

## ПРОГРАМНО-АПАРАТНЕ ТЕСТУВАННЯ ІНФОКОМУНІКАЦІЙНИХ СИСТЕМ

<sup>1</sup> Вінницький національний технічний університет

### *Анотація*

*Здійснено аналіз проблеми стійкості до відмов програмно-апаратних інфокомунікаційних комплексів і підходів до забезпечення їх працездатності в процесі проектування.*

**Ключові слова:** адитивний білий гаусовий шум, відношення сигнал / шум, телекомунікаційна система, коефіцієнт бітових помилок, квадратурна фазова маніпуляція, двійкова фазова маніпуляція, величина вектора помилки.

### *Abstract*

*The analysis of the problem of resistance to failures of software and hardware infocommunication complexes and approaches to ensuring their efficiency in the design process is carried out.*

**Keywords:** additive white Gaussian noise, signal-to-noise ratio, telecommunication system, bit error rate, quadrature phase manipulation, binary phase manipulation, error vector value.

### **Вступ**

В даний час одним із важливих завдань сучасної вітчизняної промисловості є розробка складних пристроїв з унікальними споживчими властивостями, здатних виконувати свої функції з високим рівнем стійкості до відмов. При цьому для апаратно-програмних комплексів з великою питомою вагою програмної частини увага приділяється вивченню методів, що ведуть до скорочення термінів розробки зразків і підвищенню їх відмовостійкості. Удосконалення методів і засобів підвищення відмовостійкості для мікропроцесорних пристроїв пов'язане з проблемою ефективності застосування відомих стандартів і методик для малосерійних пристроїв інформаційних комплексів. Крім того, для регламентованої в стандартах процедури тестування цифрових пристроїв за допомогою імітації несправностей не визначено конкретних алгоритмів і необхідного комплексу технічних засобів.

Теоретичне і практичне вирішення проблеми забезпечення підвищення стійкості до відмов для проєктованих мікропроцесорних пристроїв може бути досягнуто шляхом синтезу способів експериментальних досліджень по імітації несправностей за допомогою спотворення вхідних даних і переднього оброблення статистичної інформації для програмного забезпечення (ПЗ), завантаженого в апаратне середовище мікропроцесорного пристрою, а також аналізу реакції на внесення несправності і визначення достатності обсягу випробувань за допомогою нечіткого логічного висновку.

Сучасні стандарти розробки і проектування технічних програмно-апаратних пристроїв, засновані на методиці FMEA, знаходяться в системній кризі в зв'язку з постійним зростанням складності систем управління інформаційних комплексів і умов їх застосування, з одного боку, і в зв'язку з проявом властивості емерджентності цих систем, яке не враховується на етапі проектування.

Значний внесок у підвищення стійкості до відмов складних програмно-апаратних пристроїв внесли вітчизняні та зарубіжні вчені Пархоменко П.П., Черкесов Г.Н., Ушаков І.В., Avizienis A., Randell B., Herrin S., Katsuk i D., Globl W. та ін. Питаннями проектування засобів імітації несправностей займаються вчені Лучинин В.В., Arlant J., Elks C., Rannels D., Williams R., Gaisler J., Natella R. Питанням підвищення якості та надійності ПЗ присвячені роботи вчених Ліпаєва В.В., Ковальова І.В., Boehm BW, Meyer J., Lyu MR, Levendel Y., Shooman ML, Tai A., Xie M, Zhou L. Дослідженням властивостей програмного забезпечення і безпеки програм присвячені роботи Berman O., Choi JG, Epstein D., She D., Pei K [1-5].

Існує список так і не вирішених в теорії проблем надійності, який був опублікований на Міжнародній конференції MMR-2000 в доповіді «Надійність: минуле, сучасне, майбутнє». На першому місці в цьому списку знаходиться проблема надійності програмного забезпечення, на третьому місці - питання надійності унікальних високо відповідальних систем. Проблеми надійності глобальних територіальних систем і телекомунікаційних мереж займає четверте і п'яте місце. До вирішення цих проблем є тільки підходи. Теорія надійності сформувалася як частина прикладної математики і розробила різні методи вирішення проблем надійності, розвинені в математичні моделі, які все ще не досягли рівня, придатного для застосування на практиці (проблема відсутності необхідних вихідних даних).

