика – углубление во внутренне устройство системы, за пределы ее внешних интерфейсов.

**Тестирование белого ящика – это:**

– тестирование, основанное на анализе внутренней структуры компонента или системы.

– тест-дизайн, основанный на технике белого ящика – процедура написания или выбора тест-кейсов на основе анализа внутреннего устройства системы или компонента.

Почему «белый ящик»? Тестируемая программа для тестировщика – прозрачный ящик, содержимое которого он прекрасно видит.

Методы белого ящика :

2.1.1 Метод покрытия операторов

Целью этого метода тестирования является выполнение каждого оператора программы хотя бы один раз.

2.2 Метод покрытия решений (покрытия переходов)

Более сильный метод тестирования известен как покрытие решений (покрытие переходов). Согласно данному методу каждое направление перехода должно быть реализовано по крайней мере один раз.

2.3 Метод покрытия условий-

Лучшие результаты по сравнению с предыдущими может дать метод покрытия условий. В этом случае записывается число тестов, достаточное для того, чтобы все возможные результаты каждого условия в решении выполнялись по крайней мере один раз

2.4 Критерий решений (условий)

Критерий покрытия решений/условий требует такого достаточного набора тестов, чтобы все возможные результаты каждого условия в решении выполнялись по крайней мере один раз, все результаты каждого решения

2.5 Метод комбинаторного покрытия условий.

Критерием, который решает эти и некоторые другие проблемы, является комбинаторное покрытие условий. Он требует создания такого числа тестов, чтобы все возможные комбинации результатов условия в каждом решении выполнялись по крайней мере один раз. Набор тестов, удовлетворяющих критерию комбинаторного покрытия условий, удовлетворяет также и критериям покрытия решений, покрытия условий и покрытия решений/условий.

**13) Надійність програмного забезпечення.**

Надежность программного обеспечения существенно отличается от надежности апаратури.Програмы не изнашиваются, поломка программы невозможна.

О надежности программного обеспечения речь идет только с точки зрения ошибок в нем самом. Совершенно не затронута важная тема использования программ для исправления ошибок аппаратуры или их последствий Важной характеристикой надёжности програмного обеспечения является его восстанавливаемость, которая определяется затратами времени и труда на устранение отказа через проявилась ошибки в программе и его последствий. Восстановление после отказа в программе может заключаться в корректировке восстановлении текста программы, исправлении данных, внесение изменений в организацию вычислительного процесса, часто оказывается необходимым при работе ЭВМ в реальном масштабе времени

Организационные методы обеспечения надежности программного обеспечения включают также моделирование процесса разработки и достижимых уровней надежности. Основным показателем надежности является вероятность того, что оно работает без ошибок в течение фиксированного отрезка времени.

**14) Системное тестирование (System Testing)**

Основной задачей системного тестирования является проверка [как функциональных, так и не функциональных требований](http://www.protesting.ru/testing/testtypes.html) в системе в целом. При этом выявляются [дефекты](http://www.protesting.ru/testing/bugreport.html), такие как неверное использование ресурсов системы, непредусмотренные комбинации данных пользовательского уровня, несовместимость с окружением, непредусмотренные сценарии использования, отсутствующая или неверная функциональность, неудобство использования и т.д. Для минимизации рисков, связанных с особенностями поведения в системы в той или иной среде, во время тестирования рекомендуется использовать окружение максимально приближенное к тому, на которое будет установлен продукт после выдачи.

Можно выделить два подхода к системному тестированию:

на базе требований (requirements based)

Для каждого требования пишутся [тестовые случаи (test cases)](http://www.protesting.ru/testing/testcase.html), проверяющие выполнение данного требования.

на базе случаев использования (use case based)

На основе представления о способах использования продукта создаются случаи использования системы (Use Cases). По конкретному случаю использования можно определить один или более сценариев. На проверку каждого сценария пишутся [тест кейсы (test cases)](http://www.protesting.ru/testing/testcase.html), которые должны быть протестированы.

