УДК 62-049.5(043,2) https://doi.org/10.35546/kntu2078-4481.2023.1.17

М. В. ДОНЧЕНКО
кандидат технічних наук, доцент,
доцент кафедри інтелектуальних інформаційних систем
Чорноморський національний університет імені Петра Могили
ORCID: 0000-0002-4084-3112

ВРАХУВАННЯ НАДІЙНОСТІ ПРИ ОЦІНЦІ БЕЗПЕКИ СИСТЕМ

В цій роботі розглядається можливість оцінки безпеки складних технічних систем за параметрами їх надійності. Надійність і безпека системи є дві визначальних оцінки якості системи, але характеризують її по-різному. Надійність характеризує її з точки зору можливості виконання нею своїх функцій в заданих умовах. В той же час безпека – можливість існування або цілісності і системи, і людей, і довкілля навколо неї. При цьому вони логічно пов'язані – фактори, які приводять до ненадійності, можуть бути причиною до появи небезпечних ситуацій. Враховуючи те, що питання оцінки надійності достатньо детально розроблене і широко використовується, в той час, як оцінка безпеки, в силу складності і проблемності недостатньо розроблена, використання додаткової інформації дозволило б, в якісь мірі,частково розкрити цю проблему. Враховуючи те, що питання оцінки надійності виконується при проектуванні або при експлуатації систем, а оцінка інших параметрів не складе надто великих складнощів, таку оцінку безпеки можна вважати, в певній мірі, реальною.

Крім того, аварійна ситуація може виникати при сукупності певних несприятливих умов, в яких відмова системи може послабити її або спровокувати певні деструктивні процеси, які можуть привести до аварійної ситуації. Наприклад, втрата ходу судна чи відмова гальм автомобіля. Тому запропонована оцінка безпеки може бути використана для систем, для яких відмова може привести до критичної ситуації в певних умовах. В таких випадках, ще на стадії проектування намагаються підвищити надійність системи або її стійкість у несприятливих умовах чи конструктивно формують захист системи від можливих деструктивних змін. Введення систем захисту системи від деструктивних змін надає можливість їх зменшити або навіть не допущення таких змін, захистити людей і довкілля від негативного впливу аварій.

Запропонований метод може бути використаний для оцінки безпеки і розробки заходів для її підвищення, а також для створення систем захисту самої системи, людей і довкілля.

Ключові слова: *надійність, безпека, відмова, загроза, аварійна ситуація, оцінка безпеки.*

M. V. DONCHENKO
Candidate of Technical Sciences, Associate Professor,
Associate Professor at the Department of Intelligent Information Systems
Petro Mohyla Black Sea National University
ORCID: 0000-0002-4084-3112

RELIABILITY ACCOUNTING IN SYSTEM SAFETY ASSESSMENT

The work considers possibility of assessing the complex technical systems safety according to their reliability characteristics. Reliability and the system security are two defining assessments of the system quality, but they characterize it in different ways. Reliability characterizes it in terms of its ability to perform its functions under given conditions. At the same time, security is the possibility of existence or integrity of both the system, and the people, and the environment around it. However, they are logically connected – factors that lead to unreliability can be the cause of dangerous situations. Considering that the issue of assessment reliability has been developed in sufficient detail and is widely used, while safety assessment has not been sufficiently developed due to its complexity and problematic nature, the use of additional information would allow to some extent reveal partially this problem. Taking into account the fact that the issue of reliability assessment is carried out during the design or operation of systems, and the assessment of other parameters will not be too difficult, such an assessment of safety can be considered, to a certain extent, real.

In addition, an emergency situation can occur with a combination of certain unfavorable conditions, in which the failure of the system can weaken it or provoke certain destructive processes that can lead to an emergency situation. For example, the loss of the ship's speed or the failure of the car's brakes. Therefore, the proposed security assessment can be used for systems for which a failure may lead to a critical situation under certain conditions.

In such cases, even at the design stage, they try to increase the reliability of the system or its stability in adverse conditions or constructively form the protection of the system against possible destructive changes. The introduction of system protection systems against destructive changes provides an opportunity to reduce them or even prevent such changes, protect people and the environment from the negative impact of accidents.

The proposed method can be used to assess safety and develop measures to increase it, as well as to create systems to protect the system itself, people and the environment.

Key words: *reliability, safety, failure, threat, emergency situation, safety assessment.*

Вступ

Серед багатьох оцінок якості систем є дві базові – надійність і безпека. Ці дві оцінки мають багато спільного і, при цьому, можуть суттєво відрізнятися. В обох напрямках проведено багато досліджень. Наведемо їхні визначення. «***Надійність системи*** – це її здатність до безвідмовної роботи протягом заданого проміжку часу у визначених умовах» [5]. «***Безпека*** – це такі умови, в яких перебуває складна система, коли дія зовнішніх факторів і внутрішніх чинників не призводить до процесів, що вважаються негативними по відношенню до даної складної системи у відповідності до наявних, на даному етапі, потреб, знань та уявлень» (Вікіпедія). При всьому тому, що безпеці присвячено дуже багато розробок, питання оцінки безпеки ще до кінця не вирішене і це не тому, що воно не важливе. Скоріше, навпаки, але тут слід визнати специфіку і складність отримання такої оцінки в силу багатофакторності впливів, які приводять до негативних ситуацій (їх частіше називають: аварійними ситуаціями (АС)) [4]. Якщо методи оцінки надійності детально розроблені і вже багато років використовуються [5], то відносно безпеки таких глибоких напрацювань, на жаль, не знайдено.

