УДК 004.415.2.045

DOI: 10.18372/2073-4751.82.20371

Райчев І.Е., к.т.н,
orcid.org/0000-0003-4058-1236,
e-mail: ihor.raichev@npp.kai.edu.ua

ТЕХНОЛОГІЯ ОЦІНЮВАННЯ ЯКОСТІ КРИТИЧНИХ ПРОГРАМНИХ СИСТЕМ НА БАЗІ ОНТОЛОГІЧНОГО МОДЕЛЮВАННЯ

Державний університет «Київський авіаційний інститут»

Вступ

Для остаточного оцінювання якості програмних систем (ПС) критичного призначення організації-розробники застосовують атестаційні або сертифікаційні випробування. В обох процедурах широко використовується процеси тестування. В сучасних умовах в Україні та у країнах ЄС здебільше практикується та проводиться сертифікація систем якості організацій-розробників, установ та випробувальних лабораторій на відповідність стандартам [1-3]. Значно рідше проводиться сертифікація власне програмних систем або інших програмних продуктів на відповідність висуненим початковим вимогам замовника і розробника [4, 5].

Однак нині суттєво зростає тенденція об'єктивного оцінювання вимог до якості кожної ПС, яка розробляється. Особливої важливості задача проведення сертифікаційних чи атестаційних випробувань і підсумкового оцінювання властивостей якості набуває для критичних ПС, які широко використовуються на транспорті, в енергетиці, в медицині, для моніторингу довкілля та в інших галузях і безпосередньо пов'язані з безпекою життєдіяльності об'єкта контролю. Для множини класів таких систем актуальною стає задача формування понять, методів і підходів до виконання перевірки ПС на відповідність початковим вимогам, тобто створення онтології предметної області, в межах якої функціонує ПС критичного призначення. Базовими складовими елементами онтології є вимоги до ПС цих класів та методи і засоби оцінювання атрибутів якості компонентів ПС на етапах їх життєвого циклу [6, 7].

У статті, як типовий приклад, розглянемо клас програмного забезпечення автоматизованих систем контролю польотів (ПЗ АСКП) літальних апаратів (ЛА), які є системами критичного призначення і тому потребують проходження сертифікації на відповідність вимогам. Перевірка на відповідність вимогам може відбуватись шляхом оцінювання досягнутого загального рівня якості ПЗ систем контролю, враховуючи те, що рівень якості кожного показника, який входить до уніфікованої моделі якості системи або ПЗ, запропонованої в міжнародному універсальному стандарті [8], має досягти визначеного наперед (у вимогах до системи) мінімально припустимого рівня. В разі, якщо множина таких обмежень щодо показників якості виконується, ПС можна сертифікувати або атестувати на відповідність висуненим до неї початковим вимогам замовника і розробника та міжнародних і галузевих стандартів.

З метою всебічного аналізу відповідності атрибутів системи висуненим вимогам побудуємо в межах домену застосування концептуальну онтологічну модель системи, на базі якої технологічно сформуємо множину об'єктів і базових функцій та методи оцінювання рівня якості системи на основі створених моделей якості.

Аналіз останніх досліджень і публікацій

В науковій роботі [9] наданий всебічний аналіз і створені базові засади технології розроблення систем критичного призначення з визначенням і врахуванням небезпек, що з'являються під час їх роботи в межах ПрО їх застосування. Для формалізації виявлення цих небезпек і ризиків слід

описати їх у вимогах до ПС, як пропонується в працях [10–13], а реалізація зв'язку вимог з компонентами архітектури ПЗ критичних систем (особливо в авіації) висвітлена у роботі [14]. Вищевказані напрацювання врахуємо під час створення онтології ПЗ АСКП з метою побудови множини вимог і втілення цих вимог у моделях якості.

В роботі [15] підданий аналізу функціонал інформаційної керуючої критичної системи та розробка її інтерфейсів, але аналізу якості не виконувалось. В роботі [16] виконаний огляд методів і моделей оцінки ПЗ в інформаційно-комунікаційних системах. У статті сформовано список критеріїв для сучасних методів та моделей, а також виконано порівняння їх за цими критеріями. У роботі [17] виконаний огляд підходів до вирішення проблеми забезпечення якості програмних продуктів в межах життєвого циклу їх реалізації, а також розглянуто застосування цих підходів на етапі тестування проєкту веб-сервісу «Інтернет-банкінг» на основі вдосконалення *SQA*-процесів в організації-розробнику.

У науковій праці [18] Грицюк зазначає, що якість ПЗ можна виразити адекватно тільки за допомогою структурованої системи характеристик та атрибутів, яку прийнято називати моделлю якості. В роботі була розроблена система комплексного оцінювання якості ПЗ на базі характеристик і підхарактеристик стандарту [8], яка дає можливість визначити стан його якості. Але у фокусі спрямування статті не взяті до уваги питання всебічного аналізу ПрО, де буде функціонувати ПС, а також питання створення відповідної системи знань, на основі якої, як зазначено в працях [19–21], виявляються функціональні і нефункціональні вимоги до ПС. Лише після цього переходять до формування моделей якості з подальшим оцінюванням рівня якості.

У роботі [22] виконаний аналіз проблеми покращення безпечності ПЗ і його захисту від витоків інформації і вторгнень хакерів. У праці [23] досліджені питання прогнозування якісних показників ПС на базі інтерпретаційного методу *DeepLIFT*. В статті розглянуті властивості ефективності, продуктивності та питання виявлення дефектів у процесі тестування з метою підвищення надійності ПС.

Таким чином, у розглянутих роботах [10–23] не проводилися дослідження методів і засобів оцінювання якості та побудови моделей якості ПС критичного призначення на основі попередньо сформованих вимог. Крім того, у досліджених працях не проводилися, з цією метою, онтологічні дослідження ПрО застосування критичних ПС.

Постановка проблеми та її актуальність

Польотна інформація (ПІ), що включає траєкторні параметри ЛА, а також інформацію про функціонування систем ЛА та дії екіпажу по його керуванню, є параметричною і, відповідно до вимог *ICAO*, має використовуватися для контролю стану ЛА і дій екіпажу. Інформація польоту обробляється по алгоритмах контролю на борті ЛА чи наземними системами після його посадки [24]. Обробка інформації, записаної бортовими реєстраторами (БР), є актуальною задачею, яка дозволяє забезпечувати безпеку польотів. У документах *ICAO* високо оцінюється інформація БР та рекомендується впроваджувати обробку ПІ з метою запобігання авіаційних подій, контролю дій екіпажу й поліпшення технічного обслуговування ЛА. В Україні оброблення польотної інформації всіма експлуатантами ЛА є обов'язковим [25; 26].

ПЗ класу автоматизованих систем контролю вирішує наступні загальні задачі:

відтворення параметричної інформації (візуалізація параметрів польоту ЛА);

контроль виходів параметрів об'єкта контролю за припустимі обмеження (допусковий контроль);

контроль якості функціонування ЛА, як об'єкта контролю;

підготовка градуювальних характеристик та фільтрація ПІ.

Залежно від призначення ПЗ АСКП ці задачі можуть вирішуватися як у режимі реального часу, так і після функціонування об’єкта контролю наземними системами обробки польотної інформації, яка є параметричною цифровою інформацією датчиків, що фіксується БР.

ПЗ систем цього класу складається з підсистеми відтворення параметричної інформації, підсистеми допускового контролю, підсистеми контролю якості функціонування об'єкта контролю (в нашому випадку – ЛА) і підсистеми градуювальних характеристик та фільтрації ПІ (рис. 1).

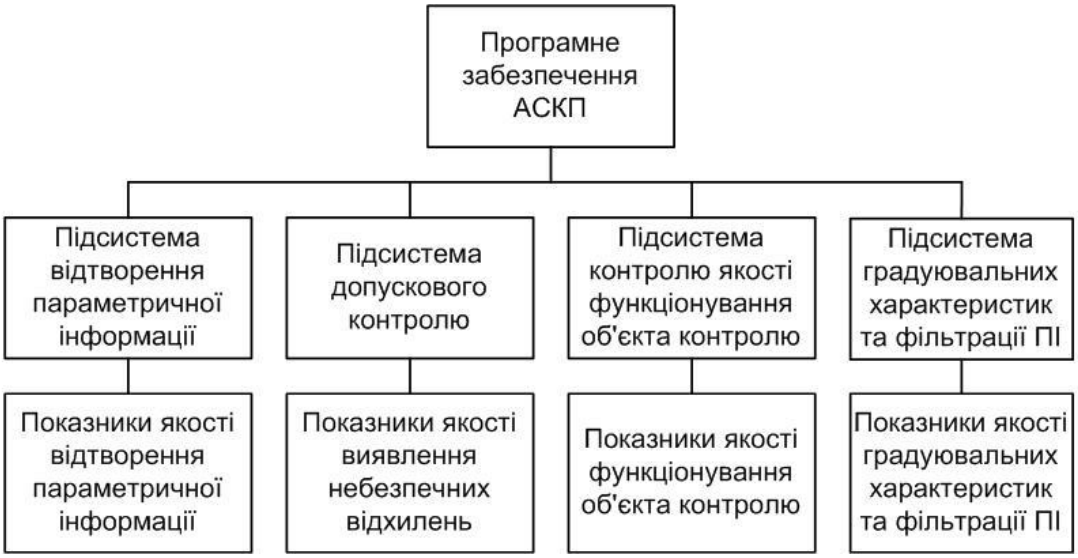

Рис. 1. Склад підсистем і класифікація показників якості ПЗ АСКП

Однією з головних є задача відтворення польотної інформації, яка полягає в графічному представленні зміни аналогових параметрів (АП) і разових команд (РК) у часі. Підсистема відтворення параметричної інформації присутня у будь-якій АСКП. Вона забезпечує автоматизовану обробку копії польоту з наступним формуванням графічної і табличної інформації параметрів польоту, а також візуалізацією траєкторії польоту ЛА на зовнішні дисплеї та графічні пристрої.

Основною проблемою для ПЗ АСКП, є вирішення задач допускового контролю. Відповідна підсистема повинна забезпечувати реалізацію алгоритмів контролю, встановлених для кожного типу ЛА. Підсистема характеризується ухваленням рішення про перебування ЛА в деякому стані. Для цього обчислюються деяка множина предикатів і встановлюється (чи ні) настання подій контролю. Істотною проблемою для підсистеми допускового контролю, є визначення вірогідності настання подій контролю й підтвердження факту перебування погрішності оцінки в межах допуску [27; 28].

Задача контролю якості виконання польоту полягає в здійсненні контролю за виконанням екіпажами ЛА режимів і правил льотної експлуатації з необхідним рівнем достовірності, що реалізує відповідна підсистема контролю якості функціонування об'єкта. Ця підсистема спирається на результати допускового контролю ЛА.

Підсистема градуювальних характеристик та фільтрації виконує задачі аналізу параметричної ПІ, видалення викидів, викривлень, шумів, що присутні в ній, та наближення ділянок спотвореної інформації бортових приладів і датчиків ЛА до достовірних значень з метою подальшої обробки цієї інформації іншими підсистемами.

