УДК 004.415.2.045

І.Е. Райчев, Київ
О.Г. Харченко, Київ
В.А. Василенко, Київ

# ВИЗНАЧЕННЯ ВИМОГ ДО ПРОГРАМНИХ СИСТЕМ КРИТИЧНОГО ПРИЗНАЧЕННЯ З ВИКОРИСТАННЯМ ЗАСОБІВ ДОМЕННОГО АНАЛІЗУ

**Abstract.** The problem of revealing and the analysis of requirements to critical program systems is considered. The system of concepts of a subject domain of the control of flights is created. The developed ontologic model determines classification, structure, composition and interrelation of requirements and forms the mechanism of creation of quality model of critical program systems and evaluation her characteristics for a class of the automated control systems.

## Вступ

В сучасних умовах в Україні 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 (ПС) або інших програмних продуктів на відповідність висуненим початковим вимогам [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, 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 (галузі), в межах якої функціонує ПС критичного призначення, а також онтології процедур сертифікації та атестації. Базовими складовими елементами цих онтологій є вимоги до програмних систем таких класів і методи та засоби оцінювання якості ПС на етапах їх життєвого циклу [6, 7].

### *1. Базові програмні комплекси автоматизованих систем контролю*

У статті як приклад розглянемо клас програмного забезпечення автоматизованих систем контролю (ПЗ АСК) літальних апаратів (ЛА), що 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 АСК, враховуючи те, що рівень якості кожного показника, який входить до новітньої уніфікованої моделі якості системи або ПЗ (запропонованої в

 

міжнародному 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.

Програмне забезпечення класу автоматизованих систем контролю вирішує наступні загальні задачі:

- відтворення контрольованої параметричної інформації;
- контроль виходів параметрів об’єкта контролю за обмеження;
- контроль якості функціонування об'єкта.

Залежно від призначення ПЗ АСК ці задачі можуть вирішуватися як у режимі реального часу, так і після функціонування об’єкта. Тому ПЗ систем цього класу складається з комплексів програм відтворення параметричної інформації, допускового контролю та контролю якості функціонування об'єкта контролю (в нашому випадку – ЛА, рис. 1).


Рис. 1. Класифікація показників якості ПЗ АСК

Польотна інформація включає траєкторні параметри, а також інформацію про функціонування систем ЛА і діях екіпажа по його керуванню, широко використовується для контролю стану ЛА і виявлення помилок у діях екіпажа. Ця інформація обробляється по алгоритмах контролю на борті ЛА чи наземними системами після його посадки. У документах ІСАО високо оцінюється інформація БР і рекомендується впроваджувати обробку польотної інформації з метою запобігання авіаційних подій, вивчення дій екіпажа й поліпшення технічного обслуговування ЛА. На Україні використання польотної інформації всіма експлуатантами ЛА є обов'язковим і регламентується документами [9 – 11].

ПЗ автоматизованих систем контролю польотів (АСКП) складається із сотень програмних модулів, що взаємодіють у процесі вирішення цільової задачі, якою є обробка параметричної інформації з метою прийняття діагностичних і управляючих рішень про стан ЛА, як об'єкта контролю, та якість його функціонування. Для прийняття відповідного рішення з необхідною достовірністю потрібно, щоб АСКП мала високу надійність.

ПЗ АСКП призначено для обробки параметричної польотної інформації (ПІ), яка є складною структурованою інформацією, що містить параметри польоту ЛА (висота, швидкість, положення рулів висоти, кут крену, кут тангажу, положення елеронів, кути відхилення ручок керування двигунами, оберотиви двигунів і багато ін.), розпізнавальні дані (час, дата, номер борта, номер рейса) та деяку контрольну інформацію. Копія польоту ЛА має складну організацію і характеризується циклічним повторенням кадрів інформації, 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 екіпажа й системами ЛА і проводиться післяпольотна обробка ПІ за допомогою ПЗ АСКП. У бортових засобах реєстрації сучасних літаків цивільної авіації (ЦА) в кожному кадрі ПІ записується, як правило, десятки тисяч параметрів, що змінюються з плином часу, і які в подальшому необхідно контролювати.