Постановка проблеми і формулювання мети

Дане дослідження має на меті поєднати ці дві важливі категорії якості, визначити їх взаємний «вплив» і отримати можливість, в якісь мірі, оцінки безпеки через надійність.

Викладення основного матеріалу дослідження

Як уже було відмічене вище, ці характеристики оцінюють властивості системи, як би в одному напрямку, але з різних точок зору. Обидві характеризують функціонування системи і його припинення, але там де появляється відмова – надійність припиняється, а небезпека тільки розвивається. Надійність характеризується «появами відмов», точніше їх «не появою». Відмова – це неможливість нормального функціонування в заданих умовах. А безпека – це відсутність АС в реальних умовах. Точніше – це відсутність негативного впливу на життя і здоров'я людей, деструктивного впливу на саму систему і на довкілля. Розглянемо ці характеристики детальніше.

Фактично, відмова – це ситуація, в якій система не може нормально функціонувати в заданих умовах. Ця подія може виникнути в результаті накопичення негативних змін в самій системі (старіння, знос і т.п.). Цей процес базується на фізичних процесах змін в матеріалах деталей системи (старіння) чи змін геометрії механічних з'єднань між елементами системи (знос). Ці процеси досить складні, але існує достатньо великий об'єм досліджень у цьому напрямку, що надає можливість прогнозувати, з певною ймовірністю, появу критичних змін, які можуть привести до відмови. Відмови, які появляються в результаті таких змін називають поступовими [5]. Інший вид відмов – це відмови, які виникають в результаті випадкової появи зовнішніх екстремальних впливів на систему, що, в результаті, може привести до деструктивних змін в конструкції системи і неможливості нормального функціонування і, навіть, до АС. Появу таких впливів досить складно спрогнозувати, тому ймовірність їх появи визначають на основі статистичних даних експлуатації системи чи спеціальних випробувань.

Що стосується безпеки, то тут все набагато складніше. В нашому дослідженні ми будемо розглядати тільки ті системи, для яких характерна можливість появи АС після відмови системи. Безпека забезпечується відсутністю загроз для людей, самої системи і довкілля. В залежності від призначення системи, її конструктивних особливостей і умов використання можна виділити загрози і напрямки їх можливого впливу та рівня негативних змін при появі відмови, яка:

- може привести до деструктивних змін в самій системі;
- провокує до негативних змін оточуючих систем;
- може бути небезпечна для операторів і людей навколо;
- може привести до катастрофічних змін в системі і довкіллі.

Звичайно, така градація достатньо умовна, але визначення негативних впливів ставить вимоги як до проектування системи, та і до оцінки її безпеки.

За аналогією з надійністю оцінку безпеки зручніше виконувати за явною появою небезпечних подій (або АС). Властивість же надійності системи втрачається при появі такої відмови. Поява відмови може бути причиною появи негативних впливів на людей, довкілля і на саму систему. Наприклад, втрата ходу судна чи відмова гальм у автомобіля. В нашому випадку, відмова стає очевидною загрозою як цілісності системи, так і для здоров'я і життя людей та негативних змін довкілля. Тому, маючи параметри надійності (ймовірність відмови), можна говорити, що є передумови появи АС.

Розглянемо події:

А – відмова не настала;

Б – поява відмови;

В – настала АС*;*

С – АС не настала.

Для нашого випадку, події А і С не розглядаються, оскільки на безпеку не впливають. Подія Б розглядається при умові, що вона передує події В. Тоді, події Б і В несумісні тому, що спочатку появляється подія Б,

а потім В. Більше того, подія В залежна від того, чи появилася подія Б. Подія Б не залежить від події В тому, що при появі події В розгляд появи події Б втрачає смисл.

Тоді подія появи АС може настати у випадку відмови і настання аварійної ситуації в результаті її появи. Оскільки ці події взаємопов'язані і часовий проміжок між ними практично нульовий, то можна говорити про спільну появу обох подій.

$$N=БВ,$$

Якщо перейти до ймовірностей появи подій, то ми отримаємо:

$$P(N)=P(Б)*P(В/Б),$$

де P(Б) = Q(t) – ймовірність появи відмови системи, яка може привести до *АС*;

P(В/Б) – ймовірність настання аварійної ситуації в результаті відмови системи.