Процедура аналізу видів, причин і наслідків відмов РЕА є обов'язковою складовою частиною процесу проектування і відпрацювання пристроїв, починаючи з розробки ескізного проекту до випробувань дослідних зразків.

На основі проведеного аналізу зроблено висновок про доцільність розробки технічних рішень для практичного застосування методики FMEA до мікропроцесорних пристроїв у вигляді розроблених алгоритмів, методик і пристроїв.

Основна ідея роботи полягає у використанні попередньо опрацьованих статистичних даних про функціонування пристрою, що перевіряється в алгоритмах імітації та виявлення помилок ПЗ і апаратних відмов.

Метою роботи є підвищення стійкості до відмов мікропроцесорних пристроїв за допомогою технічних і програмних засобів тестування на основі імітації несправностей інформаційного комплексу.

### Результати дослідження

Однією з тенденцій останнього покоління програмного забезпечення є дослідження програмних засобів на потенційно вразливі місця з точки зору інформаційної безпеки, а також для обліку можливості фізичної перезапису програм або впливу на пристрої живлення, стійкості до електромагнітних атак використовуються спеціальні апаратні пристрої, що контролюють механізми безпеки функціонування програм при зміні умов функціонування апаратного середовища. Оскільки при розробці довірених програмних засобів мікропроцесорних пристроїв проектування здійснюється за допомогою засобів компіляції, бібліотек інтерфейсів і протоколів, які представляють собою величезну кодову базу, тому атестація і верифікація коду для зниження ризику прояви вразливостей є тенденційним завданням. Для верифікації властивостей програм і перевірки коректності функціонування використовуваних бібліотек, які застосовані при розробці програм мікропроцесорних пристроїв використовуються сучасні засоби статичного аналізу, що дозволяють визначити потенційно вразливі місця коду в процесі його проектування. Оскільки верифікація коду представляє окрему складну задачу, тому економічна доцільність проведення верифікації для мікропроцесорних пристроїв недоцільна. Тому розглядають різні інші дослідження програм, в тому числі із застосуванням моделі «чорний ящик» (таблиця 1) [1].

Таблиця 1. Моделі тестування програми

Критерії	«Білий Ящик»	«Сірий ящик»	«Чорний ящик»
Рівень застосування	Модульне тестування	Інтеграційне тестування	Приймальне тестування
Відповідальність	Розробник	Розробник	Незалежний тестувальник/ Розробник
Знання реалізації	Обов'язково	Обов'язково для інтерфейсів	Не вимагається
Знання використання сценарію	Необхідно	Необхідно	Невідомо
Матеріали для сценаріїв тестів	Код для всієї системи	Код для інтерфейсів та окремих модулів	Специфікація

Для неперевірених бібліотек, драйверів і протоколів формується алгоритм тестування за методикою «сірого» або «чорного» ящика. Це означає, що властивості бібліотек вважаються невивченими і досліджуються в заданих станах виконання програми. Сформована діаграма переходу станів дозволяє оцінити коректність роботи тестованих модулів. Проте, розробка програм мікропроцесорних пристроїв без урахування властивостей програми в частині базових зв'язків програмних компонентів і модулів призводить до підвищення складності семантичних і синтаксичних властивостей програми, що в свою чергу призводить до ризику появи помилок. Для зниження рівня складності програм використовується проектна архітектура, яка представляє організацію системи і описує зв'язки між компонентами цієї системи (а також зовнішнім середовищем). Архітектура дозволяє визначити принципи проектування і розвитку програми [2-4]. Тестування мікропроцесорної програми представляє процес дослідження, випробування, що має на меті перевірку відповідності між реальною і очікуваною поведінкою програми на наборі тестів, розроблених з урахуванням вимог технічного завдання та алгоритмів роботи.

