УДК 656.02:338.47(045)

О.М. Авдєєв, асп.

ОЦІНЮВАННЯ РІВНЯ ПОВНОТИ БЕЗПЕКИ АВІАЦІЙНИХ СИСТЕМ

Розглянуто питання визначення рівня повноти безпеки технічних систем, які використовуються під час формування та керування процесами технічної експлуатації сучасної авіаційної техніки.

Considered to the questions of a level detection of completeness of safety of an engineering system which are used at formation and control of technical maintenance processes of a modern aircraft.

авіаційна техніка, безпека авіаційних систем, вимоги стандарту, відмови технічних засобів

Вступ

Нині в Україні відбуваються складні еволюційні процеси у галузі цивільної авіації. Їх першоосновою, безумовно, є:
– подальший розподіл власності;
– загострення боротьби за існування у її крайніх проявах;
– перехід у керуванні авіаційною галуззю на європейські стандарти;
– переорієнтація суб'єктів авіаційних послуг на споживача.
Унаслідок економічної кризи різко знизилися обсяги авіаційних перевезень, ускладнилися фінансові взаєморозрахунки, стали більш частими випадки порушення розкладу через затримки заправки літаків паливно-мастильними матеріалами і несвоєчасне обслуговування в аеропортах, зросла соціальна напруженість у трудових колективах.
В умовах кризи галузь утратила відносну рівновагу, загострились взаємовідносини не тільки із зовнішніми організаціями, але й між самими авіаційними підприємствами.
Незважаючи на те, що на території СНД відбувається скорочення кількості авіаційних підприємств, потреба авіації в нових літаках неухильно зростає. Так, за даними Авіаційної адміністрації Росії кожен рік списується 200–350 повітряних суден. В інших країнах СНД ситуація ще гірша у зв'язку з тим, що або зовсім немає державної підтримки власної авіаційної та авіаремонтної промисловості, або її недостатньо.
Проблеми скорочення авіаційного парку загострились також через брак сучасних систем керування ризиками, які виникають під час експлуатації повітряних суден.
Ця ситуація складається на фоні спаду виробництва у світовій авіаційній промисловості у зв'язку з деякими об'єктивними і суб'єктивними факторами.

Постановка проблеми

Розглядаючи ризики, які виникають під час експлуатації авіаційної техніки, усіх суб'єктів авіатранспортної системи цікавлять передусім виникнення ризику великих аварій, які у більшості випадків є передвісниками катастроф.
При цьому зростає усвідомлення того, що більшість відмов сучасних літаків належать до систем керування і безпеки.
Прикладами систем цього типу є:
– системи протипожежного захисту;
– системи аварійної зупинки двигунів;
– системи розподіленого керування;
– системи керування повітряними польотами.
Такі терміни, як «пов'язані з безпекою» і «критичні для безпеки», стали частиною сучасного технічного словника.
Розходження між ними стали стиратись, і є тенденція використати їх як синоніми.
Термін «критична для безпеки» застосовується переважно у тих випадках, коли небезпека може призводити до фатальних результатів, а термін «пов'язана з безпекою» використовується у більш широкому контексті [1–6]. Для цих термінів існує багато визначень, усі вони мають невеликі розбіжності, наприклад, деякі визначення:
– розрізняють множинні та одиночні жертви;
– передбачають нанесення тілесного ушкодження, виникнення захворювання та отримання непрацездатності, крім смерті;
– охоплюють вплив на навколишнє середовище.
У деяких визначеннях йдеться про ушкодження системи.
Однак натепер досягнуто домовленості розрізняти зміст цих термінів таким чином:
– системи, пов'язані з безпекою, – це ті з них, які поодинці або разом з іншими пов'язаними з безпекою системами переводять кероване устаткування у безпечний стан або підтримують його в цьому стані;
– системи, критичні для безпеки, – це ті з них, які самостійно забезпечують або підтримують безпечний стан керованого ними устаткування.