Наслідки низької якості ПЗ АСКП та помилкові результати роботи базових підсистем, що оцінюють стан об'єкта контролю (рис. 1), можуть привести до катастрофічних наслідків [29; 30]. Дійсно, навіть якщо мова йде про наземні системи оброблення польотної інформації, то у випадку

невірної оцінки пілотування і роботи агрегатів та обладнання ЛА, існують ризики дозволити подальші польоти непідготовленому екіпажу чи борту ЛА, який має дефекти устаткування. Означені фактори можуть спричинити авіаційний інцидент, який може безпосередньо вплинути на безпеку життю людей, а також цілісність ЛА.

Тому проблема підвищення безпеки функціонування об'єктів, контрольованих за допомогою АСКП, є повсякчас актуальною [27; 28]. Одним із шляхів досягнення цієї мети є забезпечення високого рівня якості ПЗ АСКП і його надійного функціонування.

Метою статті є побудова методів і засобів створення онтологічної моделі компонентів ПЗ АСКП в межах ПрО її використання та ефективного застосування онтологічних схем для подальшої побудови моделей якості. Онтологічну модель використаємо для створення цільової моделі якості розробника, а також для побудови експлуатаційної моделі якості ПЗ АСКП.

Цільова модель якості розробника ПЗ відображає вимоги до програмної системи, а рівень якості характеристик цієї моделі має досягати, або перевищувати той рівень якості, що мається на меті для результуючого програмного продукту. Цільова якість встановлює необхідні значення якості для кожної з характеристик моделі шляхом подання цих значень у специфікаціях вимог до функцій ПС. Експлуатаційна модель якості (модель якості у використанні) є користувацькою якістю, а рівень її характеристик вимірюється в термінах результату використання ПС.

Для побудови моделей якості ПЗ АСКП скористаємося системою знань щодо ПрО їх використання, а для цього необхідно спочатку сформувати онтологію цих систем критичного призначення.

Доменний аналіз і модель онтології предметної області застосування програмних систем контролю польотів

На кожному етапі польоту ЛА необхідно контролювати значну кількість подій (алгоритмів) контролю одночасно, що є нетривіальною і досить складною задачею. Для вирішення цієї задачі пропонується використати онтологічну модель області застосування ПЗ КП, з врахуванням об'єктів і функцій (задач) онтології. Найбільш сучасним і наближеним до практичної реалізації ПС у заданій предметній області є підхід, який подає аналізовану предметну область (домен застосування ПС) у вигляді структурованої множини концептів (понять, термінів) на функціональному рівні абстракції. У межах домену формується така загальна концептуальна модель системи, яка забезпечує структурування знань, вибір способів подання цих знань, а також реалізацію пошуку функціональних алгоритмічних елементів ПрО, що безпосередньо закладає фундамент для подальшого технічного втілення ПС.

Доменний аналіз розпочнемо з розгляду та аналізу галузевого стандарту наземних систем автоматизованої обробки польотної інформації [24], що складаються з комплексів програм (підсистем), показаних на рис.1. Виділимо основні об'єкти онтології ПрО ПЗ АСКП, враховуючи положення стандарту [24], який встановлює загальні вимоги до характеристик таких систем.

Формальну модель онтології ПрО ПЗ АСКП подамо як впорядковану трійку скінченних множин:

$$\Omega_{ПЗАСКП} = \langle C, R, F \rangle, \qquad (1)$$

де C – скінченна непуста множина понять, концептів або термінів (концепти базуються на об'єктах ПрО), R – множина відношень між концептами ПрО, F – функції інтерпретації, що задані на поняттях і/або відношеннях онтології $\Omega_{ПЗАСКП}$.

Стандарт [24] встановлює вимоги до загальних характеристик (властивостей) компонентів довільних реалізацій ПЗ АСКП, причому системи цього класу, що задовольняють вимогам стандарту, можуть бути сертифіковані у встановленому порядку та допускаються до експлуатації в авіаційних підприємствах України. Терміни онтології задають і описують

сукупність базових об’єктів, які знаходяться у деяких відношеннях і взаємодіють між собою. Тому основні терміни *C* (поняття, концепти) онтології ПрО ПЗ АСКП будуть визначати об’єкти (або перелік чи сукупність об’єктів), які є загальними описовими артефактами концептуального подання вимог (під час проєктування та програмування вони можуть бути реалізовані у виді ієрархії класів контейнерного типу з відповідними атрибутами та методами).

З метою подальшого аналізу онтології ПЗ АСКП застосуємо стандарт онтологічного дослідження *IDEF*5 [31] та спеціальну схематичну графічну мову (*Schematic Language*, *SL*), призначену для представлення системи основних даних ПрО у формі онтологічної інформації. Схеми будь-якої онтології згідно стандарту *IDEF*5 мають задавати систему понять (множину базових об’єктів), їх класифікацію, композицію, взаємозв’язки та стани в процесі взаємодії. Аналізуючи [24–26], передусім побудуємо діаграму класифікації вимог до компонентів АСКП (рис.2).

Клас «Вимоги до переліку обов’язкових задач» підпорядкований класу «Вимоги до основних компонентів ПЗ АСКП». Він є найбільш вагомим з усіх (рис.2) і тісно пов’язаний з іншими базовими класами онтології (1), які безпосередньо залежать від нього.

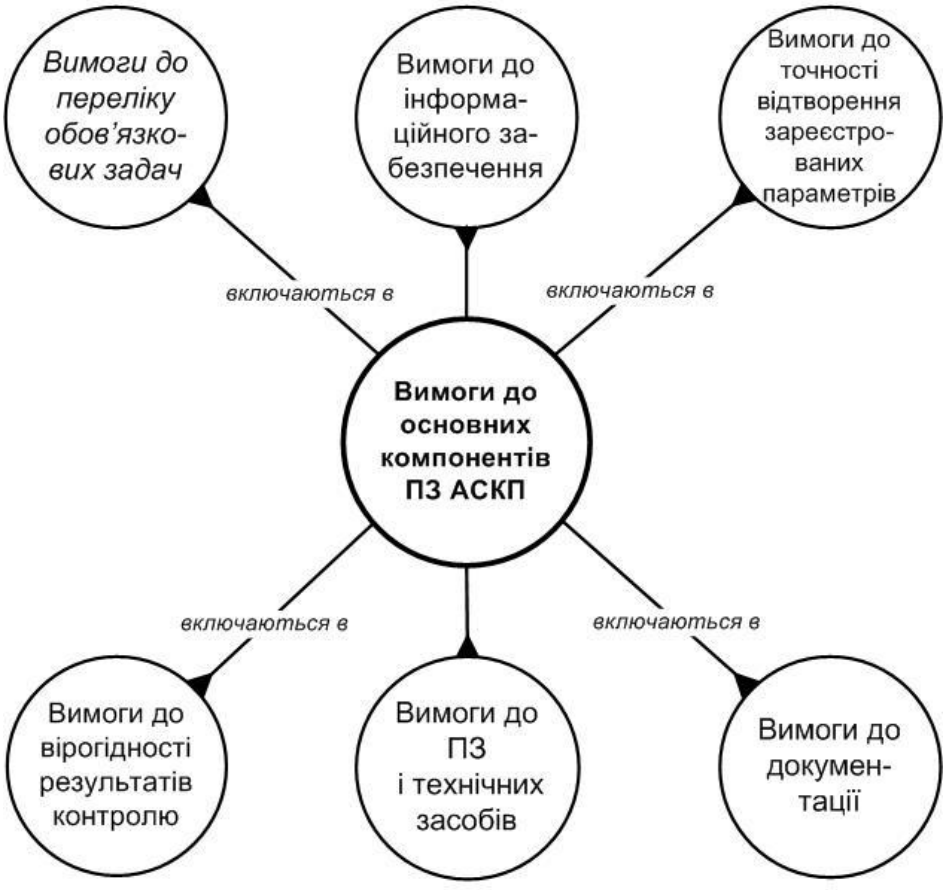

Рис. 2. Онтологія складових компонент вимог до ПЗ АСКП
(концептуальна схема класифікації вимог)

Тому композиційна схема класу «Вимоги до переліку обов’язкових задач» (рис.3) по суті є графічним поданням складу класів онтології $\Omega_{ПЗАСКП}$, де множина відношень між об’єктами *R* складається з відношень класифікації та взаємозв'язків узагальнення і агрегації. Композиційна схема вимог показана на рис.3 [30].

Рис. 3. Загальна онтологія вимог до переліку обов'язкових задач ПЗ АСКП (композиційна схема вимог)

Клас «Вимоги до переліку обов'язкових задач» є батьківським, в тому числі і для класу «Вимоги до відтворення зареєстрованої ПІ», який у свою чергу агрегує класи «Файл-копію ПІ» та «Опис екземпляру ЛА та опис аеропортів» (рис.3). Останній клас містить «Опис алгоритмів виявлення небезпечних відхилень в діях екіпажу і систем ЛА», де розміщуються відношення і зв'язки з класами подій контролю ЛА. Таким чином, множина алгоритмів контролю стає відомою і доступною класу «Вимоги до виявлення небезпечних відхилень у польоті ЛА».

Розглянемо ризики помилкової роботи основних комплексів ПЗ АСКП (рис.1). Комплекс програм відтворення ПІ вирішує задачу відтворення польотної інформації, яка полягає в графічному представленні зміни АП і РК у часі. В роботі комплексу існують небезпеки неточного обчислення фізичних значень АП і розбіжності результатів повторних обробок ПІ.

Комплекс програм допускового контролю вирішує задачі контролю допусків. Відповідне ПЗ має забезпечувати реалізацію всіх алгоритмів контролю, встановлених для даного типу ЛА, та характеризується ухваленням рішення про

перебування об'єкта контролю в тому чи іншому стані. Істотною проблемою для цього комплексу в задачах прийняття рішень є коректне визначення вірогідності настання подій контролю і підтвердження факту перебування погрішності оцінки в межах допуску, що безпосередньо впливає на прийняття рішення.

Комплекс програм контролю якості функціонування об'єкта вирішує задачу контролю якості виконання польоту, яка полягає в здійсненні контролю за виконанням екіпажами режимів і правил льотної експлуатації. У комплексі мають бути реалізовані алгоритми контролю в обсязі не меншому встановленого Генеральним конструктором кожного типу ЛА та наявна процедура підтвердження виявлених відхилень. Небезпеками для цього комплексу, як і для комплексу програм допускового контролю, є можливість неточного обчислення відповідними функціями помилок *I* та *II* роду, що також впливає на достовірність рішення.

Поняття небезпек і ризиків введемо до онтології (1) і побудуємо діаграму (схему) взаємозв'язків між вимогами і небезпеками їх недодержання для підсистем АСКП, яка показана на рис.4.

