КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (22), 2023
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2023.22.134147
УДК 621.007.5:004.8

Толюпа Сергій Васильович
доктор технічних наук, професор, професор кафедри кібербезпеки та захисту інформації
Київський Національний університет імені Тараса Шевченка, Київ, Україна
ORCID 0000-0002-1919-9174
tolupa@i.ua

Самохвалов Юрій Якович
доктор технічних наук, професор, професор кафедри інтелектуальних технологій
Київський Національний університет імені Тараса Шевченка, Київ, Україна
ORCID 0000-0001-5123-1288
yu1953@ukr.net

Хусаінов Павло Валентинович
кандидат технічних наук, доцент, професор кафедри кібербезпеки
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна
ORCID 0000-0002-0675-0369
indesys@ukr.net

Штаненко Сергій Станіславович
кандидат технічних наук, доцент, доцент кафедри телекомунікаційних систем та мереж
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна
ORCID 0000-0001-9776-4653
sh_sergei@ukr.net

САМОДІАГНОСТУВАННЯ ЯК СПОСІБ ПІДВИЩЕННЯ КІБЕРСТІЙКОСТІ ТЕРМІНАЛЬНИХ КОМПОНЕНТІВ ТЕХНОЛОГІЧНОЇ СИСТЕМИ

Анотація. У статті запропоновано підхід щодо визначення технічного стану термінальних компонентів технологічної системи, основою яких є мікропроцесорні системи, реалізовані на програмно-реконфігурованій логіці. Проведено аналіз існуючих методів та способів тестування програмованих логічних інтегральних схем, розкриті недоліки та переваги. Доведено, що найбільш ефективним є метод використання схем самодіагностики BIST — Built-Inself-Test, який в подальшому може стати основою як контроль та діагностування мікропроцесорних систем, реалізованих на програмно-реконфігурованій елементній базі. Розглянуто існуючі методи визначення технічного стану мікропроцесорних систем, реалізованих на великих/надвеликих інтегральних схемах із жорсткою архітектурою, представлено математичний базис їхнього технічного діагностування. З метою підвищення кіберстійкості термінальних компонентів технологічної системи запропоновано за елементну базу використовувати програмовані логічні інтегральні схеми, які здатні змінювати внутрішню алгоритмічну структуру шляхом перепрограмування внаслідок кіберінцидентів та кібератак. При цьому реконфігурацію алгоритмічної структури мікропроцесорної системи в базисі програмно-реконфігурованої логіки запропоновано здійснювати за результатами самодіагностування, тобто шляхом застосування діагностичної системи з елементами штучного інтелекту, яка реалізує метод BIST — Built-Inself-Test. Передбачається, що синергізм мікропроцесорної системи та діагностичної системи з елементами штучного інтелекту дозволить реалізувати принцип активної відмовостійкості (кіберстійкості), який полягає в виявленні та локалізації несправностей (реагуванні на кіберінциденти та кібератаки), а також відновленні правильного функціонування термінальних компонентів технологічної системи шляхом реконфігурації їхньої внутрішньої алгоритмічної структури за результатами самодіагностування.

Ключові слова: кіберстійкість; технологічна система; термінальний компонент; мікропроцесорна система; програмно-реконфігурована логіка; самодіагностування; штучний інтелект.

ВСТУП

Постановка проблеми. Бурхливий розвиток мікропроцесорної техніки, зокрема масове застосування персональних комп'ютерів, засобів автоматизації, спеціалізованих й побутових обчислювальних пристроїв і систем, висунули на передній план проблему забезпечення надійного їхнього функціонування. В свою чергу, забезпечення необхідних показників надійності на різних етапах життєвого циклу складних технічних систем, якими є мікропроцесорні системи, неможливо без інтенсивного розвитку теорії та засобів технічної діагностики [1].

Сучасні мікропроцесорні системи широко використовуються в різних галузях науки і техніки, виробництві, сфері національної економіки, а також застосовуються як термінальні компоненти сучасних технологічних систем. При цьому згідно з [2] під технологічною системою будемо розуміти автоматизовані, автоматичні системи, які є сукупністю обладнання, засобів, комплексів та систем обробки, передачі та приймання, призначені для організаційного управління або управління технологічними процесами незалежно від наявності доступу системи до мережі Інтернет або інших глобальних мереж передачі даних.