Розбіжності охоплюють кількість рівнів захисту. Термін «застосування, пов'язане з безпекою» позначає таку функцію керування або безпеки, відмова або відмови яких можуть призвести до смерті, тілесного ушкодження або заподіяти збитки навколишнього середовища.

Термін «система, пов'язана з безпекою» застосовують до будь-якої технічної або програмувальної системи, коли відмова, одинарна або в комбінації з іншими відмовами/дефектами, може спричинити смерть, тілесне ушкодження або збитки для навколишнього середовища.

Розв'язання проблеми

Певна одиниця технічного або програмного забезпечення не може бути виключена з категорії виробів, пов'язаних з безпекою, просто через виявлення того, що існують також альтернативні засоби захисту. Це питання треба обговорити заздалегідь і провести формальне оцінювання повноти безпеки.

Системи керування і системи захисту розрізняють так. Системи керування спонукають технологічний процес перебігати певним чином, у той час як системи захисту мають справу з умовами несправності, і тому їх функції придушують дії системи керування. Іноді устаткування, що забезпечує виконання усіх цих функцій, об'єднано, а іноді – розділено. Обидва устаткування можуть бути пов'язані з безпекою. Однак системою безпеки може бути лише та система, відмова якої може призвести до небезпеки.

Часто помилково висувається аргумент про те, що система не пов'язана з безпекою, тому що на випадок її відмови є інший рівень захисту. Прикладом може бути ланцюг автоматичного закриття клапана у разі підвищення тиску у трубопроводі. Це потенційно небезпечне підвищення тиску може також спрацьовуватися додатковим захистом, запобіжним клапаном.

Однак із цього не випливає, що ланцюг закриття клапана перестає бути пов'язаним із безпекою. У конкретному випадку так може бути, але це залежить від інтенсивності відмов обох систем і від цільового значення рівня повноти безпеки.

Донедавна у загальному випадку застосовувався підхід, за якого для кожної з можливих небезпечних відмов передбачалася наявність, принаймні, двох рівнів захисту. Тобто для того щоб виникла небезпека, мали відбутися дві незалежних відмови. Використовуючи підхід, описаний у роботі [7], можна вважати достатнім одинарний (симплексний) пристрій, хоча, зазвичай, для того, щоб зробити частоту інцидентів прийнятно низькою, потрібно передбачити резервування.

Повнота безпеки іноді визначається як імовірність виконання системою, пов'язаною з безпекою, необхідних функцій безпеки за всіх передбачених умов протягом заданого періоду часу. Виникає питання про те, як це можна виразити у вигляді цільових завдань, на відповідність яким такі системи можуть бути оцінені.

Стандарти і керівництва дотримуються концепції рівнів повноти безпеки (РПБ), що передбачає вибір заданого значення РПБ і потім порівняння, як із кількісними, так і з якісними вимогами відповідного РПБ. Задані значення для чотирьох РПБ подано у табл. 1.

Таблиця 1

Значення РПБ

РПБ	Імовірність	
	небезпечних відмов на рік	відмов за наявності запиту
4	10^{-5} до 10^{-4}	10^{-5} до 10^{-4}
3	10^{-4} до 10^{-3}	10^{-4} до 10^{-3}
2	10^{-3} до 10^{-2}	10^{-3} до 10^{-2}
1	10^{-2} до 10^{-1}	10^{-2} до 10^{-1}

Рівень 1 є найнижчим, а рівень 4 – найвищим. Обґрунтуванням наявності двох варіантів задачі РПБ (для високої та низької частоти запитів) служить той факт, що є дві фундаментально різні ситуації, у яких може знадобитися опис цільового завдання. Вони принципово різні і не повинні розглядатися як еквівалентні. Їх навіть визначають за допомогою різних параметрів (тобто інтенсивності та ймовірності). Відмінність між ними найкраще можна зрозуміти на прикладах.