Настання АС край небажана подія і, як правило, вона фіксується. За статистикою АС маємо можливість отримати розподілення щільності ймовірності і ймовірності настання АС. Маючи розподіл ймовірності відмови системи нескладно отримати ймовірність появи АС.

$$N(t)=Q(t)*P_{AC}(t).$$

Відповідно, для оцінки безпеки зручніше мати ймовірність протилежної події – ймовірність не настання АС S(t):

$$S(t)=1-N(t)=1-[Q(t)*P_{AC}(t)].$$

Оскільки настання АС пов'язано в великими втратами в, тому числі, і серед людей, ведуться серйозні дослідження в напрямку зменшення чи обмеження ризику появи АС. Це – цілеспрямоване проектування, організація експлуатації, врахування «людського фактору», удосконалення систем захисту.

Сучасні САПР дозволяють значно підвищити ефективність проектування з метою покращення показників надійності, зменшення можливості появи загроз АС, введення конструктивного, експлуатаційних і організаційних систем захисту від можливих загроз та врахування «людського фактору».

Крім цього, існують умови, які сприяють чи провокують появу АС. Вони можуть бути як зовнішні, так і внутрішні. Врахування таких умов дозволить точніше оцінювати рівень безпеки і направляти дослідження та проектування на зменшення рівня їх впливу. Очевидно, щоб настала АС необхідно спільне настання відмови, можливості настання АС і умов для її появи.

$$S(t)=1-N(t)=1-[Q(t)*P_{AC}(t)*U(t)],$$

де U(t) – ймовірність появи сприятливих умов для настання АС.

Логічно було б врахувати і ефективність систем захисту, якщо вони є. В цьому випадку нас цікавить ймовірність зниження можливості настання АС системами захисту { Z(t)=0} – захисту немає чи не спрацьовує; {Z(t)=1} – повний захист. Тоді для спільного настання перерахованих подій формула прийме вигляд:

$$1-N(t)=1-\{Q(t)*P_{AC}(t)*U(t)*[1- Z(t)]\},$$

де 1- Z(t) – ймовірність зниження загрози АС при наявності систем захисту.

Функцію розподілу ймовірності не спрацювання систем захисту можна отримати за експериментальними дослідженнями або шляхом імітаційного моделювання. Розподіл отримати буде достатньо складно і дорого, а коефіцієнт врахування систем захисту отримати реально.

Висновки

Запропонована можливість оцінки безпеки систем за показниками її надійності, умов експлуатації і наявності систем захисту. Метод може бути корисним при проектуванні і аналізі безпеки складних систем.

Список використаної літератури

1. Донченко М. В., Казарєзов А. Я. Підвищення безпеки суден на базі геоінформаційних систем. Наукові праці : наук. журн. Вип. 295. Т. 307. Комп'ютерні технології. Миколаїв : Вид-во ЧНУ ім. П. Могили, 2017. С. 36-41.

2. Донченко М. В., Казарєзов А. Я. Використання геоінформаційних систем для раннього виявлення надзвичайних ситуацій. Наукові праці : наук. журн. Вип. 308. Т. 320. Комп'ютерні технології. Миколаїв : Вид-во ЧНУ ім. П. Могили, 2018. С. 31-37.

3. Mykhailo Donchenko SAFETY ASSESSMENT OF EMERGENCY SYSTEMS: SCIENTIFIC JOURNAL OF POLONIA UNIVERSITY, #53, 2022. С. 225-230.

4. ДСТУ 2860-94 Надійність техніки. Терміни та визначення

5. Сухенко Ю.Г., Литвиненко О.А., Сухенко В.Ю. Надійність і довговічність устаткування харчових і переробних виробництв: Підручник. К.: НУХТ, 2010. С. 424.

References

1. Donchenko M. V., Kazariezov A. Ya. (2017) *Pidvyshchennia bezpeky suden na bazi heoinformatsiinykh system* [Ships safety improving based on the geographic information systems]. *Naukovi pratsi* [Scientific studies] (scientific journal), vol. 295, no. 307, pp. 36-41. Mykolaiv: BNU named after Petro Mohyla publication.

2. Donchenko M. V., Kazariezov A. Ya. (2018) *Vykorystannia heoinformatsiinykh system dlia rannoho vyiavlennia nadzvychainykh sytuatsii* [Use of geographic information systems for early detection of emergencies]. *Naukovi pratsi* [Scientific studies] (scientific journal), vol. 308, no. 320 *Kompiuterni tekhnolohii*, pp. 31-37. Mykolaiv: BNU named after Petro Mohyla publication.

3. Donchenko, M. (2022). *Safety assessment of emergency systems.* Scientific Journal of Polonia University, no. 53, pp. 225-230.

4. DSTU 2860-94 (1994). *Nadiinist tekhniki. Terminy ta vyznachennia* [Reliability of equipment. Terms and definitions]

5. Sukhenko, Yu. H., Lytvynenko, O. A., &Sukhenko, V. Yu. (2010). *Nadiinist i dovhovichnist ustatkuvannia kharchovykh i pererobnykh vyrobnytstv: Pidruchnyk* [Reliability and durability of equipment for food and processing industries: Textbook]. K: NUHT, p. 424.