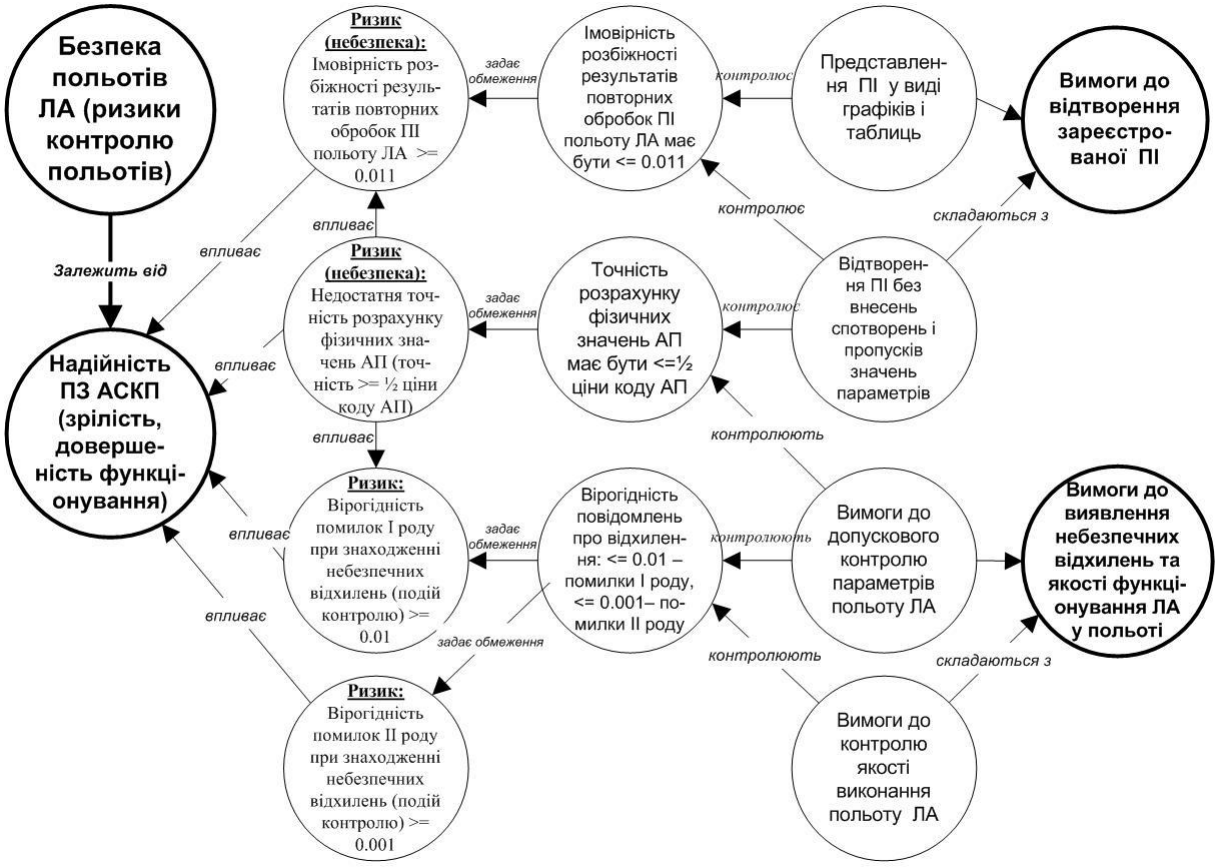

Рис. 4. Онтологія контролю польотів ЛА (схема взаємозв'язків вимог і небезпек та ризиків)

Функціями інтерпретації *F*, що задані на відношеннях онтології (1), для схеми з рис.4 слугують предикати кожного з алгоритмів контролю ЛА. Наприклад, для класу «Вимоги до допускового контролю параметрів польоту ЛА» (рис.4), одним із множини контрольованих алгоритмів є логічний вираз класу події контролю S073 , який означає "Перевищення максимальної експлуатаційної швидкості польоту" на етапі «політ згідно з маршрутом»:

$S073 = (7120 \le H_б \le 10300) \wedge (V_{пр} \ge 588)$, де $H_б$ – висота барометрична, $V_{пр}$ – швидкість приладова. Подібні функції інтерпретації (контроль допусків поблизу граничних

значень предикатів) мають охоплювати повну множину алгоритмів контролю для кожного типу ЛА.

З приведеного аналізу (див. рис.4) випливає, що в процесі побудови подібних класів інформаційних систем критичного призначення, в першу чергу необхідно застосовувати специфікації вимог до властивостей надійності та безпеки під час функціонування ПЗ контролю.

Формування специфікацій критеріїв і обмежень для задач прийняття рішення в системах критичного призначення

Перевірка повної відповідності програмного забезпечення специфікаціям узгоджених між замовником і розробником вимог вкрай необхідна для критичних систем, невідповідність яких вимогам призводить до небезпечних ситуацій. Вимоги до безпеки ПЗ критичних систем визначаються шляхом аналізу потенційних небезпек і ризиків, що можуть виникнути при роботі системи. На основі цього аналізу конкретизуємо вимоги до ПЗ таким чином, щоб або усунути ці небезпеки і ризики, або зменшити їхній вплив. Цю процедуру можна виконати, базуючись на концепції "безпечного" життєвого циклу ПЗ, що запропонована у стандарті *IEC* 61508 [32]. Парадигма безпечного життєвого циклу ПЗ критичних систем заснована на таких послідовних правилах: 1) аналіз властивостей ПрО системи і визначення функціональності ПС; 2) аналіз небезпек, відмов і ризиків для ПС; 3) розподіл вимог по функціях підсистем і специфікація вимог до нефункціональних характеристик якості безпека (свобода від ризиків) і надійність функціонування [8].

Аналіз небезпек і ризиків складається з всебічного аналізу системи і домену її використання, який проведено вище. В результаті були виявлені потенційні небезпеки і виконана класифікація небезпек і ризиків (рис.4). Після цього вибираються ті з них, які є потенційно найбільш небезпечними і ймовірними. Для небезпек, отриманих у результаті вибору, аналізуються можливі причини їхнього виникнення з подальшою побудовою дерева відмов і небезпечних помилок [9]. Після цього оцінюються ризики, пов'язані з виявленими небезпеками, які впливають на прийняття рішення про стан об'єкта контролю.

Коректне прийняття рішення про стан ЛА залежить від правильності функціонування ПЗ контролю. Для задачі прийняття рішення виконаємо аналіз механізмів попередження виникнення небезпек і зменшення імовірності ризиків. Підчас функціонування ПЗ контролю польотів множину небезпек і ризиків можна описати у виді неправильного визначення стану ЛА в контрольованих ситуаціях. З аналізу системи визначаємо, що потенційно серйозною небезпекою, що може виникнути через неякісне ПЗ, є помилкове визначення стану ЛА, як об'єкта контролю. При цьому можливі два варіанти помилкових рішень: $\alpha = S_i\left(\overline{x_i} \in X / x_i \in \overline{X}\right)$ і $\beta = S_i\left(\overline{x_i} \in \overline{X} / x_i \in X\right)$. Тут $\overline{x_i}$, x_i – дійсне й обчислене значення вектора контрольованих параметрів у момент часу t_i, X і $\overline{X}$ – припустима і неприпустима області значень, S_i – алгоритм *i*-ї події контролю польоту.

Оскільки ці рішення можуть реалізуватися з визначеною імовірністю, то, з огляду на технічні й економічні фактори, накладаються обмеження: $P(\alpha) \le \alpha_d$ і $P(\beta) \le \beta_d$. Тут α_d і β_d – досить малі граничні значення імовірностей подій. Описані рішення будемо трактувати як критерії з обмеженнями для ПЗ КП. Відзначимо, що ймовірності $P(\alpha)$ і $P(\beta)$ визначають помилки *I* і *II* роду, які можна використати в якості метрики атрибута "достовірність контролю", котрий можна віднести до характеристики функціональна придатність, підхарактеристики функціональна правильність, точність (модель якості системи і ПЗ [8]).

Зважаючи на онтологію контролю польотів (1), а також схему взаємозв'язків вимог і небезпек та ризиків (рис.4), узагальнимо суттєві небезпеки і ризики для АСКП, як компоненти небезпек функціонування для будь яких різновидів ПС

критичного призначення. При аналізі багатокритеріальних ситуацій контролю об'єкта будемо вважати, що повна вхідна область даних програми D компонується із сукупності повних вхідних областей параметрів D_h, що входять у формули алгоритмів контролю і є незалежними. Будь-який алгоритм контролю події являє собою загальний логічний вираз (сукупний предикат) P, який можна подати у досконалій кон'юнктивній нормальній формі (ДКНФ) виду: $P = P_1 \cdot P_2 \cdot \ldots \cdot P_h \cdot \ldots \cdot P_H$, де H – кількість предикатів у алгоритмі контролю ($h = \overline{1, H}$), а P_h – довільний предикат контролю.

Критерії прийняття рішення щодо події мають відповідати обмеженням і спираються на обчислене значення загального логічного виразу (сукупного предикату) алгоритму контролю (*true* – подія контролю відбулася, *false* – подія контролю не відбулася). При цьому для кожної змінної з кожного предикату, які входять у ДКНФ алгоритму контролю, під час його обчислення додатково проводиться аналіз і перевірка знаходження досить малих величин помилок *I* і *II* роду в припустимих межах (0.01 і 0.001), особливо зважаючи на знаходження кожної змінної предикату поблизу границь своїх класів еквівалентності, які утворюються на основі умов нерівностей чи рівностей у кожному предикаті.

Саме величини помилок *I* і *II* роду (ознака достовірності) приймемо за обмеження *L* для критеріїв прийняття рішення і будемо вважати *L* як ознаку обмеження для кожного критерія прийняття рішення, оскільки кожний критерій базується на значенні обчисленого предиката з врахуванням цих обмежень, а розраховані програмами значення обмежень безпосередньо впливають на прийняття остаточного рішення.

Зважаючи на отримані результати, а також на висновки праць [19; 20; 21; 33], вводимо до моделі онтології критерії з обмеженнями *L*. Тоді формула (1) набуває вигляду:

$$\Omega_{ПЗАСКП} = \langle \mathrm{C}, R, F, L \rangle \qquad (2)$$

Таким чином, концепти *C* розглядаються як об'єкти, що на нижньому рівні ієрархії утворюють класи подій контролю. Події контролю є неподільними об'єктами нижнього рівня, які містять назву події, опис події (на природній мові) і алгоритм контролю, причому кожний з цих алгоритмів представляє собою одну функцію інтерпретації з множини *F*. До того ж, для кожної функції інтерпретації існує критерій прийняття рішення, тобто $\forall F_i \in F \exists L_i \in L$. Обмеження у критерії визначає знаходження ЛА в «штатному режимі» (подія контролю не відбулася), або «не в штатному режимі» (подія контролю відбулася: відмови у роботі агрегатів і систем ЛА, чи порушення пілотування з боку екіпажу). Головною задачею АСКП є безпомилкове діагностування подій контролю польоту. Особливо важливим позитивним наслідком роботи систем є повне і достовірне виявлення небезпечних відхилень у роботі систем ЛА та діях екіпажу з врахуванням вірогідності помилок *I* і *II* роду, які мають бути в межах допусків (критерії відповідності обмеженням у задачах прийняття рішень онтології (2)).

