ОСОБЛИВОСТІ ОЦІНЮВАННЯ БЕЗВІДМОВНОСТІ І БЕЗПЕКИ АПАРАТНО-ПРОГРАМНИХ КОМПЛЕКСІВ

Мірських Г. О., к.т.н., доцент
Національний університет біоресурсів і природокористування України, м. Київ, Україна

Основні принципи оцінювання безвідмовності та безпеки функціонування технічних об'єктів (ТО) мають чимало загальних рис, але й багато в чому відрізняються. Особливо це стосується об'єктів, які визначаються як апаратно-програмні комплекси (АПК), тобто об'єкти функціонування яких напряму пов'язане з якістю відповідного програмного забезпечення (ПЗ). Адже сучасні парадигми побудови ПЗ передбачають наявність модулів, до яких програма в процесі функціонування «звертається» багаторазово. Причому це відбувається в різні моменти часу, при обробленні даних, що надходять від різних складових. Мета даної роботи провести аналіз загальних принципів оцінювання безвідмовності та безпеки ТО (як і апаратних складових АПК), а також АПК в цілому, виявити загальне та відрізнене у відповідних алгоритмах оцінювання показників вказаних категорій та запропонувати до використання алгоритми, які б надавали можливість узагальнити основні етапи відповідних обчислень.

Основним поняттям теорії надійності є *відмова*, а отже всі розрахунки, пов'язані з визначенням безвідмовності починаються з усвідомлення понять працездатного і непрацездатного станів. За вказаних умов обчислення безвідмовності ТО нерідко здійснюється (принаймні на рівні складових) без урахування його структурних особливостей, що приводить до найпростішої каскадної моделі включення окремих елементів. Такий підхід можна вважати прийнятним виключно для структурно-простих ТО, і не може бути застосований до АПК, адже наявність ПЗ «автоматично переводить» ТО до класу структурно-складних, а тим більше для АПК, при аналізі яких доводиться враховувати логіку зв'язків не тільки окремих складових, але й логіку побудови ПЗ, що виключає можливість зведення задачі обчислення безвідмовності (як і інших показників надійності) до аналізу каскадної моделі [1]. Більше того, проявлення помилки в ПЗ, або його функціонування в умовах надходження неповної та/або викривленої інформації від складової, що відмовила, може призвести до ситуації, яка подібна одночасній відмові декількох складових з мало прогнозованими наслідками.

Основним поняттям теорії безпеки є поняття *аварійної ситуації*, а отже аналіз ТО щодо його стійкості до деградації починається з усвідомлення сутності поняття аварійного стану, при ідентифікації якого об'єкт аналізується з точки зору можливості відмови *будь-якої складової* (незалежно від того чи відмовили на даний момент інші складові) на шляху до повної де-

градації цього об'єкта [2]. Це в багатьох випадках може в більшій або меншій мірі співпадати з результатом проявлення помилки у ПЗ.

За вказаних умов найбільшу інформацію можна отримати на підставі не стільки прямих розрахунків безвідмовності АПК, скільки на підставі розроблення відповідних сценаріїв його функціонування під час переходу від одного стану до іншого. Розроблені сценарії відображаються відповідною моделлю АПК, якою враховуються як матеріальні, так і віртуальні (реалізовані відповідним ПЗ) зв'язки окремих складових. Звичайно, отриману модель не можна звести до каскадної. На підставі розробленої моделі будується логічна функцію, що описує той чи інший стан АПК в залежності від конкретного сценарію. Вказана логічна функція стає основою реалізації алгоритму обчислення безвідмовності АПК, розроблення алгоритму процесу діагностування з метою встановлення місця відмови, а також основою встановлення ознак переходу АПК до аварійного стану, який можна ідентифікувати на підставі відповідних алгоритмів [2], серед яких найбільше поширення отримали алгоритми засновані на принципах: «від кінця у початок» та «від початку у кінець».

Алгоритм аналізу аварії за принципом «*від кінця у початок*» полягає в тому, що після визначення аварійного стану розробляється сценарій, в процесі якого будується логічна схема зв'язків (це пропонується робити на підставі відповідної форми подання структурно-логічної схеми АПК, звичайно, з урахуванням логіки побудови ПЗ). Побудована логічна схема відображатиме відповідний сценарій, який містить всі можливі сполучення подій, здатних (окремо або у сукупності) привести до аварійної ситуації.