Отже, враховуючи різноманітність та масовість використання мікропроцесорних систем у повсякденній діяльності людини, контроль та діагностування апаратних і програмних складових сучасної мікропроцесорної техніки є одним із найскладніших технологічних процесів. Його складність обумовлена потребою розуміння процесів, які відбуваються в середині мікропроцесорної системи, знанням архітектури процесора, системи команд, режимів адресації, управління операціями тощо. Контроль та діагностування також ускладнюється ступенем інтеграції елементної бази, яка інтегрована в мікро- та нанотехнології, відсутністю доступу до складових та контрольних точок мікропроцесорної системи, а також наявністю як елементної бази програмно-реконфігурованої логіки.

Так, наведені специфічні особливості мікропроцесорних систем, а також поява сучасної елементної бази у вигляді Програмованих Логічних Інтегральних Схем (ПЛІС) викликали значні зміни як у процесі проєктування мікропроцесорних систем, так і в процесі розробки методів й засобів контролю і діагностування (реагування на кіберінциденти та кібератаки) з метою виявлення та локалізації несправностей (порушень правильного функціонування), які пов'язані з фактором впливу кіберзагроз природного, технічного, технологічного та навмисного характеру.

Отже, розробка математичного базису технічного діагностування мікропроцесорних систем, які функціонують в умовах кіберзагроз та реалізовані на програмно-реконфігурованій елементній базі, є **актуальною задачею.**

Аналіз останніх досліджень і публікацій. На сьогодні задачам технічного діагностування мікропроцесорних систем присвячено велику кількість наукових праць. Так, у роботі [3] проведено досить повний аналіз існуючих методів контролю та діагностування, як універсальних, так і спеціалізованих обчислювальних систем, які синтезовані на інтегральних схемах із жорсткою архітектурою. Робота [4] присвячена лазерному діагностуванню мікропроцесорної техніки, яка застосовується в комічній галузі, де несприятливий вплив чинять важкі заряджені частинки — протони, альфа-частинки та іони великих енергій, що псують мікросхему, внаслідок чого з'являються програмні помилки або константові несправності. В роботі [5] діагностування мікропроцесорної системи на етапі проєктування здійснюється шляхом порівняння двох мікроархітектур мікропроцесорних систем нової та старої версії. При цьому висувається

гіпотеза, якщо при новій мікроархітектурі продуктивність мікропроцесорної системи вища за продуктивність при попередній мікроархітектурі, то проєкт вважається справним, незважаючи навіть на суттєву регресію продуктивності мікропроцесорної системи. В роботі [6] представлений метод тестування ПЛІС, який пов'язаний з формуванням списків несправностей при дедуктивному моделюванні для надання таблиці переходів послідовного пристрою у вигляді кубічного покриття в двотактному алфавіті. Але метод кубічного моделювання несправностей дуже добре підходить для ПЛІС першого покоління, які мають структуру комбінаційного типу на відміну від сучасних схем, які складаються з програмованих логічних блоків — макрокомірок. Робота [7] розглядає діагностування мікропроцесорних систем у базисі ПЛІС з точки зору самодіагностування, шляхом реалізації на рівні прошивки ПЛІС спеціалізованої схеми (пристрою), що дозволяє шляхом реалізації методу використання схем самотестування (BIST — Built-Inself-Test), методу повторювальних тестових множин та методу зчитування вихідних відгуків у вигляді вбудованих інтерфейсів оцінювати технічний стан мікропроцесорної системи.

Проте проведений аналіз свідчить, що традиційні методи та способи контролю та діагностування мікропроцесорних систем орієнтовані, як правило, на конкретну архітектуру, що не завжди є прийнятним для використання щодо іншої архітектури. Також має місце контроль і діагностування не самої мікропроцесорної системи, а її складових (процесора, модулів пам'яті, модулів введення/виведення даних, периферійного обладнання), що являють собою окремі інтегральні мікросхеми, на відміну від ПЛІС, які реалізовані за принципом System-on-Chip. Крім цього, запропоновані методи і способи діагностування мікропроцесорних систем у базисі ПЛІС визначають, як правило, технічний стан з точки зору справного та працездатного стану, на відміну від стану правильного функціонування, який може бути порушений згідно з [3] не лише несприятливим впливом природного, технічного та технологічного характеру, а і несприятливим впливом навмисного характеру, а саме цілеспрямованими кібератаками. Крім цього слід зазначити, що на сьогодні особливу загрозу несуть вразливості нульового дня (zero day), проти яких ще не розроблено механізми захисту, а також апаратні закладки (hardware backdoor), які являють собою заздалегідь вбудовані в пристрій електронні схеми, які здатні втручатися в роботу мікропроцесорної системи, переводячи її в стан неправильного функціонування або повного виведення її з ладу.