Наприклад, клас «Опис алгоритмів виявлення небезпечних відхилень в діях екіпажу і систем ЛА» (рис.3) містить зв'язки з багатьма класами, що використовують події контролю ЛА, в тому числі з класом «Вимоги до виявлення небезпечних відхилень та якості функціонування ЛА у польоті» (рис.4). Події контролю, в свою чергу, мають відношення асоціації з усіма «зацікавленими» в них класами онтології (в тому числі з класом «Вимоги до допускового контролю параметрів польоту ЛА») і є неподільними об'єктами нижнього рівня ієрархії класів онтології (1) і (2). Обмеженнями для критеріїв задачі прийняття рішення по кожному з предикатів функції інтерпретації можуть бути: «Вірогідність повідомлень про відхилення: <= 0.01 – помилки *I* роду, <= 0.001– помилки *II* роду», «Точність розрахунку

фізичних значень АП повинна бути <=½ ціни коду АП» тощо.

Проведені в цьому напрямку дослідження виявили, що будь-який з предикатів алгоритмів контролю ЛА, тобто функцію інтерпретації з (2), можна формалізувати, використовуючи систему канонічних рівнянь скінченного автомата [34]. На основі цієї формалізації уніфікованим чином у праці [35] були побудовані логічні схеми автоматних моделей, які ефективно виявляють контрольовані небезпечні відхилення для даного типу ЛА шляхом побудови відповідних програм. Для врахування обмежень критеріїв прийняття рішень онтології (2) можна використати результати досліджень достовірності виявлення подій контролю, які були розглянуті в роботах [7; 36; 37].

Аналіз відмов, ризиків та небезпек функціонування критичних програмних систем

За допомогою аналізу польотної інформації вирішуються задачі контролю режимів польоту й перевірка виконання правил льотної експлуатації екіпажу літака, оцінюється працездатність агрегатів і систем ЛА та визначаються причини авіаційних інцидентів [25; 26]. ПЗ контролю польотів призначено для обробки параметричної польотної інформації, яка є складною структурованою багатоканальною інформацією і містить параметри польоту ЛА (висота, швидкість, положення рулів висоти, кут крену, кут тангажу, положення елеронів, кути відхилення ручок управління двигунами, оберти двигунів та багато інших), розпізнавальні дані (час, дата, номер борта, номер рейсу) та деяку контрольну інформацію. Копія польоту ЛА має складну організацію і характеризується циклічним повторенням у часі кадрів інформації (зі шпаруватістю, наприклад у 0.5 чи 1 секунду), структурною організацією каналів реєстрації усередині кадру, наявністю розпізнавальних даних. ПІ відбиває динаміку руху й стан систем ЛА на протязі польоту. З метою контролю за діями екіпажу й системами ЛА і проводиться після-польотна обробка ПІ за допомогою ПЗ контролю польотів.

Виконаємо аналіз відмов та інших ризиків і небезпек, які безпосередньо впливають на безпеку функціонування компонентів цих критичних ПС. Зважаючи на онтологію контролю польотів ЛА (2) та онтологічну схему взаємозв'язків вимог і небезпек та ризиків (рис.4), узагальнимо суттєві небезпеки і ризики для АСКП на рис.5.

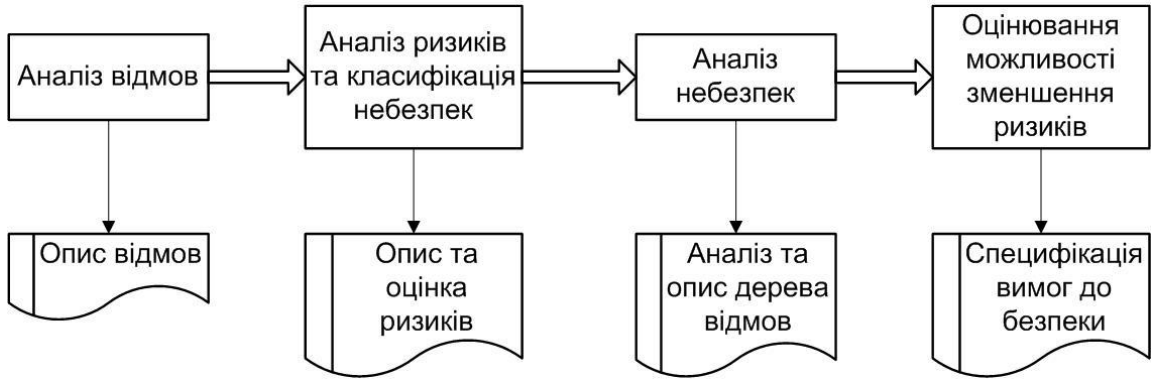

Рис. 5. Складові аналізу небезпек функціонування критичних програмних систем

Відмовами для систем контролю польотів будемо вважати низьку вірогідність виявлення небезпечних відхилень у процесі виконання польоту, а саме ситуації, коли ймовірність помилок *I* роду при знаходженні небезпечних відхилень (подій контролю) >=0.01, а ймовірність помилок *II* роду при знаходженні небезпечних відхилень >=0.001. Також неприпустимими є недостатня точність розрахунку фізичних значень АП (тобто точність >= ½ ціни коду АП) та ситуація, коли імовірність розбіжності результатів повторних обробок інформації польоту ЛА >= 0.011. Такі ситуації під час наземного контролю польоту провокують дозволи на подальші

польоти непідготовленому екіпажу чи борту ЛА, який має дефекти устаткування.

Аналіз ризиків настання відмов та класифікація небезпек, що спричиняють відмови, а також аналіз цих небезпек з описом дерева відмов дозволяють суттєво зменшити ризики і побудувати специфікації вимог до безпеки ПЗ АСКП. Беручи до уваги взаємозв'язки вимог до реалізації обов'язкових задач ПЗ АСКП та виконавши аналіз відповідних небезпек і ризиків (рис.3, рис.4 та рис.5), створимо класифікацію небезпек і ризиків для ПЗ контролю польотів (табл. 1).

Таблиця 1. Класифікація небезпек і ризиків для ПЗ контролю польотів

Види небезпек	Вірогідність небезпеки	Серйозність небезпеки	Ступінь ризику	Допустимість небезпеки
Вірогідність помилок *I* роду при фіксуванні небезпечних відхилень (подій контролю) >= 0.01	середня	середня	середній	мінімально припустима
Вірогідність помилок *II* роду при фіксуванні небезпечних відхилень (подій контролю) >= 0.001	середня	висока	високий	неприпустима
Імовірність розбіжності результатів повторних обробок ПІ польоту ЛА >= 0.011 (а має бути <= 0.011)	низька	середня	середній	мінімально припустима
Недостатня точність розрахунку фізичних значень АП (наявна точність є >= ½ ціни коду АП , а має бути <= ½ ціни коду АП)	середня	висока	високий	неприпустима
Відтворення ПІ із внесенням спотворень і пропусків значень параметрів (АП та РК)	середня	висока	високий	неприпустима

Дійсно, довільна подія контролю (алгоритм контролю) є неподільним елементарним об'єктом (класом), функція інтерпретації якого описується множиною предикатів. В кожному предикаті приймають участь параметри польоту ЛА. Настання (чи не настання) кожного з предикатів додатково контролюється функцією вірогідності контролю, тобто відсутністю помилок *I* і *II* роду в процесі оцінювання параметрів предикату. Тому операцій оцінки вірогідності для кожної з подій контролю (яких є декілька сотень) потрібно розраховувати від двох-трьох операцій до декількох десятків.

Через це небезпечні помилки під час функціонування АСКП виникають як прояв дефектів у ПЗ цих систем. Потенційно найбільш небезпечні та ймовірні небезпеки функціонування ПС окреслимо у виді дерева небезпечних помилок (рис.6).

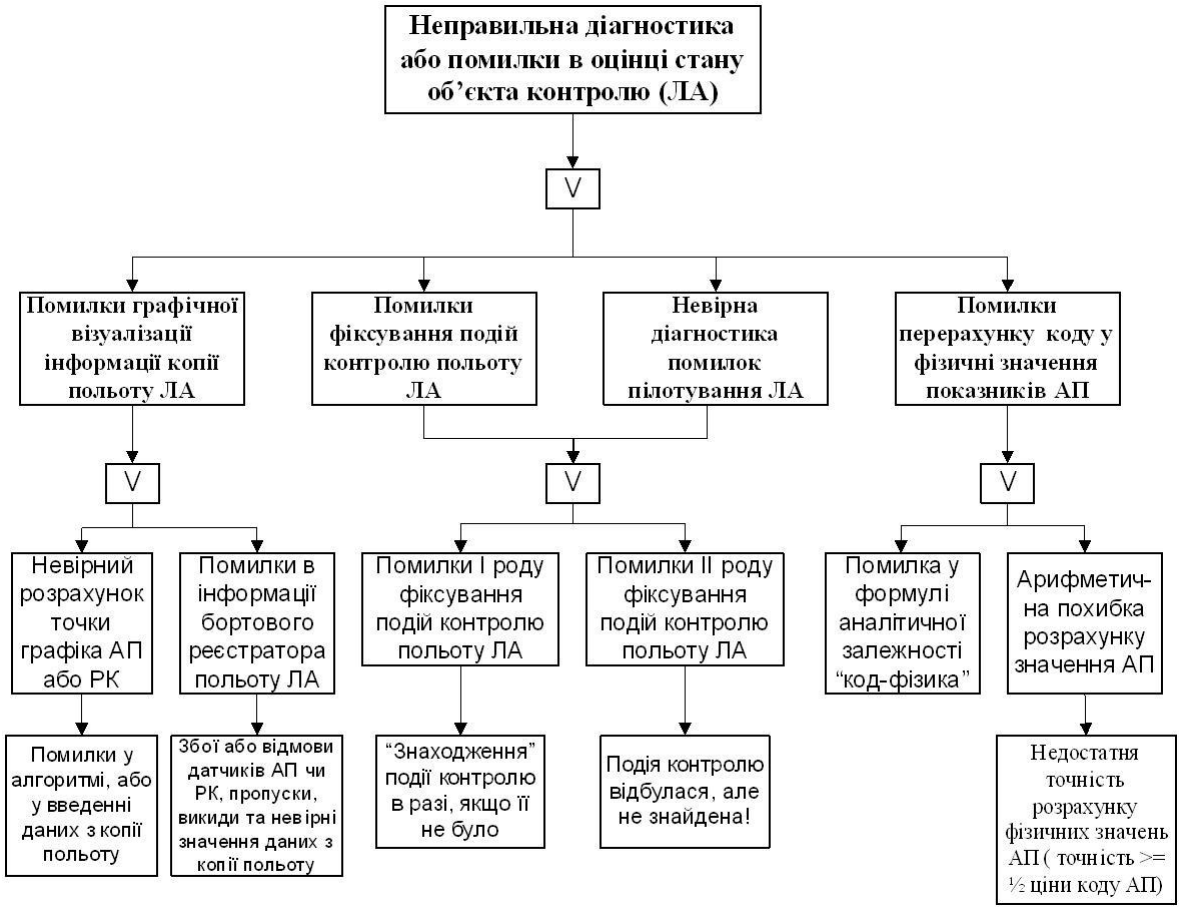

Рис. 6. Дерево небезпечних помилок програмних систем контролю польотів

Найважливішими остаточними критеріями якості для будь-яких ПЗ АСК є високі показники безпеки та надійності функціонування. Для наземних систем післяпольотного контролю безпека особливо залежить від коректності (точності) результатів функціонування цих критичних ПС, оскільки системи працюють незважаючи на плин реального часу, на відміну від систем контролю, що функціонують на борті ЛА. Загалом безпека залежить від прояву ризиків, вплив яких будемо оцінювати по наслідках функціонування ПС. Особливо важливими наслідками роботи ПС є повне, коректне, точне і достовірне виявлення небезпечних відхилень у роботі систем ЛА та діях екіпажу з врахуванням достовірності помилок *I* і *II* роду, які мають бути в межах допуску, що забезпечить безпомилкове діагностування подій контролю. Також необхідно досягти високої якості роботи підсистеми фільтрації для усунення пропусків та невірних значень даних параметрів з копії польоту [29].