Контроль польотів – це сукупність дій по обробці ПІ з метою перевірки виконання екіпажем норм льотної безпеки, оцінки якості пілотування й стану систем ЛА. У процесі контролю політ розбивається на ряд етапів: передзлітне рулювання, зліт, набір висоти, політ згідно з маршрутом, зниження, глісада, відхід на друге коло (якщо він мав місце), посадка, післяпосадкове рулювання. Дії екіпажа, режими роботи систем ЛА, ознаки етапів, готовності настання контрольованих подій та інші характеристики польоту регламентуються алгоритмами контролю. Алгоритми контролю польотів складаються розробниками даного типу ЛА, і являють собою складні й громіздкі логіко-алгебраїчні вирази, що містять десятки й сотні предикатів і логічних функцій на множині визначення цих предикатів (як правило, першого порядку), що регламентують поведінку ЛА як об'єкта контролю на протязі всіх етапів польоту. Для сучасного літака ЦА таких алгоритмів налічується не менше трьохсот. Контроль польотів здійснюється по цих алгоритмах контролю за допомогою ПЗ АСКП.

З вищесказаного випливає, що для оцінювання рівня якості ПЗ АСК, необхідно передусім побудувати узгоджену модель якості. Модель якості ПЗ АСК насамперед буде складатися з показників якості, які слід класифікувати згідно з наявними базовими програмними комплексами цих систем (рис. 1). Введені в розгляд множини показників якості мають бути універсальними для ПЗ таких класів інформаційних систем, оскільки вони повинні характеризувати якість основних комплексів програм, з яких складається ПЗ цих систем [12, 13], а тому співвіднесемо галузеві вимоги і показники [9] із уніфікованими характеристиками якості загального базового стандарту

якості [8]. Побудова моделі якості ПЗ АСК полягає у визначенні властивості якості (відповідного атрибута, підхарактеристики та характеристики) з моделі стандарту [8], що відповідає специфікації кожної вимоги, яка задана в онтології предметної області. Процес побудови моделі якості виконаємо після проведення всебічного доменного аналізу предметної області (ПрО), в якій функціонують автоматизовані системи контролю польотів.

### *2. Доменний аналіз галузі застосування ПЗ контролю польотів*

Найбільш сучасним і наближеним до практичної реалізації ПС є підхід, який подає 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 їхнього представлення, а також реалізацію пошуку функціональних структурно-алгоритмічних елементів ПрО, що закладає основи для подальшого технічного втілення реальної ПС.

Доменний аналіз розпочнемо із розгляду та аналізу галузевого стандарту наземних систем автоматизованої обробки польотної інформації [9], що складаються з комплексів програм, показаних на рис.1. Виділимо основні об’єкти онтології ПрО ПЗ АСКП, враховуючи положення стандарту [9], який встановлює загальні вимоги до характеристик таких систем. Формальна модель онтології ПрО ПЗ АСКП являє собою впорядковану трійку скінченних множин:

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

де **C** – скінченна непуста множина концептів (термінів) ПрО, **R** – множина відношень між концептами ПрО, **F** – функції інтерпретації, що задані на поняттях і/або відношеннях онтології $\Omega_{ПЗ\,АСКП}$ .

Стандарт [9] встановлює вимоги до загальних характеристик (властивостей) компонентів будь-яких реалізацій ПЗ АСКП, причому системи, що задовольняють вимогам стандарту можуть бути сертифіковані у встановленому порядку та допускаються до експлуатації в авіаційних підприємствах України. Терміни онтології задають її базові об’єкти, які знаходяться у деяких відношеннях між собою. Тому основні терміни (поняття, концепти) онтології ПрО ПЗ АСКП визначають об’єкти, які в подальшому реалізуються у вигляді класів.