Мета статті. Підхід до самодіагностування мікропроцесорних систем у базисі програмно-реконфігурованої логіки з метою виявлення порушення правильного функціонування потоків виконання термінальних компонентів технологічної системи внаслідок цілеспрямованих кібератак.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Контроль та діагностування мікропроцесорних систем

Мікропроцесорна система як об'єкт контролю та діагностування є складною обчислювальною структурою. З погляду організації процесу контролю та діагностування мікропроцесорна система характеризується сукупністю параметрів X_i, $i=\overline{1,\ r}$ та може бути описана математичною моделлю M_j, $i=\overline{1,\ r}$, з тим чи іншим ступенем адекватності. За даною моделлю визначаються показники (параметри), які оцінюються

за допомогою технічних засобів. При цьому діагностична модель використовує принципи загальної теорії ідентифікації, тобто спостереження, керування та помітність.

Мікропроцесорна система називається повністю спостережувальною на інтервалі часу t_0, t, якщо її початковий стан $X(t_0)$ можна визначити за виміряним на цьому ж інтервалі вектор $Y(t)$. Мікропроцесорна система називається повністю керованою, якщо із деякого початкового стану $Y(t_н) \in D$ вона може бути переведена у будь-який інший стан $Y(t_1) \in D$ за кінцевий інтервал часу $\tau = t_1 - t$ впливом на неї управління $Y(t) \in G$, де G — деякий заданий клас функцій. Так, розглянуті перші дві властивості дозволяють визначити технічний стан мікропроцесорної системи, сформулювати умови працездатності та помітності, а також оцінити можливості їх реалізації. Зазначимо, що умовами працездатності є правила, які поділяють кінцеву множину X можливих станів мікропроцесорної системи на підмножини працездатних X_0 і непрацездатних $X_н$ станів, $X = X_0 \bigcup X_н$. При цьому ознакою наявності несправності є перебування мікропроцесорної системи в стані (працездатний, справний та правильно функціонуючий), що відноситься до підмножини $X_н$.

Так, визначення технічного стану мікропроцесорних систем нині проводиться Системами Контролю та Діагностування (СКД). При цьому під контролем розуміється процес отримання інформації, що дозволяє визначити технічний стан (справний та працездатний) мікропроцесорної системи шляхом застосування апаратних, програмних і комбінованих методів і засобів контролю, а також відповідність отриманої інформації вимогам, що висуваються до системи [8].

Діагностування, у свою чергу, є сукупністю задач перевірки правильного функціонування мікропроцесорної системи, а також задач виявлення та локалізації несправностей, що порушують правильне функціонування [9]. У більшості випадків всі ці задачі вирішуються Вбудованими Системами Контролю та Діагностування (ВСКД) мікропроцесорних систем.

Слід зауважити, що існуючі СКД розробляються на стохастичних та детермінованих принципах. Стохастичні СКД будуються на основі ймовірнісних моделей об’єктів контролю та випадкових стимулюючих впливів. Детерміновані СКД засновані на детермінованих моделях об’єктів контролю та регулярних методах побудови стимулюючих впливів у інтегрованому середовищі Систем Автоматизованого Проєктування (САПР). Враховуючи, що детерміновані СКД вимагають значних обчислювальних ресурсів, найбільш перспективними є СКД, побудовані на стохастичних принципах.

Зазначимо, що визначення технічного стану мікропроцесорних систем стохастичними методами виконується, як у процесі їхнього функціонування, так і в перервах між роботою. Так, на першому етапі в якості систем пошуку і виявлення несправності, як правило, використовуються ВСКД. На наступних етапах з метою виявлення та локалізації несправностей можуть використовуватися як ВСКД так і спеціалізовані діагностичні засоби вбудованого та зовнішнього виконання. При цьому основною задачею діагностичних засобів є збирання та обробка діагностичної інформації, а також виявлення несправностей шляхом перевірки ознак наявності несправностей.