Оцінювання можливості зменшення ризиків та подальшу специфікацію вимог до безпеки функціонування ПЗ АСК виконаємо у процесі аналізу та створення моделей якості критичних ПС на основі онтологічної моделі (2). Розглянемо використання цієї технології на прикладі побудови процедури оцінювання якості ПЗ АСКП.

Побудова моделей якості програмних систем критичного призначення

Основна специфікація вимог до безпеки функціонування ПЗ АСКП – це підвищення точності функціоналу виявлення небезпечних відхилень об'єкта контролю від штатних режимів, тобто надійне виявлення подій контролю, які відбулися на протязі поточного чи виконаного польоту. Таким чином, специфікації безпеки трансформуються у вимоги до якості базових функцій систем контролю польотів.

Тому необхідно будувати моделі якості ПС і проводити тестові випробування для оцінювання досягнення необхідного рівня якості базових функцій системи. Фактичний досягнутий рівень якості характеристик, що входять до моделі якості, дає відповідь на питання: чи відповідає та чи інша функція специфікаціям вимог до безпеки використання ПЗ АСКП. Отже, специфікації вимог до якісних властивостей функцій ПС є складовими безпеки використання АСКП.

Загалом моделі якості автоматизованих систем контролю необхідні для оцінювання рівня інтегральної якості цих критичних систем, який має досягати наперед визначеного значення. Тому під час сертифікації і подальшого допуску до експлуатації має бути задіяний механізм перевірки досягнення необхідного рівня якості характеристик таких систем. Перша модель якості – це цільова модель якості розробника ПЗ, яка використовується для інкорпорації в систему, що розробляється, визначених властивостей якості. Таким чином, необхідно залучити ці властивості в компоненти архітектури, коди програм, а також на етапі тестування оцінити рівень досягнутої якості цих властивостей. Друга модель якості – це модель експлуатанта, (користувацька модель), що призначена для оцінки задоволення потреб користувачів системи, в тому числі безпечності (свободи від ризиків) під час експлуатації.

Цільова модель якості акумулює у собі характеристики та підхарактеристики якості, які відповідають специфікаціям вимог до ПС, причому вимоги утворюються на базі онтологічного моделювання (онтологічної моделі).

Таким чином, на базі онтологічної моделі (2) та відповідних схем (рис.3 – рис.6) були побудовані вимоги до базових функцій ПЗ АСКП та враховані супутні небезпеки і ризики. Зараз на основі вимог до функцій ПС побудуємо цільову модель якості розробника, яка необхідна для проведення сертифікаційних випробувань систем критичного призначення на відповідність вимогам.

В галузевих стандартах і нормативних документах зафіксовані нормовані обмеження на властивості ПЗ, які є бажаними показниками якості для користувача. Оскільки більшість галузевих вимог нормовані, то цим задаються обмеження та інструкції для виміру й оцінки відповідних властивостей якості. Тому необхідно узгодити вимоги, побудовані на базі онтології (2), із характеристиками загальних стандартів якості та вирішити задачу відображення вимог галузевих стандартів і нормативних документів на уніфіковані показники стандарту якості [8].

В процесі оцінювання якості критичних систем отримуємо групу характеристик якості, що, як правило, неоднорідні за своєю природою. З цієї множини завжди можна виділити підмножину, яка містить показники якості, що безпосередньо впливають на оцінку цільового функціонального призначення системи (для АСКП – оцінювання стану об’єкта контролю). Такі показники будемо вважати критичними, а інші – другорядними. Критичні показники мають вирішальну вагу для оцінювання рівня цільової функціональності системи. Другорядні показники не впливають на оцінку цільового призначення системи, доки їх, у випадку потреби, не вводять до критичних характеристик. Критичні показники пов’язані з оцінкою функціонування об'єкта контролю і мають вирішальний вплив на якість ПЗ критичних систем. Формування набору критичних показників здійснюється у відповідності з наступними етапами:

Відображення вимог галузевих стандартів і нормативних документів з онтології (2) на множину уніфікованих показників якості загального стандарту [8].

Доповнення отриманої множини необхідними характеристиками якості із моделей загального стандарту [8], що не ввійшли до відображення.

Вибір з отриманої моделі якості тих характеристик, що пов’язані з оцінкою функціонування об'єкта контролю.

Якщо ввести до цільової сертифікаційної моделі якості всі характеристики та

під-характеристики, що рекомендовані в стандарті якості [8], то одержимо необґрунтовано трудомістку й вартісну процедуру їх перевірки. Тому побудована процедура не рекомендує включення в модель якості всіх показників, установлених стандартом [8]. Навпроти, експертам із лабораторії сертифікації рекомендується, враховуючи емпіричні критерії, розумно обмежити кількість характеристик і підхарактеристик якості при побудові моделі, не погіршуючи, однак, застосовності моделі й точності оцінки. Не слід, також, об'являти всі підхарактеристики критичними. З метою спрощення моделі пропонується, по-перше, ввести в модель критичні характеристики (надійність, безпеку, функціональність і відображення необхідних галузевих характеристик), а, по-друге – ввести другорядні некритичні характеристики, які впливають на загальний рівень якості.

Побудована в такий спосіб модель забезпечить належний рівень якості критичних систем цільового призначення, якими є АСК. Застосуємо запропонований метод (процедуру) для побудови моделі якості ПЗ АСКП, зважаючи на онтологію (2), модель якості стандарту [8], та перелік обов'язкових задач (рис.3). Модель якості продукту (системи або ПЗ) стандарту *ISO*/*IEC* 25010 складається з 8 характеристик і загалом 32 підхарактеристик якості. Базуючись на цій моделі побудуємо цільову модель якості:

Характеристика Функціональна придатність. Підхарактеристики функціональна повнота (1.1) і функціональна точність (1.2) є критичними, оскільки вони безпосередньо впливають на оцінку функціонування об'єкта контролю. Зауважимо, що узгодженість функціональної придатності з галузевими вимогами проводиться в обов'язковому порядку шляхом відображення показників вимог. Перші дві підхарактеристики (*functional completeness* (1.1) і *functional correctness* (1.2)) звичайно з'являються після відображення галузевих вимог онтології (2) і вимог користувача на множину властивостей якості стандарту *ISO*/*IEC* 25010 [8].

Характеристика Ефективність виконання. Не вводимо до моделі характеристику *Performance efficiency*, як таку, що не впливає на здатність наземних систем обробки польотної інформації до контролю польотів.

Характеристика Сумісність (*Compatibility*). Характеристику сумісність та її підхарактеристику інтероперабельність (*interoperability*) (3.2), тобто здатність до взаємодії з іншими авіаційними системами вводимо до моделі, як некритичну властивість бо вона не впливає на оцінку функціонування об'єкта контролю.

Характеристика Зручність використання (*Usability*). Здатність до вивчення (виучуваність) (4.2) вводимо до цільової моделі як некритичну підхарактеристику.

Характеристика Надійність (*Reliability*). Зрілість (завершеність, *maturity*) (5.1) – критична підхарактеристика, а відмовостійкість (5.3) і відновлюваність (5.4) можуть бути як критичними, так і ні. Це залежить від того, як використовується система: в режимі реального часу, або на землі після функціонування об'єкта. В останньому випадку ці дві підхарактеристики навіть не будемо вводити до моделі якості. Відмови ПЗ систем контролю безпосередньо впливають на безпеку об'єкта контролю тільки для систем реального часу, тобто для бортових систем ЛА. Але для наземних систем контролю польотної інформації підхарактеристики відмовостійкість (*fault tolerance*) і відновлюваність (*recoverability*) є неважливими, бо якщо в процесі роботи навіть виникає відмова (збій) – це не є критичним чинником для подальшої роботи системи (візуалізації ПІ та виявлення небезпечних відхилень) після усунення відмови.

Характеристика Захищеність (*Security*) можна опустити через те, що системи критичного призначення працюють переважно в автономному режимі у сеансі з навченим персоналом та експертами, а не із зовнішніми користувачами.

Характеристика Супроводжуваність (*Maintainability*) не включаємо до моделі, оскільки будь-яка модифікація системи

(зміна коду її компонентів) тягне за собою повторне проходження сертифікаційних випробувань для подальшого допуску системи контролю польотів до експлуатації.

Характеристика Мобільність (*Portability*). Адаптованість (8.1) і зручність установки (8.2) є другорядними підхарактеристиками, які теж уведемо до моделі.

Таким чином, на основі проведеного аналізу до цільової моделі якості розробника ПЗ АСКП обрано 5 характеристик і 7 підхарактеристик якості, як показано на рис.7. Характеристики і підхарактеристики мають номери і назви відповідно до загальної моделі якості універсального стандарту *ISO*/*IEC* 25010.

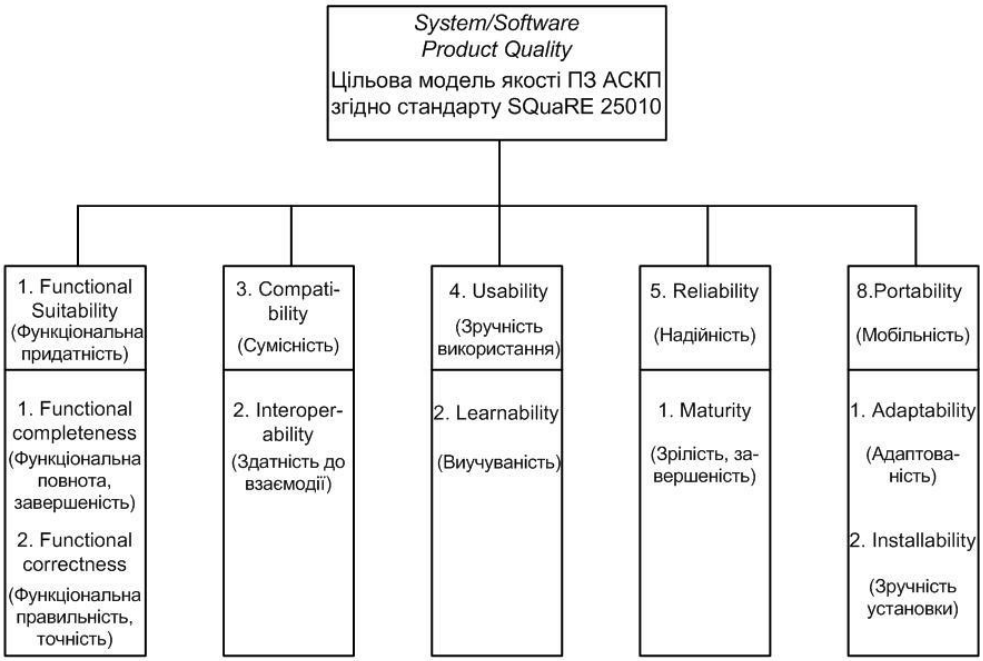

Рис. 7. Цільова модель якості ПЗ АСКП згідно стандарту *SQuaRE* 25010

Загальну ієрархічну модель якості ПЗ АСК опишемо у виді множини:

$$Q_G = \left\{C_i \left\{S_{ij} \left\{A_{ijk}(M_{ijk}, W_{ijk})\right\}_{k=1}^{K_{ij}}\right\}_{j=1}^{J_i}\right\}_{i=1}^{I}, \quad (3)$$

де C_i – і -та характеристика, S_{ij} – j -та підхарактеристика і -ї характеристики, A_{ijk} – k -й атрибут j -ї підхарактеристики і -ї характеристики якості, I – загальна кількість характеристик у моделі, J_i – загальна кількість підхарактеристик і -ї характеристики, K_{ij} – загальна кількість атрибутів j -ї підхарактеристики і -ї характеристики якості. Для того щоб модель (3) була завершеною, необхідно обрати метрики M_{ijk} вимірювання атрибутів підхарактеристик A_{ijk}, та відповідні вагові коефіцієнти W_{ijk}, які відображають рівень значущості кожного з атрибутів якості.

