УДК 681.324

МОДЕЛІ АНАЛІЗУ НАДІЙНОСТІ, ЖИВУЧОСТІ ТА БЕЗПЕЧНОСТІ СИСТЕМ КОНТРОЛЮ ТА УПРАВЛІННЯ ЛІТАЛЬНИХ КОМПЛЕКСІВ

д.т.н., проф. В.С. Харченко

Проведений аналіз взаємозв'язку властивостей надійності, живучості та безпечності, моделей їх опису - діаграм деградації та відповідних структурних схем, і особливостей систем контролю та управління літальних комплексів як об'єктів забезпечення цих властивостей.

Вступ. Надійність, живучість та безпечність є важливими властивостями систем контролю та управління (СКУ) літальних комплексів (ЛК), оскільки вони впливають на їх функціональні та експлуатаційні характеристики. Слід відзначити, що означені властивості тісно пов'язані між собою. Але незважаючи на це, вони, як правило, розглядаються окремо, а іноді навіть протиставляються одне одному як конкуруючі характеристики. Крім того, серед фахівців довгий час не вщухають дискусії термінологічного плану щодо визначення понять надійності програмних засобів і живучості та безпечності СКУ взагалі, проблем гармонізації у цьому сенсі національних і міжнародних стандартів. Вони певним чином обумовлені тим, що в англомовній науково-технічній літературі термін “reliability” фактично відповідає терміну “безвідмовність”, але перекладається як “надійність”, а надійність, живучість та безпечність об’єднані терміном “dependability”, який іноді перекладають як “гарантоздатність” [1-3].

Мета статті полягає у аналізі взаємозв’язку властивостей надійності, живучості та безпечності, моделей їх опису відповідно до СКУ ЛК і особливостей таких систем.

Взаємозв’язок властивостей. Продемонструємо це шляхом аналізу множини станів MS, у яких можуть знаходитись система [4] . Ця множина розділяється на підмножини:

- справних $\mathbf{MS_c}$ та несправних $\mathbf{MS_{\bar{c}}}$ станів (у справному стані $\mathbf{S_{ci} \in MS_c}$ система відповідає всім вимогам до неї, які надаються у технічній документації, у несправному стані $\mathbf{S_{\bar{c}j} \in MS_{\bar{c}}}$ - не відповідає хоча б одній з таких вимог), $\mathbf{MS = MS_c \cup MS_{\bar{c}}}$, $\mathbf{MS_c \cap MS_{\bar{c}} = \varnothing}$, $\mathbf{Card MS_c = 1}$, $\mathbf{Card MS_{\bar{c}} \geq 1}$ ($\mathbf{Card MS}$ - кількість елементів множини $\mathbf{MS}$);

- працездатних $\mathbf{MS_п}$ та непрацездатних $\mathbf{MS_{\bar{п}}}$ станів (у працездатному стані $\mathbf{S_{пν} \in MS_п}$ значення всіх параметрів, які визначають спроможність

системи виконувати задані функції, відповідають заданим вимогам, у непрацездатному стані $S_{\bar{п}\mu} \in MS_{\bar{п}}$ – значення хоча б одного такого параметру не відповідає вимогам), $MS = MS_{п} \cup MS_{\bar{п}}$, $MS_{п} \cap MS_{\bar{п}} = \varnothing$.

Відомо, що система може бути несправною, але працездатною. Це можливо при виникненні несправностей – пошкоджень, які не впливають на спроможність виконувати задані системою функції. Якщо система непрацездатна, то вона, зрозуміло, несправна (внаслідок несправності – відмови): $MS_{\bar{п}} \cap MS_{\bar{с}} \neq \varnothing$, $MS_{\bar{п}} \subset MS_{\bar{с}}$. У свою чергу множина непрацездатних станів декомпозується на:

- частково непрацездатні (або непрацездатні) стани $S_{ч}$, що групуються у підмножини $MS^{1}_{ч}, ..., MS^{d}_{ч}$ залежно від рівня якості, який відповідає цим станам. Кількість підмножин визначається з урахуванням припустимих рівнів деградації **d** (деградація – це, як відомо, процес зниження якості системи внаслідок відмов):

$$MS_{ч} = \bigcup_{i=1}^{d-1} MS^{i}_{ч},\ MS^{i}_{ч} \cap MS^{j}_{ч} = \varnothing\ (i, j \in \overline{1, d-1},\ i \neq j).$$