Схеми будь-якої онтології мають задавати систему понять (базові об’єкти), їх класифікацію, композицію, взаємозв’язки та стани. Аналізуючи стандарт [9], передусім побудуємо діаграму класифікації вимог до компонентів АСКП (рис. 2).

Клас вимог до переліку обов'язкових задач ПЗ АСКП є найбільш вагомим і тісно пов'язаний з іншими базовими класами онтології (1), які

безпосередньо залежать від нього. Тому композиційна схема вимог до переліку обов'язкових задач по суті є графічним поданням складу класів онтології $\Omega_{ПЗ\,АСКП}$, де множина відношень **R** складається з відношень класифікації та агрегації. Композиційна схема вимог показана на рис. 3, де: ПІ – це параметрична інформація польоту, зареєстрована бортовими системами ЛА (інакше: ПІ – польотна інформація); ІУС – інформаційна управляюча система; ТНД – тестові набори даних (а також їх структура та методи застосування у процесі випробувань); БР – бортовий реєстратор (пристрій, який фіксує параметри ЛА у польоті); АП – аналогові параметри польоту ЛА, РК – разові команди).

Обробка інформації, записаної бортовими реєстраторами, є актуальною задачею, яка дозволяє забезпечувати безпеку польотів. За допомогою аналізу польотної інформації вирішуються задачі контролю режимів польоту й перевірка виконання правил льотної експлуатації ЛА екіпажем, оцінюється працездатність агрегатів і систем ЛА та визначаються причини авіаційних інцидентів [10, 11].

Помилкові результати роботи базових програмних комплексів, що оцінюють стан об'єкта контролю (рис. 1 – 3), можуть привести до катастрофічних наслідків. Дійсно, якщо мова йде про наземні системи автоматизованої обробки ПІ, то у випадку невірної оцінки якості пілотування і роботи обладнання ЛА існує ризик дозволити подальші польоти непідготовленому екіпажу чи борту ЛА, який має дефекти устаткування, що може спричинити щонайменше авіаційний інцидент.

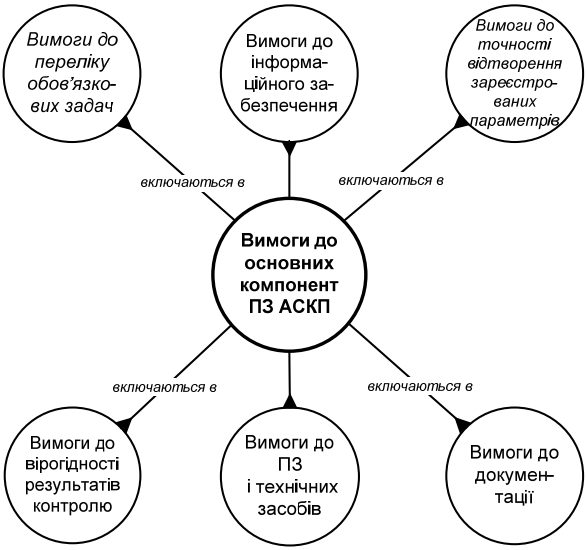


Рис. 2. Онтологія складових компонент вимог до ПЗ АСКП (класифікація вимог)