Не знижуючи рівня застосовності моделі (3), можна прийняти, що кожна підхарактеристика містить тільки один найважливіший атрибут. Тоді модель якості (3) можна спростити і привести до наступного вигляду:

$$Q_G = \left\{C_i \left\{S_{ij} \left\{A_{ij}(M_{ij}, W_{ij})\right\}_{j=1}^{J_i}\right\}_{i=1}^{I} \quad (4)$$

Врешті, з метою деталізації та наповнення моделі необхідно вирішити задачу визначення атрибутів підхарактеристик якості. Атрибути пропонується формувати на основі метрик тих підхарактеристик загальних стандартів якості *SQuaRE* [8; 38], які увійшли до моделі (4), і були отримані шляхом відображення вимог до переліку обов'язкових задач з об'єктів (класів) онтології (2), що створена на основі галузевих стандартів і нормативних документів

(див. онтологічні схеми на рис.2, рис.3, рис.4).

Отже, загальна цільова модель якості ПЗ АСКП приймає остаточний вигляд:

Функціональна придатність (*Functional suitability*). Для підхарактеристики функціональна повнота (1.1) сформуємо атрибут Функціональне покриття, який буде вимірюватися метрикою *Functional coverage* (п.8.2.1 стандарту [38]), причому повнота переліку обов'язкових задач системи контролю складається з 22 задач (див. рис.3). Функції, які вирішують ці задачі, мають бути наявні у системі в повному обсязі, тобто міра якості цього показника, обрахована згідно метрики, повинна прямувати до одиниці. Для підхарактеристики функціональна точність (1.2) визначимо атрибут Функціональна правильність з однойменною метрикою *Functional correctness* (п.8.2.2 стандарту [38]), причому з переліку 22-х задач перевірку на точність мають проходити 8 обов'язкових задач (див. рис.3). Міра якості цього показника, обрахована згідно метрики, повинна прямувати до одиниці, тобто всі 8 задач повинні мати саме той високий рівень точності, що встановлений у вимогах.

Сумісність (*Compatibility*). Для підхарактеристики інтероперабельність (3.2) визначимо атрибут Здатність до взаємодії, який вимірюється метрикою *External interface adequacy*, тобто Адекватність зовнішнього інтерфейсу з іншими, заданими у специфікаціях вимог, зовнішніми ПС (п.8.4.2 стандарту [38]). Міра якості цього показника має бути чим більшою, тим краще.

Зручність використання (*Usability*). Для підхарактеристики виучуваність (*learnability*) (4.2) уведемо атрибут Здатність до вивчення, який буде вимірюватися метрикою *User guidance completeness* (Повнота керівництв користувача) (п.8.5.2 стандарту [38]), що перевіряється за допомогою простої перевірки наявності *on-line* допомоги та повноти документації, достатньої для експлуатації системи, а також наявністю описів алгоритмів контролю. Міра якості показника має бути чим більшою, тим оцінюється краще.

Надійність (*Reliability*). Підхарактеристика зрілість (*maturity*) (5.1) позначає гарно протестоване зріле ПЗ, що не містить дефектів та надійно функціонує. Для підхарактеристики зрілість визначимо атрибут Свобода від дефектів у компонентах системи, який буде вимірюватися метрикою *Fault correction* (Виправлення помилок) (п.8.6.1 стандарту [38]). Ця метрика представляє собою відношення кількості виправлених помилок до загальної кількості виявлених помилок. Міра відношення переважно пов'язана саме з надійністю функціонування програмної системи і має прямувати до одиниці.

Мобільність (*Portability*). Для підхарактеристики адаптованість (*adaptability*) (8.1) уведемо однойменний атрибут Адаптованість, який вимірюється метрикою *Operational environment adaptability*, тобто Адаптованість до операційних середовищ (п.8.9.1 стандарту [38]). Міра якості цього показника має бути чим більшою, тим краще. Для підхарактеристики зручність установки (*installability*) (8.2) визначимо однойменний атрибут Зручність установки, який буде вимірюватися метрикою *Easy of installation*, тобто Полегшена інсталяція (п.8.9.2 стандарту [38]). Міра якості цього показника має бути чим більшою, тим оцінюється краще.

Таким чином, цільова модель якості містить 3 критичні підхарактеристики з 7. Модель якості у використанні ПЗ АСКП (модель якості експлуатанта) утворюється шляхом усвідомлення впливу кожної з властивостей якості побудованої цільової моделі на розгорнуту модель *Quality in use* стандарту [8], яка загалом містить п'ять характеристик і одинадцять підхарактеристик.

Необхідно взяти до уваги той факт, що критичні підхарактеристики функціональна повнота (1.1), функціональна точність (1.2) та зрілість (5.1) прямо вказують на потребу включити до експлуатаційної моделі АСКП наступні властивості:

Характеристика Ефективність. Підхарактеристика результативність (*effectiveness*) (1.1) – точність і завершеність, з якими експлуатанти досягають специфікованих цілей під час роботи. Підхарактеристика є критичною, тому що вона безпосередньо впливає на оцінку стану об'єкта контролю.

Характеристика Продуктивність. Підхарактеристику *efficiency* – ресурси, що витрачені для досягнення завершеності, з якими експлуатанти досягають специфікованих цілей – не включаємо до моделі через те, що продуктивність впливає на швидкість виконання, однак не впливає на результати контролю.

Характеристика Задоволеність (*Satisfaction*). Підхарактеристика довіра (*trust*) (3.2) – ступінь, у якому експлуатанти системи мають довіру, що система буде поводитися так, як визначено. Підхарактеристика не є критичною.

Характеристика Свобода від ризику. Підхарактеристика *Health and safety risk mitigation* (Зменшення ризику здоров'ю та безпеці людей) (4.2) – ступінь, у якому програмна система зменшує потенційний ризик для людей у контексті використання системи. Підхарактеристика є критичною.

Характеристику Охоплення контексту (*Context coverage*) не включаємо до моделі тому, що точність і повнота контролю та вимоги до безпеки польотів вже специфіковані контекстах використання.

Отже, експлуатаційна модель якості містить дві критичні підхарактеристики з трьох. Відзначимо, що функціональна повнота, точність і зрілість коду системи значно впливають на результативність роботи експлуатантів, на їх довіру до ПС та безперечно зменшують ризики безпеці екіпажу, пасажирів та ЛА у подальших польотах.

Дійсно, у більшості випадків дефекти (помилки) у ПЗ можуть не призводити до відмов (або збоїв) при функціонуванні ПЗ АСКП, але вони призводять до небезпечних помилок під час вирішення задачі контролю польотів, наприклад, до помилкового або невірного діагностування настання (чи не настання) небезпечних відхилень у польотах ЛА через помилки *I* і *II* роду, а також прийняття рішень щодо виходу (чи не виходу) параметрів польоту за межі заданих допусків. Такі помилки призводять до ризиків і небезпек (рис. 7), що прямо і безпосередньо впливають на надійність результатів роботи ПЗ АСКП, від яких залежить безпека подальших польотів ЛА і життя людей.

Атрибути моделі якості експлуатанта будемо формувати на основі метрик підхарактеристик стандартів якості *SQuaRE* [8; 39]. В результаті модель якості експлуатанта АСКП буде мати остаточний вигляд:

Ефективність. Для підхарактеристики результативність (*effectiveness*) (1.1) сформуємо атрибут однойменний підхарактеристиці – Результативність, який буде вимірюватися метрикою *Tasks completed* (п.8.2 стандарту [39]). Для цієї метрики повнота переліку обов'язкових задач системи контролю польотів складається з 22 задач онтології (2) (див. рис.3). Міра якості показника, обрахована згідно метрики, повинна прямувати до одиниці.

Характеристика Задоволеність. Для підхарактеристики довіра (*trust*) (3.2) визначимо атрибут Довіра експлуатантів, який вимірюється метрикою *User trust* (п.8.4.3 стандарту [39]). Якість вимірюється шляхом застосування анкетування. Міра якості цього показника має бути чим більшою, тим краще.

Характеристика Свобода від ризику (*Freedom from risk*). Для підхарактеристики Зменшення ризику здоров'ю та безпеці людей (4.2) визначимо атрибут Ризик безпеці людей (*Safety risk*). Метрикою атрибута оберемо *Safety of people affected by use of the system* (Безпека людей, на яку впливає використання системи) (п.8.5.3 стандарту [39]). Значення метрики залежить від кількості людей, які наражаються на небезпеку через використання ПС. Міра якості цього показника, обрахована згідно метрики, повинна прямувати до нуля, тоді рівень якості буде наближатися до одиниці.

Остання властивість є найбільш критичною в авіації, оскільки безпека подальших польотів ЛА значною мірою залежить від повноти виявлення подій контролю. Атрибут Ризик безпеці людей означає, що, в разі знаходження подій контролю, ризики життю людей в цих моментах виконаного польоту прямували до 100%. Тому, якщо це були помилки в діях екіпажу, то екіпаж повинен не допускатися до подальших польотів і проходити додаткове навчання на тренажерах. А якщо це були відмови в роботі агрегатів ЛА, то необхідно негайно проводити регламентні роботи на борту ЛА.

Після визначення всіх елементів цільової моделі якості (4) для систем критичного призначення можна переходити до сертифікаційних випробувань, у ході яких обчислюються фактичні значення атрибутів підхарактеристик якості. Для критичних атрибутів ці значення порівнюються з нормативними обмеженнями. Якщо отримані фактичні значення показників якості відповідають нормативним вимогам, то подальшу оцінку можна провести, використовуючи інтегральний показник якості, в якому вага кожного критичного показника має бути більше суми ваг другорядних.