15)  Модель комплексного управління якістю програмного забезпечення (на базі ISO).

В качестве примера рассмотрим построение обобщенной модели качества информационной системы в виде 4-уровневой иерархической структуры показателей качества. Уровнями модели будут выступать:

• Факторы – первый уровень.

• Характеристики – второй уровень.

• Метрики – третий уровень.

• Оценочные элементы – четвертый уровень.

В простейшем варианте модели качества выделим таких три основных фактора, которые принадлежат самому верхнему уровню в иерархии структуры показателей качества:

• Программа и данные.

• Документация пользователя.

• Описание продукта.

Рассмотрим формирование требований собственно к программам и данным. По стандарту ISO/IEC 9126 необходимо определить свойства программного обеспечения по каждой из шести характеристик, а именно:

• Функциональность.

• Надежность.

• Используемость (удобство использования).

• Эффективность.

• Сопровождаемость.

• Мобильность.

Для каждой из шести характеристик необходимо обосновать и выбрать полный перечень метрик для построения модели качества системы. Например, характеристика “Функциональность” может быть описана такими метриками:

• Инсталляция.

• Наличие функций.

• Корректность.

• Совместимость внутренняя.

• Совместимость внешняя.

16)  Модель вимірювання характеристик якості програмного забезпечення.

Качество – это характе-ка кот поддается воздействию.

Характерика качества – отображает св-ва ПО по кот можно судить что оно качественое(по кот на него можно воздействовать).

Поскольку очень сложно измерить,доказать качество то вводят иерархические системы измерения качества.

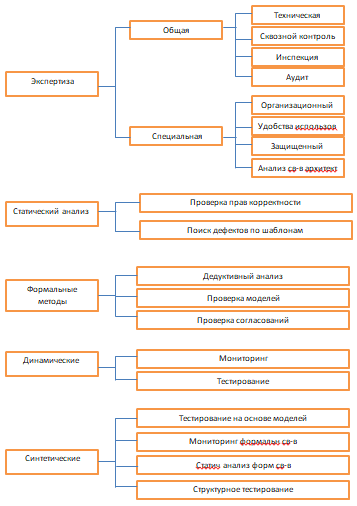
Каждый Программный Продукт описывается своей уникальной системой качества, а представление модели ISO явл общей.

Фактор качества – это свойства в той или иной степени описывающие качество ПО.

При оценке качесттва учитывается 2,3 фактораю Для численой оценки качества используют 1 или несколько критериев.

Критерий качества – это вычислимое выражение кот устанавливает растояния(интервал) по кот мы можем сделать вывод о качестве По с точки зрения заданого фактора.

17)  Класифікація методів верифікації.

  
18)  Мутаційні критерії вибору тестів.

В основе их применения – будем считать, что программист пишет с 1го раза почти правильный программный код. Назовем мутациями – мелкие ошибки. Мутанты – те программы, которые отличаются мутациями. Метод означает, что в разрабатываемой программном коде Р, намеренно вносят мутации, формируя набор программного кода с ошибками Р1, …,Рm. Если вес тестовые наборы заблокировали копии программного кода, то программа Р – протестирована.   
19)  Основні проблеми процесу тестування програмного забезпечення.

1. Верна ли версия компонент, используемая в программном продукте?
2. Доступны ли все файлы данных?
3. Являются ли корректными ссылки на эти файлы данных?
4. Сама система собр на правильн версии платформы, библиотеки и т.д.?
5. Правильная ли версия компилятора и сопутствующего программного обеспечения?

20)  Ролі в процесі веріфікації програмного забезпечення.

1 роль – Заказчик : имеет право менять требования лишь во взаимодействии с менеджером или лидером проекта.

2 роль – Менеджер проекта : обеспечивает коммуникационный канал между заказчиком и командой. Основная обязанность – получить требования.