Повітряний трап для аварійного покидання літака – це система з низькою частотою запитів (вони відбуваються з інтервалами у роки або десятки років). Отже, інтенсивність відмов мало придатна для опису повноти безпеки такої системи, оскільки її відмови приховані і потрібно розглядати також інтервал між перевірками, тому становить інтерес комбінація інтенсивності відмов з часом простою, і отже, встановлюємо ймовірність відмови під час запиту.

Для гальм літака коефіцієнт неготовності мало корисний, тому що гальма використовуються під час кожного зльоту та посадки. Тут важлива саме інтенсивність відмов, тому що вона дорівнює тій частоті, з якою літак піддається небезпеці.

Як приклад вибору значення РПБ за низької частоти запитів приймемо ситуацію, для якої ненавмисний ризик (наприклад, ризик загибелі споживача/пасажира), що дорівнює $A = 10^{-5}$ на рік, вважається припустимим. Припустимо, що 10^{-1} (B) від загальної кількості розглянутих небезпечних подій, призводять до фатального результату. Інтенсивність відмов, яка супроводжується небезпечними подіями, можна записати як $C = A/B = 10^{-4}$.

Припустимо, що аналіз дерева відмов показує, що інтенсивність порушень у процесі, не оснащеному захистом, може досягати тільки 0,05 на рік (D). Тоді для системи безпеки інтенсивність відмов за запитом має становити $E = C/D = 0{,}002$. Звірившись із правим стовпчиком табл. 1, побачимо, що прийнятно рівень РПБ 2.

Для іншого варіанта, з високою частотою запитів, прикладом може бути неперервний витратомір газу, що у випадку відмови і наступного помилкового відкриття буде призводити до витоку негорючого газу із приладу. Якщо максимальний припустимий ризик становить $A = 10^{-5}$ на рік, і можливість відмови, що приводить до смертельного результату, B = 1:200, тоді максимальна припустима інтенсивність відмов становить $A/B = 0{,}002$ на рік, що обумовлює цільове значення РПБ 2.

Альтернативний підхід до встановлення рівнів повноти безпеки, відомий як метод "графа ризиків" [4; 6; 7; 9]. Без кількісного оцінювання максимально припустимого ризику загибелі через використання якісних суджень. Приклад графа ризиків показано на рисунку.

НР	НР	3	3	2	2	1	–	Відносно висока
НР	3	3	2	1	1	–	–	Низька
НР	3	2	1	1	–	–	–	Дуже низька

Граф ризиків

Перевага такого графа полягає в тому, що застосовувати його легше і швидше, однак він менш точний. Інтерпретація таких термінів, як "інколи", "можливі" тощо, може бути у різних експертів різною. Крім того, виникає необхідність насамперед у калібруванні таблиці, а зробити це без кількісного оцінювання нелегко, тому що РПБ визначено у числових межах.

Попередній підхід, оснований на кількісному оцінюванні ризиків, завжди має бути кращий.

Не всі відмови можуть бути оцінені кількісно за допомогою очікуваної інтенсивності відмов. Для випадкових відмов технічних засобів дані з прогнозованої інтенсивності відмов у більшості випадків доступні. Втім систематичні відмови, особливо відмови засобів програмного забезпечення, не легко описати таким способом, тому що вони не є випадковими повторюваними відмовами. Отже, ідея використання інтенсивності відмов для прогнозування їх майбутнього стану не може бути застосовна. Тому традиційний прогноз показників безвідмовності для цього випадку застосовувати недоцільно.

Якби існували тільки випадкові відмови технічного забезпечення, то ми застосовували б терміни інтенсивності і не було б потреби встановлювати "смуги" цільових значень.