Інтегральний показник якості можна застосувати для вибору кращого ПЗ із декількох конкуруючих, за умови врахування важливості критичних характеристик, вимоги до яких повинні виконуватися обов'язково. Але, оскільки в моделі є показники з різними метриками, такими, як неперервні числові, бальні, якісні та інші, необхідно попередньо провести узгодження та нормування метрик. Це можна зробити шляхом введення шкал для якісних та категорійних критеріїв і заданням вагових множників.

Крім того, можна здійснювати оцінювання досягнутої якості в процесі експлуатації АСКП шляхом виміру метрик атрибутів експлуатаційної моделі якості.

Диференціальний метод не може забезпечити одержання інтегральної оцінки якості ПЗ критичного призначення, оскільки він надає можливість оцінювати тільки окремі атрибути. Тому застосуємо комплексний метод оцінки рівня якості, що заснований на використанні узагальненого показника якості із залученням ранжування для оцінки ступеня задоволення вимогам [8; 28]. Метод полягає в тому, що для оцінки якості ПЗ використовується узагальнений показник якості U, що обчислюється як середній зважений арифметичний показник:

$$U = \sum_{i=1}^{N} Q_i W_i \quad , \qquad (5)$$

де Q_i – відносний показник якості, що визначається зі співвідношення $Q_i = \frac{P_i}{P_{ib}}$; P_i – рівень якості i-го елемента показника якості ($i = \overline{1,N}$); P_{ib} – базове значення i-го елемента; W_i – ваговий коефіцієнт (параметр значимості) i-го елемента показника якості. При використанні цього підходу пропонуємо задавати параметр значимості кожного критичного показника більшим, ніж сума вагових коефіцієнтів усіх другорядних показників. Базове значення P_{ib} можна прийняти рівним 1 для всіх показників, а рівень якості P_i пропонується остаточно обчислювати відповідно до відносної шкали і, якщо рівень якості є задовільним, то будемо застосовувати класифікаційну метрику, тобто в результаті рівень елемента може дорівнювати 0 (властивість відсутня), чи 1 (властивість присутня).

Для розрахунку узагальненого показника якості ПЗ АСКП $U_{ПЗАСКП}$ врахуємо формули (4) і (5). Для багаторівневої ієрархічної структури номенклатури показників якості розрахунок рівня якості ПЗ провадиться знизу наверх. Одержимо формулу (6):

$$U_{ПЗАСКП} = \sum_{i=1}^{I} W_i \sum_{j=1}^{J_i} W_{ij} \cdot Q_{ij} \quad , \qquad (6)$$

де I – кількість характеристик в моделі якості, J_i – кількість підхарактеристик i-ї характеристики якості, W_i – ваговий множник i-ї характеристики, W_{ij}– вага j-ї підхарактеристики i-ї характеристики якості,

Q_{ij} – досягнутий рівень якості ij-го атрибута якості.

Помітимо, що у процесі попередньої оцінки необхідно зафіксувати досягнення граничного задовільного рівня якості для кожного атрибута, щоб таким чином класифікувати наявність даної властивості.

Висновки

У статті наданий повний і детальний аналіз базових програмних комплексів, з яких складаються автоматизовані системи контролю. В якості прикладу були обрані програмні системи контролю польотів ЛА, які є типовими представниками цього класу.

На основі проведеного аналізу систем контролю польотів створена технологія оцінювання якості критичних програмних систем на базі онтологічного моделювання.

Отримані наступні результати:

Виконано всеосяжний доменний аналіз галузі застосування ПЗ контролю польотів і побудовано формальну модель онтології (2) для ПрО застосування АСКП.

Створено онтологію складових компонент вимог до ПЗ АСКП (схему класифікації вимог), загальну онтологію вимог до переліку обов'язкових задач ПЗ АСКП (композиційну схему вимог), та формалізовану онтологію контролю польотів ЛА (схема взаємозв’язків вимог до ПЗ АСКП та небезпек і ризиків).

У побудованій онтології (2) враховано повну множину понять, концептів і об’єктів ПрО використання, систематизовані й структуровані знання щодо об'єктів ПрО АСКП, а також визначені відношення і взаємозв'язки між об'єктами предметної області.

Виявлені функції інтерпретації для об'єктів онтології та визначені критерії і обмеження прийняття рішення про стан ЛА для функцій інтерпретації.

Враховані події контролю і ризики для об’єкта контролю (ЛА) та здійснений необхідний контроль на основі врахування ризиків з акцентом на критичних допусках.

На основі виявлення та узагальнення компонентів аналізу ризиків і небезпек функціонування програмних систем критичного призначення сформовані специфікації вимог до надійності й безпеки АСКП.

Створено класифікацію ризиків і небезпек для ПЗ АСКП, причому потенційно найбільш небезпечні та ймовірні небезпеки функціонування систем контролю польотів подані у виді дерева небезпечних помилок, що виникають через прояв дефектів у ПЗ.

Розроблено процедуру зменшення ризиків шляхом подальшої специфікації вимог до безпеки функціонування ПЗ АСК у процесі аналізу та створення загальної цільової моделі якості (4) та експлуатаційної моделі якості систем контролю.

Створені правила формування набору критичних показників, наявність яких є обов’язковою для моделі якості систем критичного призначення.

Зважаючи на модель якості із [8], а також загальну онтологію (2) та вимоги до переліку обов'язкових задач (рис.3, рис.4), виконано відображення вимог на властивості, що увійшли до цільової моделі якості.

Одержано цільову модель і модель якості експлуатанта для заданої ПрО та побудовано методологію оцінювання інтегрального рівня якості ПЗ контролю (6).

Моделі якості систем критичного призначення визначають та надають інструментальні засоби для оцінювання рівня зрілості коду (надійність), повноти і точності функцій системи (функціональна придатність) та безпечності (свободи від ризиків) як найважливіших властивостей якості критичних систем. На основі коректного вирішення задачі прийняття рішення про стан ЛА та за рахунок редукції ризиків досягаються високі показники функціональної придатності, надійності і безпеки функціонування систем контролю польотів.

Побудовані моделі якості можуть бути успішно використані для проведення подальшої атестації, а також сертифікації систем контролю, яка є обов’язковою

процедурою для класів систем критичного призначення.

Створені моделі якості та онтологічна модель з її функціями інтерпретації можуть бути застосовані для розроблення ПС контролю будь-яких типів, оскільки інформаційні системи контролю характеризуються наявністю об'єкта контролю, який контролюється сукупністю параметрів, що вимірюються за допомогою вимірювальних приладів. Системи цього класу завжди працюють із задачами і подіями контролю, які формуються аналогічно поданим у статті.

Перспективи подальших досліджень

Розроблені у статті методи та засоби досить легко модифікувати, адаптувати і використати в інших споріднених областях застосування, особливо у ПрО, де функціонують критичні ПС, для яких стан об'єкта контролю оцінюється на основі параметричної інформації датчиків або вимірювальних приладів (авіація, енергетика, медицина, довкілля, транспорт тощо).

З метою удосконалення та підвищення ефективності технології оцінювання якості критичних програмних систем плануються більш глибокі дослідження інтегрального оцінювання рівня якості ПС, особливо в частині нормування і нормалізації метрик атрибутів якості з метою їх уніфікації.

Література

1. ДСТУ ISO 9000:2001. Системи управління якістю. Основні положення та словник. [Чинний від 2001–07–01]. Київ: Держстандарт України, 2001.

2. ДСТУ ISO 9001:2001. Системи управління якістю. Вимоги: (ISO 9001:2000). [Чинний від 2001–06–27]. Київ: Держстандарт України, 2001. 23 с.

3. ISO/IEC 17025:1999. General Requirements for the Competence of Testing and Calibration Laboratories.

4. ДСТУ 2462:1994. Сертифікація. Основні поняття. Терміни та визначення. [Чинний від 1995–01–01]. Київ: Держстандарт України, 1994. 27 с.

5. ДСТУ 2844:1994. Програмні засоби ЕОМ. Забезпечення якості. Терміни та визначення. [Чинний від 1996–01–01]. Київ: Держстандарт України, 1995. 15 с.

6. IEEE Std. 830-1993. Recommended Practice for Software Requirements Specification. 1993. 36 p.

7. Raichev I. E., Kharchenko A. G., Egorov O. A. The Features of Testing Critical Program Systems While Their Certification. *Journal of Automation and Information Sciences*. 2011. Vol. 43, iss. 4. P. 35–44.

8. ISO/IEC 25010:2011. Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – System and software Quality models. 2011. 34 p.

9. Sommerville I. Software Engineering. 10th ed. Pearson India Education Services, 2017. 808 p.

10. Bernstein M. E., Braude E. J. Software Engineering: Modern Approaches. 2nd ed. Waveland Press, Inc., 2016. 782 p.

11. Wiegers K., Beatty J.. Software Requirements (Developer Best Practices). 3rd ed. Microsoft Press, 2013. 672 p.

12. Hockanson K., Wiegers K. Software Requirements Essentials: Core Practices for Successful Business Analysis. Longman (Pearson Education), 2023. 651 p.

13. Dick J., Hull E., Jackson K. Requirements Engineering. 4th ed. Cham : Springer, 2017. 239 p.

14. Bass L., Clements P., Kazman R. Software Architecture in Practice. 4th ed. Addison – Wesley (SEI Series in Software Engineering), 2021. 464 p.

15. Куваєв В. та ін. Розробка інтерфейсу оператора складних інформаційно-керуючих систем критичних до режиму реального часу. *Information Technology: Computer Science, Software Engineering and Cyber Security*. 2023. Вип. 1. С. 50–57. DOI: 10.32782/IT/2023-1-7.

16. Гамрецький Р. М., Гнатюк В. О. Огляд та аналіз методів та моделей оцінки якості програмного забезпечення в інформаційно-комунікаційних системах. *Наукоємні технології*. 2024. №4(64). С.435–448.

17. Грицюк П. Ю., Іванишин А. В., Грицюк Ю. І. Забезпечення якості програмного продукту за стандартом IEEE 730-2014 в межах життєвого циклу реалізації проєкту. *Науковий вісник НЛТУ України*. 2023. Т. 33, №2. С.101–117.

18. Грицюк Ю. І. Система комплексного оцінювання якості програмного забезпечення. *Науковий вісник НЛТУ України*. 2022. Т. 32, №2. С.81–95.

19. Буров Є. В., Пасічник В. В. Програмні системи на базі онтологічних моделей задач. *Вісник Національного університету "Львівська політехніка"*. 2015. № 829. С.36–57.

20. Буров Є. В. Ефективність застосування онтологічних моделей для побудови програмних систем. *Математичні машини і системи*. 2013. № 1.С. 44–55.

21. Карпов І. А., Буров Є. В. Використання онтологічних мереж у системах підтримки прийняття рішень в умовах неоднозначності. *Інформаційні системи та мережі*. 2020. № 7. С.8–15.

22. Коваленко А.А. та ін. Огляд методів аналізу безпечного програмного забезпечення. *Системи управління, навігації та зв'язку*. 2025. № 1. С. 156–161. DOI: 10.26906/SUNZ.2025.1.156-161.

23. Шантир А., Зінченко О. Прогнозування показників якості програмних систем із застосуванням модифікацій інтерпретаційного методу DeepLIFT. *Сучасний стан наукових досліджень та технологій в промисловості*. 2024. №4(30). С.110–124. DOI: 10.30837/2522-9818.2024.4.110.