Причинами деградації можуть бути як зовнішні фактори (екстремальні, збурюючі дії, які викликають відмови елементів СКУ), так і внутрішні причини – поступове накопичення певної кількості відмовивших елементів. Зниження якості полягає в тому, що система не може виконувати одну чи декілька функцій, або виконує їх з погіршеною якістю (продуктивністю, точністю, завадостійкістю та ін.);

- повністю непрацездатні стани $S_{\bar{п}п\rho} \in MS_{\bar{п}п}$, тобто такі, коли не виконується навіть мінімальна сукупність функцій, або рівень якості їх виконання неприпустимо низький. Тоді $MS_{\bar{п}} = MS_{ч} \cup MS_{\bar{п}п}$, $MS_{ч} \cap MS_{\bar{п}п} = \varnothing$. Крім того, множина повністю непрацездатних станів декомпозується на дві пари підмножин станів. Перша пара складається з:

- граничних станів $S_{г\eta} \in MS_{г}$, тобто станів, у яких подальше використання системи за призначенням неможливе, а відновлення економічно недоцільне або небезпечне;

- повністю непрацездатних неграничних станів $S_{\bar{п}\bar{г}\omega} \in MS_{\bar{п}\bar{г}}$. Маємо:

$$MS_{\bar{п}п} = MS_{г} \cup MS_{\bar{п}\bar{г}},\ MS_{г} \cap MS_{\bar{п}\bar{г}} = \varnothing.$$

До другої пари відносяться множини:

- критичних або небезпечних станів $MS_{к}$, які характеризуються тим, що обумовлюють виникнення аварії або катастрофи літального комплексу (загибель людей, екологічні катастрофи, значні економічні та військові втрати та ін.);

- некритичних або захищених станів $MS_{\bar{к}}$, за яких виникнення аварії або катастрофи ЛК неможливе:

$$\mathbf{MS_к} \cup \mathbf{MS}_{\overline{\mathbf{к}}} = \mathbf{MS}_{\overline{\mathbf{пп}}},\ \mathbf{MS_к} \cap \mathbf{MS}_{\overline{\mathbf{к}}} = \varnothing .$$

Слід зазначити, що множина критичних станів є часткою множини граничних станів, $\mathbf{MS_к} \subset \mathbf{MS_г}$. Крім того, можлива ситуація, коли система знаходиться у граничному, але захищеному (некритичному) стані, тобто

$$\mathbf{MS}_{\overline{\mathbf{к}}} \cap \mathbf{MS_г} \neq \varnothing .$$

З урахуванням проведеного аналізу можна виділити підмножини станів, які є визначальними для опису властивостей надійності, живучості та безпечності (рис.1).

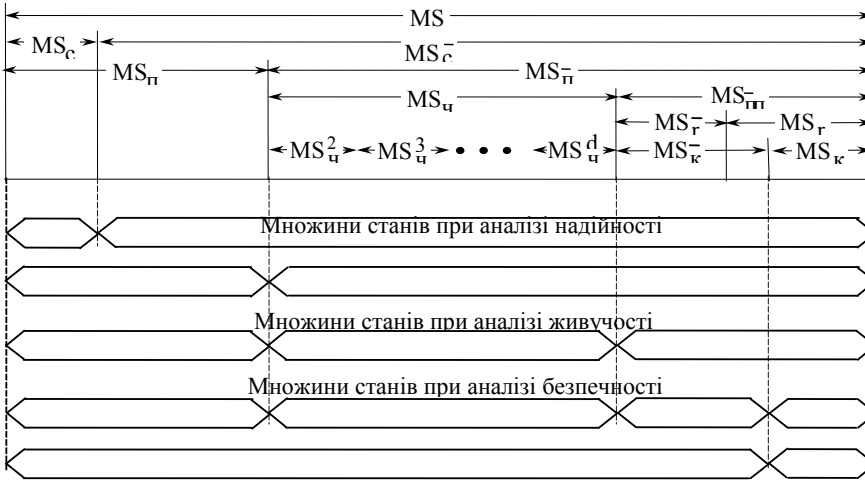

Рис.1. Стани та властивості СКУ

1. Теорія надійності вивчає поведінку СКУ у межах множин станів $\mathbf{MS_с}, \mathbf{MS}_{\overline{\mathbf{с}}}$ і $\mathbf{MS_п}, \mathbf{MS}_{\overline{\mathbf{п}}}$. *Надійність СКУ* – це, таким чином, є властивість зберігати справний або працездатний стани, тобто виконувати задані функції (у повному обсязі) на протязі заданого часу, у заданих нормальних умовах експлуатації, тобто за відсутністю екстремальних впливів.