3 роль – Менеджер ПО : управляет командой внутри проекта (коммуникатор). Отвечает за разработку функциональных спецификаций. Может их менять, распределять разработчикам задачи и отчитыв за этапы.

4 роль – Разработчик : исходный прог код

5 роль – Специалист по тестированию : разработка тест планов по тестированию.

6 роль – Специалист по контр качества: отвечает за альфа и бета тестирование.

7 роль – Специалист по верификации.

8 роль – Специалист по внедрению и сопровождению.

9 роль – Специалист по безопасности.

10 роль – Технический писатель.  
21)  Кількісні характеристики програмного забезпечення та його надійності.

**1) Вероятность безотказной работы***http://ok-t.ru/studopedia/baza14/101510417807.files/image156.jpg —*это вероятность того, что в пределах заданной наработки отказ системы не возникает.

http://ok-t.ru/studopedia/baza14/101510417807.files/image158.jpg

где http://ok-t.ru/studopedia/baza14/101510417807.files/image160.jpg - случайное время работы программно обес­печения до отказа; http://ok-t.ru/studopedia/baza14/101510417807.files/image162.jpg - заданная наработка.

**2) Вероятность отказа**— вероятность того, что в пределах заданной наработки отказ программной системы возникает.

http://ok-t.ru/studopedia/baza14/101510417807.files/image164.jpg

**3) Интенсивность отказов ПО системы***http://ok-t.ru/studopedia/baza14/101510417807.files/image166.jpg*— это условная плот­ность вероятности возникновения отказа программного обеспечения в определенный момент времени при усло­вии, что до этого времени отказ не возник.

http://ok-t.ru/studopedia/baza14/101510417807.files/image168.jpg

где http://ok-t.ru/studopedia/baza14/101510417807.files/image170.jpg — плотность вероятности отказа в момент времени *t.*

http://ok-t.ru/studopedia/baza14/101510417807.files/image172.jpg

Связь между http://ok-t.ru/studopedia/baza14/101510417807.files/image174.jpg определяется следующим соотношением:

http://ok-t.ru/studopedia/baza14/101510417807.files/image176.jpg

**Средняя наработка до отказа** http://ok-t.ru/studopedia/baza14/101510417807.files/image178.jpg — это математическое ожидание време­ни работы программного обеспечения АСОИУ до очередного отказа.

http://ok-t.ru/studopedia/baza14/101510417807.files/image180.jpg

где http://ok-t.ru/studopedia/baza14/101510417807.files/image182.jpg — время работы программного или информационного обеспечения http://ok-t.ru/studopedia/baza14/101510417807.files/image184.jpg

http://ok-t.ru/studopedia/baza14/101510417807.files/image186.jpg

где http://ok-t.ru/studopedia/baza14/101510417807.files/image188.jpg — время работы программного средства между отказами; i=1,2,..n – количество отказов.

**Среднее время восстановления** http://ok-t.ru/studopedia/baza14/101510417807.files/image190.jpg – это математическое ожидание времени восстановления http://ok-t.ru/studopedia/baza14/101510417807.files/image192.jpg , времени, затраченного на восстанов­ление и локализацию отказа http://ok-t.ru/studopedia/baza14/101510417807.files/image194.jpg , времени устранения отказа http://ok-t.ru/studopedia/baza14/101510417807.files/image196.jpg , времени пропускной проверки работоспособности http://ok-t.ru/studopedia/baza14/101510417807.files/image198.jpg :

http://ok-t.ru/studopedia/baza14/101510417807.files/image200.jpg

**Коэффициент готовности***http://ok-t.ru/studopedia/baza14/101510417807.files/image202.jpg*оценивается как вероятность того, что программное и информационное обеспечение АСОИУ будет нахо­диться в работоспособном состоянии в произвольный момент вре­мени его использования по назначению:

http://ok-t.ru/studopedia/baza14/101510417807.files/image204.jpg

22) Функціональні критерії вибору тестів.