24. ДСТУ 3275:1995. Системи автоматизованого оброблення польотної інформації наземні. Загальні вимоги. [Чинний від 1996–07–01]. Київ: Держстандарт України, 1996. 7 с.

25. Звід авіаційних правил України. Порядок збирання та практичного використання інформації бортових систем реєстрації на підприємствах цивільної авіації України. АПУ–3. Експлуатація повітряних суден. Введено в дію наказом Міністерства транспорту України від 02.12.1996 № 386. Київ, 1996. 110 с.

26. Програма перевірки відповідності програмного забезпечення контролю польоту вимогам ДСТУ 3275–95 і «Порядку збирання та практичного використання інформації бортових систем реєстрації на підприємствах цивільної авіації України». Київ: Державний департамент авіаційного транспорту України, 1997. 11 с.

27. Райчев І. Е. Проблеми сертифікації програмного забезпечення автоматизованих систем контролю. *Вісник НАУ*.2004. №1. С. 23–28.

28. Райчев І. Е., Харченко О. Г. Концепція побудови сертифікаційної моделі якості програмних систем. *Проблеми програмування*. 2006. №2-3. С. 275–281.

29. Райчев І.Е. та ін. Оцінювання якості програмного забезпечення фільтрації цифрового сигналу в реальному часі для систем критичного призначення. *Наукоємні технології*. 2021. №1(49). С.23–32.

30. Райчев І. Е., Харченко О. Г., Василенко В. А. Визначення вимог до програмних систем критичного призначення з використанням засобів доменного аналізу. *Моделювання та інформаційні технології*: зб. наук. пр. 2019. Вип.87. С.41–48.

31. Ontology Description Capture Method. URL: http://www.idef.com/idef5-ontology-description-capture-method/ (date of access 30.06.2025).

32. IEC 61508:2010. Functional Safety of electrical/electronic/programmable electronic safety-related systems. Geneva: International Electrotechnical Commission, 2010.

33. Карпов І. А., Буров Є. В. Онтології у процесі прийняття рішень. *Вісник Хмельницького національного університету*. 2023. Т. 1, №2(319). С. 149–153.

34. Райчев І. Е. Синтез автоматних моделей контролю. *Вісник НАУ*. 2002. № 2. С.43–52.

35. Райчев І. Е., Харченко О. Г. Конструювання програм створення тестових наборів даних на базі автоматних моделей. *Математичні машини і системи*. 2006. № 3. С.127–136.

36. Райчев І. Е. Технологія визначення показників вірогідності одновимірних та багатовимірних об'єктів контролю

за інформацією параметричних бортових реєстраторів. *Вісник НАУ*. 2002. № 1. С.17–24.

37. Райчев І. Е. та ін. Автоматизація визначення показників вірогідності об'єктів контролю при наявності разової команди. *Вісник НАУ*. 2002. № 3. С.73–78.

38. ISO/IEC 25023:2016. Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) – Measurement of system and software Product Quality. 2016. 45 p.

39. ISO/IEC 25022:2016. Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) – Measurement of Quality in Use. 2016. 41 p.

Райчев І.Е.

ТЕХНОЛОГІЯ ОЦІНЮВАННЯ ЯКОСТІ КРИТИЧНИХ ПРОГРАМНИХ СИСТЕМ НА БАЗІ ОНТОЛОГІЧНОГО МОДЕЛЮВАННЯ

У статті досліджено проблему виявлення та аналізу вимог до програмних систем критичного призначення. Для множини класів критичних систем актуальною є задача формування методів виконання перевірки цих систем на відповідність висуненим вимогам в межах предметної області застосування та аналіз ризиків і небезпек в їх життєвому циклі. Оцінювання відповідності вимогам, як правило, виконується шляхом оцінювання на етапі тестування досягнутого загального рівня якості компонентів програмного забезпечення контролю польотів. З метою всебічного аналізу відповідності атрибутів системи висуненим вимогам необхідно дослідити і структурувати значну кількість об'єктів та функцій. Для вирішення задачі систематизації в межах домену застосування запропоновано побудувати формальну концептуальну модель системи, на базі якої технологічно сформувати множину об'єктів і базових функцій та моделі якості для оцінювання рівня якості системи.

Проблема підвищення безпеки функціонування об'єктів, контрольованих за допомогою автоматизованих систем контролю польотів, є повсякчас актуальною. Одним із шляхів досягнення цієї мети є забезпечення якісного й надійного функціонування програмних систем контролю польотів, що особливо важливо під час експлуатації підсистеми контролю допусків, яка має забезпечувати повну реалізацію алгоритмів контролю, встановлених для кожного типу літального апарату. У випадку невірної оцінки пілотування і роботи агрегатів та обладнання, існують ризики дозволити подальші польоти непідготовленому екіпажу чи борту літака, який має дефекти устаткування, що може спричинити авіаційний інцидент, який прямо впливає на безпеку життю людей, а також на цілісність літального апарату.

Шляхом вирішення проблеми є ефективне застосування онтологічної моделі компонентів програмних систем контролю польотів для створення системи знань предметної області автоматизованих систем контролю польотів. У статті проведено аналіз останніх досліджень і публікацій, де показана ефективність застосування онтології для реалізації процесу прийняття рішень в контексті проблемних ситуацій неоднозначності. Для систем ПЗ контролю польотів можна ефективно використати апарат онтологічних досліджень, бо основною задачею ПЗ є прийняття рішення про надходження об'єкта контролю під час польоту в стані «в межах допуску» (штатний режим), або «за межами допуску».

Розроблена онтологічна модель визначає склад, класифікацію, структуру і взаємозв'язок вимог та ризиків і формує технологічну процедуру створення моделі якості критичних програмних систем та концепцію оцінювання її характеристик і атрибутів. Онтологічні дослідження та створена онтологія прямо вказують на ті властивості якості, які потрібно включити до моделей якості та надають засоби побудови моделей

якості: 1) цільової моделі якості для розробника системи контролю польотів; 2) моделі якості у використанні для експлуатанта літального апарату.

Проведені дослідження включають у себе: 1) виконання доменного аналізу області застосування; 2) створення онтології програмного забезпечення контролю польотів, яка систематизує і структурує знання щодо понять і об'єктів предметної області; 3)формування функцій інтерпретації онтології, а також специфікацій критеріїв та обмежень для задач прийняття рішень в системах критичного призначення; 4) формування специфікацій вимог до надійності й безпеки систем контролю польотів на основі виявлення та узагальнення компонентів аналізу ризиків і небезпек функціонування критичних програмних систем; 5)побудову цільової моделі й експлуатаційної моделі якості для заданої предметної області та створення методології оцінювання інтегрального рівня якості ПЗ контролю польотів.

У висновках зазначено, що побудована онтологічна модель та моделі якості можуть бути застосовані у життєвому циклі різних класів програмних систем контролю (в тому числі для атестації та сертифікації), оскільки будь-які інформаційні системи контролю характеризуються наявністю об'єкта контролю, що контролюється сукупністю параметрів, які вимірюються за допомогою параметричної інформації вимірювальних приладів. Отримані результати також можуть бути застосовані розробниками для створення власної системи управління якістю будь-яких програмних систем контролю в різних предметних галузях.

Подальші дослідження пропонується проводити у напрямку проведення більш глибокого аналізу технології інтегрального оцінювання рівня якості ПС, особливо в частині нормування і нормалізації метрик атрибутів якості з метою їх уніфікації.

Ключові слова: *критичні програмні системи, онтологія, програмне забезпечення, контроль польотів, об'єкти, функції інтерпретації, задачі прийняття рішення, критерії та обмеження, якість, вимоги до якості програм, вимоги до безпеки, вимоги до функціональності, вимоги до надійності, моделі якості систем критичного призначення, зменшення ризиків контролю польотів, сертифікація, тестування.*

Raichev I.E.

TECHNOLOGY OF QUALITY ASSESSMENT OF CRITICAL SOFTWARE SYSTEMS BASED ON ONTOLOGICAL MODELING

The article investigates the problem of identifying and analyzing the requirements for program systems of critical purpose. For a variety of mission-critical system classes, the task of developing methods for verifying these systems for compliance with the specified requirements within the subject domain and analyzing risks and hazards throughout their life cycle is relevant. Compliance assessment is typically performed by evaluating the overall quality level of flight control software components during the testing phase. To comprehensively analyze the compliance of system attributes with the specified requirements, it is necessary to examine and structure a significant number of objects and functions. To address the problem of systematization within the subject domain, it is proposed to build a formal conceptual model of the system, based on which a set of objects, basic functions, and a quality model to assess the quality level of the system can be technologically formed.

The problem of improving the safety of the operation of objects controlled with automated flight control systems is still relevant. One way to achieve this goal is to ensure the quality and reliable functioning of the flight control systems, which is especially important during the operation of the tolerance control subsystem, which should ensure the complete implementation of control algorithms established for each type of aircraft. In the case of incorrect piloting and operation of units and equipment, there are risks to allow further flights to an unprepared crew

or board of the aircraft, which has defects of equipment, which can cause an aviation incident that directly affects the safety of people's lives, as well as the integrity of the aircraft.

The way to solving the problem is the effective use of the ontological model of components of the flight control software systems to create a system of knowledge of the subject area of automated flight control systems. The article analyzes recent research and publications, which shows the effectiveness of using ontology to implement the decision-making process in the context of problematic ambiguity situations. For flight control systems, ontological research apparatus can be effectively used, as the main task of the software is to decide on the receipt of the control object during the flight in the state "within the admission" (regular regime) or "beyond tolerance".

The developed ontological model determines the composition, classification, structure and interconnection of requirements and risks and can forms a technological procedure for creating a quality model of critical PS and the concept of evaluating its characteristics and attributes. Ontological studies and created ontology directly indicate the quality properties that need to be included in the quality models and provide tools for constructing quality models: 1) Target quality model for the developer of the flight control system. 2) Quality in use model for the aircraft operator.

The conducted researches include: 1) Execution of ontological analysis of the subject area of application. 2) Creation of ontology of flight control software, which systematizes and structures knowledge of the concepts and objects of the subject area. 3) Formation of functions of interpretation of ontology, as well as specifications of criteria and restrictions for decision-making problems in critical systems. 4) Formation of specifications of requirements for reliability and safety of flight control systems based on the detection and generalization of components of risk analysis and dangers of functioning of critical software systems. 5)Construction of the target quality model and quality in use model for a given subject area and creation of methodology for evaluating the integral level of quality of flight control software.

The conclusions state that an ontological model and quality models can be used in the life cycle of different classes of control systems (including for certification), since any PS of control are characterized by the presence of a control object, which is controlled by a set of parameters measured by parametric information. The results, obtained in the article, can be apply by developers to create their own quality management system of any critical PS in different subject areas of application.

Further research is proposed to conduct a deeper analysis of the technology of integral assessment of the quality of the PS, especially in terms of normalization of metrics of quality attributes in order to unify them.

Keywords: *critical software systems, ontology, software, flight control, objects, interpretation functions, decision-making tasks, criteria and restrictions, quality, quality requirements, safety requirements, functionality requirements, reliability requirements, quality models of critical PS, reduction of risks of flight control, certification, testing.*