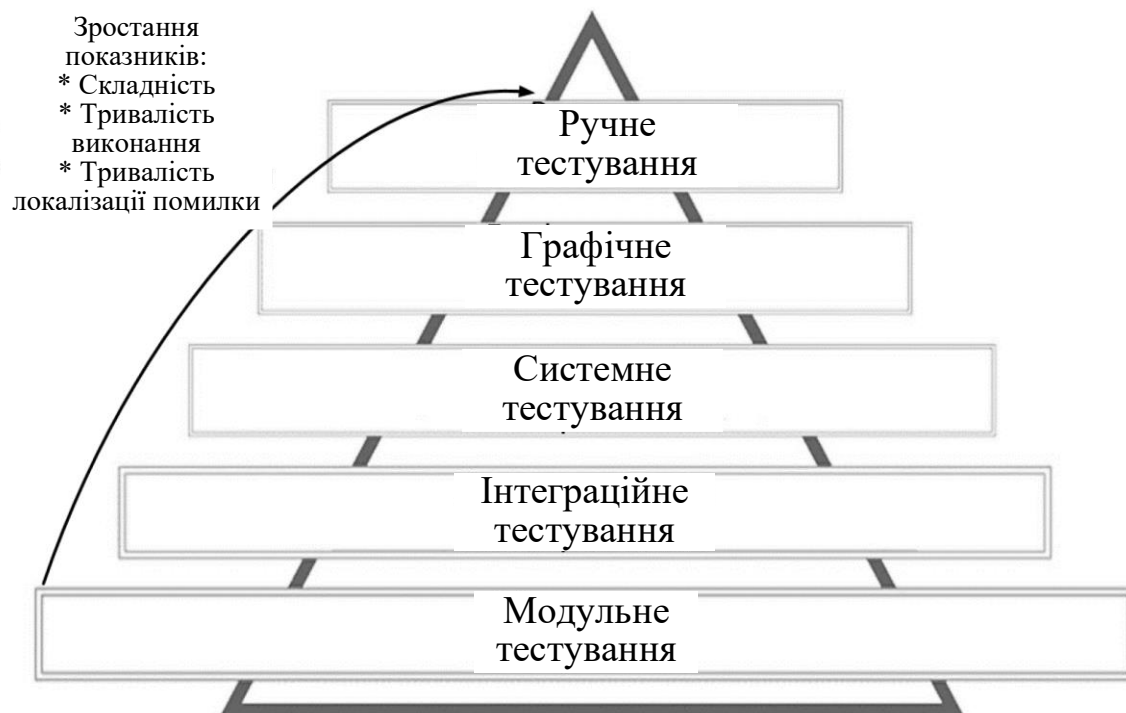


Рисунок 1. Види тестування

Для мікропроцесорних пристроїв проводяться всі типи тестування, при цьому організація інфраструктури тестування є завданням, що вимагає не тільки інженерного, а й наукового підходу. Тестування в залежності від циклу проектування програми використовує різні види. Ресурсна вартість і час проведення тестування визначається в залежності від сфери застосування програмного продукту.

В результаті аналізу робіт, присвячених питанням стійкості програмно-технічних комплексів до відмов, виявлено, що відомі методики виявлення несправностей на основі регламентованих методик випробувань пристроїв недостатньо ефективні і вимагають удосконалення. При цьому існуючі галузеві стандарти вказують на необхідність здійснення імітації несправностей при розробці (і в процесі макетування) мікропроцесорних пристроїв, але не визначають конкретних алгоритмів і необхідний комплекс технічних засобів для проведення випробувань.

Встановлено, що проектування унікальних і малосерійних пристроїв інформаційних комплексів, що мають складним для визначення або невідомі характеристики компонентів, пов'язане зі складнощами розрахунків традиційних показників надійності, тому потребує спеціально розробленому обладнанні для проведення експериментів для виявлення дефектів програмних і

апаратних засобів.

Визначено, що відсутня гармонізація між вітчизняними та зарубіжними стандартами в галузі проектування цифрових пристроїв, включаючи аналіз видів і наслідків відмов. Це ускладнює процес проектування і встановлення характеристик працездатності пристроїв в зв'язку з необхідністю заміни якісних оцінок безпеки і надійності при роботі пристрою в реальних умовах (використовуваних у вітчизняних стандартах) на кількісні показники (використовувані зарубіжними стандартами). Виходом зі сформованої ситуації є застосування експериментальних досліджень, що включають імітацію несправностей для оцінки працездатності програм і апаратури спільно.