Ф.К. – контролируют степень выполнения требований закащика к ПО. Ф.К. работает по модели *черного ящика*( неизвестно что внутри, манипуляции только со входами и выходами):

1. Тестирование пунктов спецификации( созд. Тест кот. Проверяет каждый пункт спецификации хотя бы 1 раз).
2. Тест-ние классов входных данных (проверить каждый класс не менее 1 раза).
3. Разработка тестовых наборов на осн классов эквивалентности.
4. Тестирование правил (в качестве правила рассматриваем соотв-е входных и выходных правил либо вводится спец-я грамматика).
5. Тест-е классов выходных данных.
6. Тест-е функций (это самый популярный критерий по кот мы создаем тестовые наборы, чтобы проверить хотя бы 1 раз любую из функций представленных на UML-диаграмме).

23) Класифікація програмних помилок.

Понятие надежности ПО базируется на понятии ошибка, дефект, сбой.

Отказ - это отклонение программы от функционирования или невозможность программы выполнять функции, определенные требованиями и ограничениями.

Сбой – кратковременный отказ.

Дефект – долговременный отказ.

Ошибка – 1) в ПО это неверный, неправильный перевод из одного представление в другое.

Суть представления – любая программа это трансформатор из исходных данных в понятие. Трансформация выполняется в 3 этапы 1) читающий механизм 2) печать 3) перенос информации.

Ошибка – 2) это искажение, неправильный перевод из 1 представление в др.

Сбой – 2) как правило возникает по причине аппаратного обеспечения.

Дефект – 2) следствие ошибки или группы ошибок.

24) Стохастичні критерії вибору тестів.

С.К. используют в случии стохастического тестирования. Стохастическое тестирование реализовано:

1. Разработать программу имитатор случайной последовательности, входных сигналов тестированного программного продукта.
2. Вычислить, независимым способом, значение выходных данных У кот соотв-ют Х. Т.о. мы получим тестовые наборы (Х, У).
3. Протестировать предложеные наборы.

Для контроля результата (процедуры Оракула) используют 2 метода:

1. Детерминированный контроль – простая проверка соотв полученого результата с тестовым набором.
2. Стохастический контроль – закон распределения выходных данных и закон распределения тестового набора совпадают.

Следовательно -> **сущ 2 критерия** на осн этой процедуры:

1. Cтатистический метод окончания тестирования

В осн лежит предположение о соблюдении гипотез закона распределения генерируемых данных и тест.набора.

1. Метод оценки скорости выявления ошибки. Этот критерий оценивает интервал времени между выявлениям текущей ошибки и последующей.

Формула вычисления время затрачиваемое на обнаружение N-ошибок:

Если tn+1> Td допустимого времени тестирования проекта, то тестирование заканчиваем, в противном случае продолжаем поиск ошибок.

25) Особливості інтеграційного тестування для об’єктно-орієнтовного програмування.

В соотв с ОО парадигмой карта вызовов будет существенно отличатся, это фиксированая диаграмма последовательности. Она строится после диаграммы классов, где вертикальные ячейки отображают сами классы, переходы означают вызовы методов различных классов.

Длина вертикальной линии – время выполнения метода.

В современом программном окружении ООП явл событийно управляемым. Передача управления внутри программы(объекта) выполняется не только через активный вызов, а еще через генерацию сообщений другим объектам.

Другая особеность – как таковое програмирование заменяется стандартом Look&Feel ( вызуальным связыванием объектов).

Для того что бы выполнить работу по тестированию необходимо выявить 2 – способа связи между объектами в тестир.иерархии.

1. Прямой вызов(на прямую вызыват 1-метод из другова – Р путь)
2. Обработка сообщений (ММ – путь)

Р-путь возникает в случии вызова командной строки, кот обрабатывает алгоритм и выгружается из памяти. При этом оно может создать ММ-путь.

26) Структурні критерії вибору тестів.