2. Сферою теорії живучості є поведінка системи, яка описується за допомогою множин частково непрацездатних станів, тобто сукупності множин $\mathbf{MS_п}, \mathbf{MS_ч}, \mathbf{MS}_{\overline{\mathbf{пп}}}$. *Живучість СКУ*, з урахуванням цього, є її здатність зберігати працездатність або частково працездатний (непрацездатний) стани, тобто виконувати задані функції у повному обсязі або частково – у мінімально припустимому обсязі, за відмов, викликаних у тому числі (і перед усім) зовнішніми екстремальними факторами.

3. Предмет теорії безпеки СКУ пов'язаний з аналізом множин станів $\mathbf{MS_п}, \mathbf{MS_ч}, \mathbf{MS_к}, \mathbf{MS}_{\overline{\mathbf{к}}}$. При цьому у множинах працездатних, частково

працездатних та непрацездатних некритичних станах, перш за все, аналізуються потенційно небезпечні стани, з яких можливий перехід у критичний стан. Тобто *безпечність СКУ* – це є властивість зберігати працездатний, частково працездатний або захищений (некритичний) стани і протидіяти переходу до критичного стану. Слід відрізняти цю властивість від безпеки (захищеності) інформації, яка має дещо іншу природу.

Таким чином, властивості надійності, живучості та безпеки систем тісно пов'язані і характеризують її поведінку з урахуванням кількості та типів відмов, їх наслідків з точки зору використання СКУ і усього ЛК. Необхідно підкреслити, що надійність, живучість та безпечність СКУ ЛК практично неможливо забезпечити, якщо система не має такої узагальнюючої властивості як *відмовостійкість* – властивості зберігати працездатний (частково працездатний або захищений) стан при відмовах елементів шляхом автоматичного відновлення (реконфігурації) за обмежений час.

Моделі опису властивостей СКУ. Для аналізу розглянутих властивостей СКУ, у першу чергу, живучості, доцільно використовувати так звані *діаграми деградації* [4]. Вони представляють собою графічне зображення зміни рівня якості системи у часі та за іншими характеристиками (імовірностями станів, кількістю відмов). Якщо не припускається навіть часткове зниження якості, тобто йдеться про властивість надійності, діаграма деградації має одноступеневий вигляд.

Для більш детального аналізу властивостей СКУ діаграми деградації доречно доповнити *структурними схемами надійності* (ССН), *живучості* (ССЖ) та *безпечності* (ССБ). ССН завжди використовуються при оцінці надійності і являють собою добре відпрацьований елемент методики аналізу. Якщо співставляти структурну схему надійності та діаграму деградації, то ССН описує поведінку системи у працездатному стані $\mathbf{S_1}$. Тоді для СКУ з багаторівневою деградацією кожному стану $\mathbf{S_1,...,S_d}$ можна поставити у відповідність структурні схеми, які описують умови знаходження системи у цих станах. Сукупність таких структурних схем будемо називати *структурною схемою живучості*. *Структурною схемою безпечності* назвемо схему, що задає умови переходу системи до критичного стану, аналогічно тому, як структурна схема надійності описує умови переходу системи з працездатного (справного) стану до непрацездатного стану.

Зрозуміло, що для побудови ССН, а особливо ССЖ і ССБ, необхідно провести ретельний аналіз системи, виявити множини її можливих станів (рис.1), умови переходу у кожний з цих станів залежно від відмов усіх елементів СКУ. Описані моделі – діаграми деградації та структурні схеми надійності, живучості та безпечності – є первинними моделями, на базі яких будуються більш детальні (вторинні) моделі – комбінаторно-імовірнісні, марковські чи напівмарковські, імітаційні та інші [5].

Особливості СКУ ЛК як об'єктів аналізу. У загальному випадку майже всі типи літальних комплексів і відповідно їх СКУ мають два основних режими функціонування – чергування (включаючи всі види обслуговування та підготовки до застосування) і власне застосування. З точки зору забезпечення, у першу чергу, надійності цікаво визначити тривалість та можливість відновлення працездатності у цих режимах для різних типів СКУ і ЛК – ракетних, авіаційних, ракетно-космічних. Аналіз інформації, наведеної у табл.1, дозволяє визначити такі їх особливості як об'єктів забезпечення надійності, живучості та безпечності.