Алгоритм аналізу аварії за принципом «*від початку у кінець*». реалізує пошук шляхів переходу АПК з працездатного стану до аварійного, який спирається на факт виникнення події, що ініціює вказаний перехід. Як і в описаному вище алгоритмі за результатами аналізу будується відповідна логічна схема зв'язків, що відображає розроблений сценарій небезпечного функціонування АПК, виникнення негативних подій, які здатні привести даний АПК до аварійного стану та ін.

Таким чином, встановивши відповідні ознаки, які сприяють ініціюванню аварійної ситуації, розробляється сценарій можливого розвинення аварії всередині АПК, що є наслідком виникнення вказаних ознак. При цьому особлива увага приділяється ПЗ (звичайно за його наявності у ТО), властивості якого можуть як сприяти розвиненню аварійної ситуації (при відсутності відповідних вимог до цього ПЗ), так і «парирувати» її (за умови розроблення ПЗ з урахуванням наявності інформації щодо відповідних сценаріїв). Отриманий сценарій розвинення аварії в АПК має вигляд «дерева подій», циклу, відповідної мережі тощо й являє собою логічну схему зв'язків окремих складових, яка відображає як саме розвивається аварія, які складові вона охоплює, яке обладнання зачіпатиме і т.п.

Після розроблення сценаріїв щодо розвинення виявлених (звичайно, бажано всіх можливих) аварійних ситуацій (і побудови відповідних логічних функцій) здійснюються оцінки ймовірності реалізації цих сценаріїв (кожного окремо і всієї сукупності в цілому). При цьому на практиці нерідко можуть виникати ситуації, за яких обчислення вказаних оцінок викликає суттєві труднощі, або взагалі з тих чи інших причин неможливе. За таких умов рекомендується перейти до виявлення складової АПК, яка є найбільш значима, найвагоміша або найважливіша з огляду на реалізацію відповідного сценарію. Це в більшості випадків дає можливість суттєво знизити ймовірність реалізації відповідного сценарію за рахунок підвищення безвідмовності цієї складової або за рахунок прискіпливішої уваги до ПЗ, яке забезпечує відповідним чином організоване управління вказаною і пов'язаними з нею складовими.

Перелік посилань

1. Черкесов Г.Н. Надежность аппаратно-программных комплексов. СПб.: Питер, 2005. – 479 с.

2. Рябинин И.А. Надежность и безопасность структурно-сложных систем. СПб.: Изд-во С.-Петербургского ун-та, 2007. – 276 с.

3. Горопашная А. В. Оценка важности аргументов немонотонных логических функций при логико-вероятностном анализе безопасности сложных технических систем / Вестник С.-Петербургского ун-та, 2009. Сер. 10. Вып. 1. С. 19 – 32.

Анотація

На підставі аналізу станів технічного об'єкта, до складу якого входить відповідне програмне забезпечення, зроблено висновок щодо необхідності оцінювання стабільності експлуатації таких об'єктів на підставі розроблення сценаріїв переходу об'єкту з одного стану до іншого з виділенням тих складових, які в найбільшій мірі відповідальні за реалізацію відповідного сценарію. При цьому мірою усталеного функціонування об'єкту може бути ймовірність реалізації якого-небудь сценарію, а краще – всієї сукупності сценаріїв.

Ключові слова: технічний стан, безвідмовність, аварійність.

Аннотация

На основании анализа состояний технического объекта, в состав которого входит соответствующее программное обеспечение, сделаны выводы о необходимости оценивания стабильности эксплуатации таких объектов на основе разработки сценариев перехода объекта от одного состояния к другому с выделением тех составляющих, которые в наибольшей мере ответственны за реализацию соответствующего сценария. при этом мерой стабильности функционирования объекта может быть вероятность реализации какого-нибудь сценария, а лучше – всей совокупности сценариев.

Ключевые слова: техническое состояние, безотказность, аварийность.

Abstract

On the basis of the technical state of the object, this includes appropriate software, concluded on the need assessment stabilization operation of those facilities on the basis of the development scenarios of transition from objection state to another with the release of components that are most responsible for the implementation of the relevant scenario. At the same time, the measure of the stable functioning of the object may be the likelihood of implementation of a script, but preferably – the whole set of scenarios.

Keywords: technical condition, failure-free operation, accident rate.