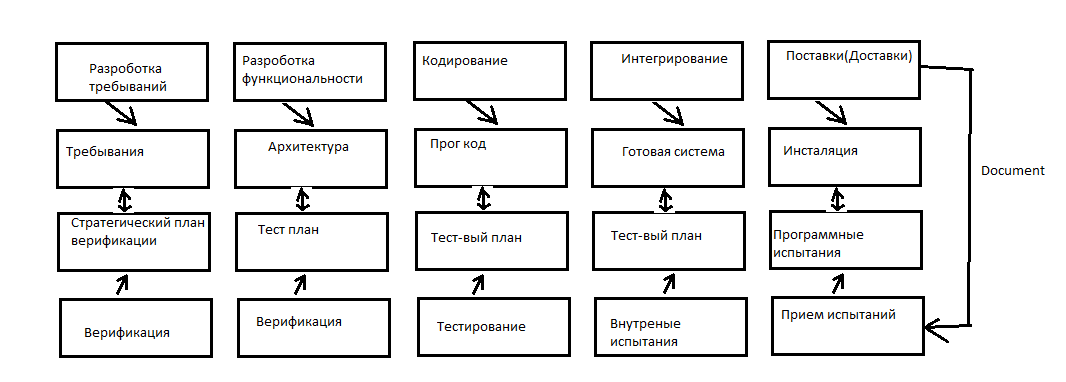
Базируется на идеи белого ящика (программный код доступен для тестировщика).

Сущ 3 осн критерия:

1. С0 – тестирование команд – это означает что необходимо создать множ.тестовых наборов. При выполнении кот каждый оператор срабатывает хотя бы 1 раз.
2. С1 – тестирование ветвей – создать набор тестов кот обеспечивает прохождения каждой ветки алгоритма минимум 1 раз.
3. С2 – тестирование путей – создать набор тестов обеспечивающих прохождения путей минимум 1 раз.

27) Документування в процесі верифікації.

Жизненный цикл



28) Визначення якості программного забезпечення (ISO, IEEE).

Качество ПО (по ISO) – 1) это полнота свойств и характеристик продукта, процеса, услуги, кот обеспечивает способность удовлетворять заявленным или подразумевающимся потребностям.

Качество ПО (по **IEEE)**– 2) это степень в которой ПО обладает требуемой комбинацией свойств ISO (factor, criteria, metrics, evaluated element).

Визначення цих характеристик і атрибутів за стандартом ISO 9126:2001:

1. Функціональність (functionality). Здатність ПЗ в певних умовах вирішувати задачі, потрібні користувачам. Визначає, що саме робить ПЗ, які задачі воно вирішує.
   1. suitability. Совместимость в смысле алгоритма.
   2. Точність (accuracy). Соответсвие между ф-ей и требываниями.
   3. Здатність до взаємодії (interoperability). Здатність взаємодіяти з потрібним набором інших систем.
   4. Відповідність стандартам і правилам (compliance).
   5. Захищеність (security).
2. Надійність (reliability).
   1. Зрелость надожности (maturity).
   2. Стійкість до відмов (fault tolerance).
   3. Здатність до відновлення (recoverability).
3. Зручність використання (usability) або практичність.
   1. Зрозумілість (understandability).
   2. Зручність навчання (learnability).
   3. Зручність роботи (operability).
   4. Привабливість (attractiveness).
4. Продуктивність (efficiency) або ефективність.
   1. Поведение во времени (time behaviour).
   2. Ефективність використання ресурсів (resource utilisation).
5. Зручність супроводу (maintainability).
   1. Аналізованість (analyzability) або зручність проведення аналізу.
   2. Зручність внесення змін (changeability).
   3. Стабільність (stability).
   4. Зручність перевірки (testability).
6. Переносимість (portability).
   1. Адаптованість (adaptability).
   2. Зручність установки (installability).
   3. Здатність до співіснування (coexistence).
   4. Зручність заміни (replaceability) іншого ПЗ даним.

1,2,3 – Разработчик

4,5,6 - Пользователь