Таблиця 1

Умови застосування різних літальних комплексів і принципів побудови СКУ

Чергування		Застосування		Тип	
Тривалість	Засоби відновлення	Тривалість	Засоби відновлення	СКУ	ЛК
Кілька років	Обслуга, автоматичні засоби	Кілька хвилин	Автоматичні засоби, обслуга	Наземні СКУ	Ракетні та ракетно-артилерійські комплекси
		Кілька хвилин, або десятків хвилин	Автоматичні засоби	Бортові СКУ	
Кілька годин, діб	Обслуга, автоматичні засоби	Кілька хвилин, або десятків хвилин	Автоматичні засоби, обслуга	Наземні СКУ	Ракетно-космічні комплекси
		Кілька хвилин	Автоматичні засоби	Бортові СКУ РН	
		Кілька років	Автоматичні засоби (екіпаж)	Бортові СКУ КА	
Кілька годин, діб	Обслуга, автоматичні засоби	Кілька років з перервою для обслуговування	Автоматичні засоби, обслуга	Наземні СКУ	Авіаційні комплекси
			Автоматичні засоби (екіпаж)	Бортові СКУ	

1. Оскільки бортові та наземні СКУ складаються з різнотипних елементів, то для забезпечення надійності цих елементів можуть застосовуватися різні методи контролю, діагностування, реконфігурації та резервування. При цьому необхідно ураховувати цілий спектр обмежень, які є специфічними для наземних і бортових систем.

2. Оскільки ядром наземних і бортових СКУ є цифрові обчислювальні машини ЦОМ, до складу яких входять як апаратні, так і програмні засоби, при вирішенні задачі забезпечення надійності слід ураховувати показники безвідмовності цих засобів. Для цього доречно використовувати компонентну модель розрахунку надійності [6].

3. Системи контролю та управління РК є об'єктом оцінки живучості, оскільки в наземних режимах і режимі польоту на них впливає сукупність екстремальних факторів – агресивні умови природного середовища та дії противника, які призводять до виникнення кратних відмов елементів СКУ. У цих умовах структура СКУ, особливо бортових систем, повинна забезпечувати можливість керованої багатоступеневої деградації, що надає змогу мінімізувати зниження якості (продуктивності, точності) в "обмін" на часткову втрату працездатності.

4. Безпечність СКУ полягає у тому, щоб виключити можливість переходу у небезпечний, критичний стан. Для наземних СКУ властивість безпечності реалізується шляхом введення підсистем, які виконують аварійне припинення пускових операцій в умовах відмов відповідних елементів СКУ або ЛК в цілому та виключають можливість проведення несанкціонованих передпускових або пускових операцій. Для бортових СКУ ця властивість забезпечується завдяки підсистемі управління самознищенням літального апарату при неприпустимому відхиленні від програмної траєкторії.

Закінчення. Надійність, живучість і безпечність СКУ є взаємопов'язаними властивостями. В даній роботі вони розглянуті та проаналізовані з використанням узагальненої теоретико - множинної моделі, діаграм деградації та структурних схем. Зрозуміло, що підсистеми наземних та бортових СКУ повинні мати високу відмовостійкість, яка надасть змогу забезпечити необхідний рівень надійності, живучості і безпечності системи в цілому.

ЛІТЕРАТУРА

1. Laprie J.-C. (ed.) Dependability Handbook. LAAS Report N 98-346, 1998. – 291 p.

2. Leveson N.G. Safeware: System Safety and Computers. – Addison-Wesley, 1995. – 252 p.

3. Харченко В.С. Исследование гарантоспособных структур управляющих вычислительных систем // Проектирование многомашинных комплексов реального времени. – М.: Знание, 1990. – С. 58 - 61.

4. Харченко В.С. Анализ и синтез живучих систем с использованием диаграмм деградации // Системы обработки информации. - Харьков: НАНУ, ПАНИ, ХВУ. – 1999. – Вып. 2(6). – С. 115 - 119.

5. Kharchenko V.S. Methods of an Estimation of Multiversion Safety Systems. Proceedings of the 17-th International System Safety Conference /Orlando, FL /August 16-21,1999. – P. 347 - 352.

6. Харченко В.С. Теоретические основы дефектоустойчивых цифровых систем с версионной избыточностью. – МОУ, 1996. – 506 с.

Подана до редколегії 20.10.2000