Однак для систематичних відмов, через те, що їх можна тільки зменшити проведенням під час життєвого циклу робіт з технічного обслуговування, потрібно визначити рівні обмежень для кожного рівня. Кількість рівнів є довільною, проте вона має бути невеликою, оскільки було б нереалістично претендувати на те, що виконання проектних робіт може бути визначене з будь-яким ступенем точності. Справді, у стандарті МЭК61508 твердження про використання чотирьох рівнів є штучним, тому що відмінність між РПБ 1 і РПБ 2, як і між відповідними роботами життєвого циклу, дуже мала [8].

Отже, потрібне і якісне, й кількісне оцінювання, яке має охоплювати:

– випадкові відмови засобів технічного забезпечення (традиційний прогноз показників безвідмовності порівняно з кількісними цільовими значеннями);

– застосування принципу ALARP [9];

– відповідність вимогам до частки безпечних відмов;

– підтвердження достатньої компетентності виконавця у сфері функціональної безпеки.

Термін «частка безпечних відмов» (ЧБВ) застосовують для позначення пропорції таких відмов, які або є «безпечними», або «небезпечними, але які виявляються з допомогою деяких засобів самоперевірки». Тобто, від одиниці треба відняти небезпечні відмови, що не виявляються.

Стандарт МЭК61508 визначає рівні значень ЧБВ, потрібні для встановлення відповідності певному РПБ, з урахуванням використовуваної кратності резервування. Є дві таблиці, які використовують залежно від того, чи певний виріб устаткування або компонент простий (з чітко виявленими видами відмов) – виріб типу А, або складний (таким, як програмувальний прилад) – виріб типу В. Відповідні вимоги подано в табл. 2.

Таблиця 2

Вимоги до ЧБВ

ЧБВ, %	РПБ для виробів		
	симплексних	типу (m + 1)	типу (m + 2)
Вироби типу А			
Менше 60	1	2	3
60–90	2	3	4
90–99	3	4	4
Більше 99	3	4	4
Вироби типу В			
Менше 60	–	1	2
60–90	1	2	3
90–99	2	3	4
Більше 90	3	4	4

Висновки

З розглянутого можна зробити висновок, що часто допускають помилкове припущення про те, що якщо якісні вимоги виконуються, то інтенсивність відмов (або коефіцієнт неготовності) буде теж відповідати встановленим вимогам. Це, зазвичай, не аргумент, тому що різні вимоги стандарту МЭК61508 висуваються до відмов різних видів. Якісні вимоги стосуються систематичних відмов, а випадкові відмови технічних засобів визначаються інтенсивностями відмов компонентів, резервуванням, інтервалами між перевірками тощо.

Література

1. *Collins J.A.* Failure of materials in Mechanical Design / J.A. Collins – Willey. – New York, 1981. – 399 p.
2. *Fullwood R.F.* Probabilistic Safety Assessment in the Chemical and Nuclear Industries / R.F. Fullwood. – Butterworth-Heinemann. – Oxford, 1999. – 438 p.
3. *Kivensen. G.* Durability and Reliability in Engineering Design / G. Kivensen. – Pitman. – London, 1972. – 303 p.
4. *O'Connor P.* Practical Reliability Engineering / P. O'Connor. − 3rd ed. – Willey. – Chichester, 1991. – 351 p.
5. *Shooman M.* Software Engineering – Reliability, Design, Management / M. Shooman. – McGraw-Hill. – New York, 1984. – 312 p.
6. *Smith D.J.* Achieving Quality Software / D.J. Smith. – 3rd ed. – Chapman Hall. – London, 1995. – 648 p.
7. *Carter A.D.S.* Mechanical Reliability / A.D.S. Carter. − 2nd ed. – Macmillian – London, 1986. – 450 p.
8. *Snedecor G.W.* Statistical Methods / G.W. Snedecor. – Ames. – Iowa State University Press, 1967. – 199 p.
9. *Moubray J.* Reliability-centered Maintenance / J. Moubray. – Butterworth-Heinemann. – Oxford, 1997. – 416 p.

Стаття надійшла до редакції 17.03.09.