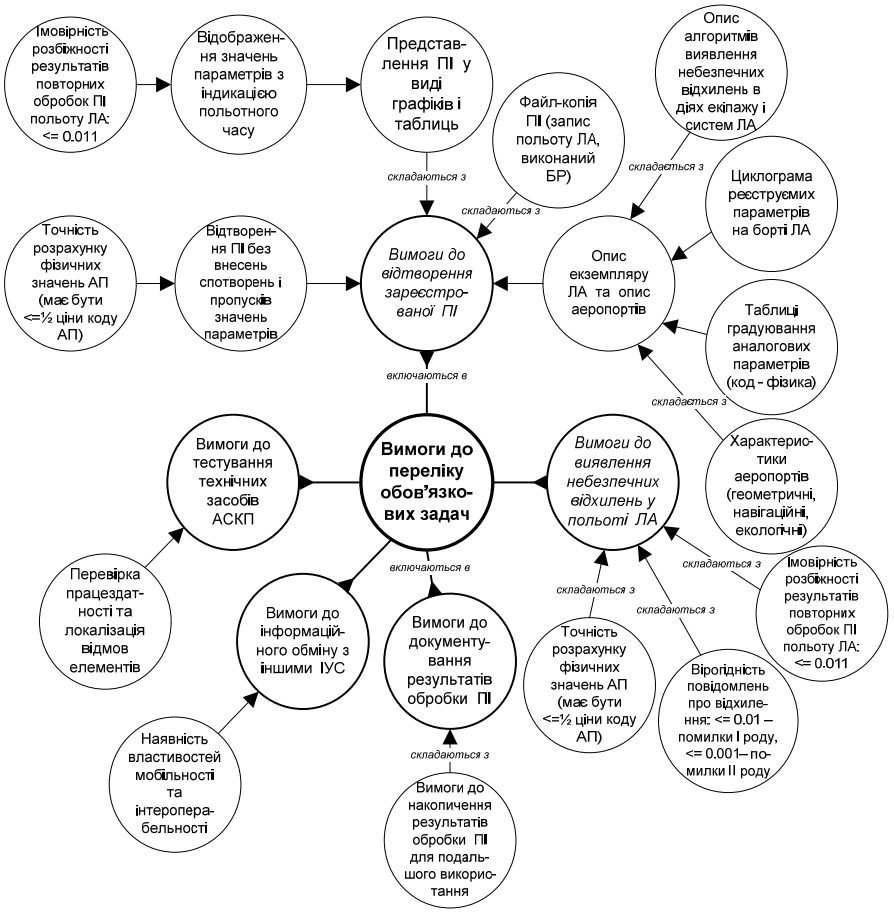


Рис. 3. Загальна онтологія вимог до переліку обов'язкових задач ПЗ АСКП

Якщо ж мова йде про автоматизовані системи контролю польоту, які функціонують у реальному часі на борті ЛА, то інцидент чи катастрофа відбудуться неминуче протягом поточного польоту. Розглянемо ризики помилкової роботи основних комплексів ПЗ АСКП.

Комплекс програм відтворення ПІ вирішує задачу відтворення польотної інформації, яка полягає в графічному представленні зміни аналогових параметрів і разових команд у часі. Під час роботи комплексу існують небезпеки неточного обчислення фізичних значень АП і розбіжності результатів повторних обробок ПІ.

Комплекс програм допускового контролю вирішує задачі допускового контролю. Відповідне ПЗ повинно забезпечувати реалізацію всіх алгоритмів контролю, встановлених для даного типу ЛА, та характеризується ухваленням рішення про перебування об'єкта контролю в деякому стані. Істотною проблемою для комплексу є коректне визначення вірогідності настання подій контролю і підтвердження факту перебування погрішності оцінки в межах допуску.

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 ЛА та наявна процедура підтвердження виявлених відхилень. Небезпеками для цього комплексу, як і для комплексу програм допускового контролю, є можливість некоректного обчислення помилок I та II роду.

Функціями інтерпретації **F**, що задані на відношеннях онтології (1), для схеми з рис.3 слугують предикати алгоритмів контролю ЛА. Наприклад, для об'єкту "Вимоги до виявлення небезпечних відхилень у польоті ЛА" (рис.3), одним із множини контрольованих алгоритмів є предикат події контролю $S073$, який означає "Перевищення максимальної експлуатаційної швидкості польоту":

$$S073 = (7120 \le H_{б} \le 10300) \wedge (V_{пр.} \ge 588) \qquad (2)$$

У формулі (2): $H_{б}$ – висота барометрична, $V_{пр.}$ – швидкість приладова. Функції інтерпретації мають охоплювати повну множину алгоритмів контролю ЛА. Кожен із предикатів алгоритмів контролю ЛА можна формалізувати, використовуючи систему канонічних рівнянь скінченного автомата [14, 15]. На основі цієї формалізації уніфікованим чином будуються логічні схеми автоматних моделей, які слугують для виявлення усіх контрольованих небезпечних відхилень [15, 16].