Встановлено, що існуючі імітатори несправностей для дослідження і забезпечення працездатності цифрових інформаційних систем, представлені на комерційних ринках, є обладнанням, внутрішній устрій якого є захищається інтелектуальною власністю. У зв'язку з цим виникає необхідність створення власних коштів для імітації несправностей і аналізу подальшої реакції мікропроцесорних пристроїв, що при проектуванні є єдиним варіантом для створення відмовостійких систем.

Встановлено, що в зв'язку з тим, що використовуються мікропроцесорні елементи апаратних засобів відносяться до класу високонадійних виробів, то основною проблемою забезпечення працездатності проєктованих пристроїв є виявлення відмов, пов'язаних з дефектами програмного забезпечення, що їх виявляють в реальному апаратній середовищі. Для виявлення цих дефектів за доцільне розробка імітаторів несправностей, які дозволяють досліджувати коректність роботи всіх програмних функцій в режимах експлуатації пристрою.

Визначено актуальність дослідження, яка обумовлена зростаючими вимогами до якості і надійності програмно-апаратних комплексів, а також відсутністю практичних рекомендацій і недостатній ефективності існуючих методів і засобів для проектування і налагодження мікроконтролерних пристроїв.

## Висновки

Встановлено доцільність розробки алгоритмів і технічних засобів, які забезпечують виявлення програмних і апаратних дефектів в інформаційних системах і можуть бути застосовані в різних областях вітчизняної промисловості.

## СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Мартин, Р. Чистая архитектура. Искусство разработки программного обеспечения / Р. Мартин. – Санкт-Петербург: Питер, 2018. – 351 с.
2. Панков Д. А. Контроль и диагностика неисправностей программноаппаратного комплекса / Д. А. Панков, Л. А. Денисова // Омский научный вестник. – 2018. – № 2 (158). – С. 128–133.
3. Панков Д. А. Проектирование программно-аппаратного комплекса: определение объема тестовых испытаний микропроцессорных устройств / Д. А. Панков, Л. А. Денисова // Автоматизация в промышленности. – 2020. – № 12. – С. 23–29.
4. Пинкевич, В. Ю. Тестирование и отладка встраиваемых вычислительных систем на основе уровневых моделей / В. Ю. Пинкевич, А. Е. Платунов // Научнотехнический вестник информационных технологий, механики и оптики. – 2018. – Т. 18, № 5. – С. 801–808.
5. Похабов, Ю. В. Надежность в цифровых технологиях / Ю. В. Похабов // Надежность. – 2020. – Т. 20, № 2. – С. 3–11.

**Нікітович Діана Вікторівна** — аспірант, спеціальності 172-Телекомунікації та радіотехніка, Вінницький національний технічний університет, Вінниця, e-mail: diananikitovych@gmail.com

**Крещенко Марина Сергіївна** — студент групи ТКТ – 18б, Вінницький національний технічний університет

**Щербань Олег Андрійович** — студент групи ТКС – 20 м, Вінницький національний технічний університет

Науковий керівник: **Васильківський Микола Володимирович** — канд. техн. наук, доцент кафедри ТКСТБ, заступник декана факультету ІРЕН, Вінницький національний технічний університет, Вінниця, e-mail: [mvasylkivskyi@gmail.com](mailto:mvasylkivskyi@gmail.com)

**Nikitovich Diana V.** - graduate student, majoring in 172-telecommunications and radio engineering, Vinnytsia National Technical University, Vinnytsia, diananikitovych@gmail.com

**Khreshchenko Maryna S.** - student of TKT group - 18b, Vinnytsia National Technical University

***Shcherban Oleg A.*** - student of TKS group - 20 m, Vinnytsia National Technical University

Supervisor: ***Vasytkivskyi Mykola V.*** — Cand. Sc. (Eng), Assistant Professor of Telecommunication system and television, Vinnytsia National Technical University, Vinnytsia, e-mail: [mvasylkivskyi@gmail.com](mailto:mvasylkivskyi@gmail.com)