**Висновки**

Визначені основні програмні комплекси автоматизованих систем контролю та побудована онтологія критичних ПС на прикладі автоматизованих систем контролю польотів ЛА. Створена онтологія наочно визначає класифікацію, склад, композицію та взаємозв'язок вимог, що дозволить більш ефективно виконати побудову моделі якості ПС шляхом встановлення відображення кожної вимоги з визначеної множини на відповідну характеристику, підхарактеристику, атрибут та метрику якості.

В процесі аналізу вимог до ПС критичного призначення виявлено, що в процесі побудови подібних класів систем, в першу чергу необхідно

застосовувати специфікації вимог до властивостей надійності та безпеки функціонування їх програмного забезпечення.

1. ДСТУ ISO 9000–2001. Системи управління якістю. Основні положення та словник. – [Чинний від 2001–07–01]. – К.: Держстандарт України.
2. ДСТУ ISO 9001–2001. Системи управління якістю. Вимоги: (ISO 9001:2000). – [Чинний від 2001–06–27]. – К.: Держстандарт України, 2001. – 23 с.
3. ISO/IEC 17025:1999. General Requirements for the Competence of Testing and Calibration Laboratories. – Режим доступу: http://www.iso.org; http://www.iec.ch.
4. ДСТУ 2462–94. Сертифікація. Основні поняття. Терміни та визначення. — [Чинний від 1995–01–01]. – К.: Держстандарт України, 1994. – 27 с.
5. ДСТУ 2844–94. Програмні засоби ЕОМ. Забезпечення якості. Терміни та визначення. – [Чинний від 1996–01–01]. – К.: Держстандарт України, 1995. – 15 с.
6. IEEE Std 830-1993. Recommended Practice for Software Requirements Specification. – 1993. – 36 p. – Режим доступу: http://www.ieee.org.
7. *Харченко О.Г.* Інструментальний засіб розробки та комунікації вимог якості до програмних систем / О.Г. Харченко, В.В. Яцишин, І.Е. Райчев // Інженерія програмного забезпечення. – 2010. – №2. – С.29-34.
8. ISO/IEC 25010. Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) – System and software Quality models. – 2011. – 34 p. – Режим доступу: http://www.iso.org; http://www.iec.ch.
9. ДСТУ 3275–95. Системи автоматизованого оброблення польотної інформації наземні. Загальні вимоги. – [Чинний від 1996–07–01]. – К.: Держстандарт України, 1996. – 7 с.
10. 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 за № 386. – К.: 1996. – 110 с.
11. 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». – К.: Держ. Департамент авіац. транс. України, 1997. – 11 с.
12. *Райчев І.Е.* Проблеми оцінювання якості критичних програмних систем при їх сертифікації / І.Е. Райчев, О.Г. Харченко // Проблемы программирования. –2004. – №2-3. – С.198-207.
13. *Райчев І.Е.* Концепція побудови сертифікаційної моделі якості програмних систем / І.Е.Райчев, О.Г.Харченко // Проблемы программирования. – 2006. – №2-3. – С.275-281.
14. *Райчев И.Э.* Применение конечных автоматов для реализации алгоритмов контроля полетов воздушных судов / И.Э. Райчев, А.Г. Харченко // Вісник НАУ. –2001. –№3. – С.136-140.
15. *Райчев І.Е.* Синтез автоматних моделей контролю / І.Е. Райчев // Вісник НАУ. – 2002. – №2. – С.43-52.
16. *Райчев І.Е.* Конструювання програм створення тестових наборів даних на базі автоматних моделей / І.Е. Райчев, О.Г. Харченко // Математичні машини і системи. – 2006. – №3. – С.127-136.

**http://doi.org/10.5281/zenodo.3612240**

*Поступила 19.09.2019р.*