Так, для мікропроцесорних систем ознаками наявності несправностей є відхилення діагностичних параметрів від номіналу, вихід характеристик за допустимі межі, відсутність логічних сигналів перемикання тощо. Загалом наявність несправностей визначається перевіркою виконання умов:

ISSN 2663 - 4023

$$x_i = \begin{cases} 1 \text{ при } y_i > y_{i0} \\ 0 \text{ при } y_i < y_{i0}; \end{cases} \qquad \bar{x}_i = \begin{cases} 1 \text{ при } y_i < y_{i0}; \\ 0 \text{ при } y_i > y_{i0}; \end{cases}$$

де x_i, $\bar{x}_{i0}$ — ознаки i-несправності; y_i, y_{i0} — поточне та еталонне значення діагностичного параметра.

Зазначимо, що діагностична інформація про технічний стан мікропроцесорної системи визначається, як правило, у контрольних точках у вигляді значень діагностичних параметрів, тобто у вигляді векторів діагностичних ознак у просторі технічного стану. Для мікропроцесорних систем діагностичними параметрами є: параметри на постійному струмі, динамічні параметри, а також функціональна поведінка [10].

Перевірка на постійному струмі призначена для виявлення грубих дефектів та несправностей. Метою перевірки динамічних параметрів є зміна різного роду часових співвідношень (час циклу, затримки тощо). Функціональні перевірки, в свою чергу, дозволяють визначити правильність функціонування мікропроцесорної системи та відсутність у неї несправностей. Для організації функціональних перевірок мікропроцесорних систем використовують робочі програми та спеціальні вбудовані тестові мікропрограми у поєднанні із зовнішніми апаратними засобами перевірок, порівнюють із еталонним мікропроцесором, який є свідомо справним, застосовуючи при цьому спеціальне тестове обладнання.

Отже, задача визначення технічного стану мікропроцесорної системи полягає у розпізнаванні двох станів: правильного (A_1) та неправильного функціонування (A_2). При цьому ситуація A_2 є об'єднанням великої кількості ймовірнісних подій (несправностей):

$$A_2 = \bigcup_{\mu=1}^{N} A_\mu ,$$

де $|N|$ — потужність простору технічного стану мікропроцесорної системи.

Враховуючи вищесказане, визначення технічного стану мікропроцесорної системи можна представити як задачу розпізнавання образів – прийняття рішення про належність поточної ситуації із заданим вектором діагностичних ознак до того чи іншого класу діагнозів $A_\mu, \mu = 1, N$. При цьому пошук рішень у просторі станів ґрунтується на перевірці статистичних гіпотез та математично формулюється наступним чином.

За вектором діагностичних ознак $X = \{x_1, ..., x_n\}$, де x_i — значення i-ї ознаки, необхідно знайти максимальне значення функції, що вирішується $A_k : H_k$, яка відноситься до класу A_μ, якщо вектор діагностичних ознак X належить до класу A_μ (1):

$$\exists_{\max} (A_\mu : H_k) \supseteq (X \in A_\mu). \qquad (1)$$

За такого підходу основна мета контролю та діагностування полягатиме у визначенні класу діагнозу, до якого належить ситуація A. Однак, при розпізнаванні мають справу також із ситуаціями A_μ, поділеними на множини (несправності) та відповідні множини технічних станів (множини несправностей або їх відсутності). При цьому вирішення задачі розпізнавання, тобто визначення технічного стану, зводиться до знаходження значень вирішальної функції, на основі якої вибирається гіпотеза про віднесення ситуації до того чи іншого класу технічних станів.

Зазначимо, що вирішення проблеми діагностування мікропроцесорних систем посилюється також наявністю нечітких даних через несприятливі впливи, внаслідок

цього пошук рішення буде відбуватись в умовах апріорної невизначеності. При цьому згідно з [11] серед існуючих методів вибору рішень в умовах невизначеності найбільш раціональними є методи нечіткої логіки, оскільки вони ґрунтуються на узагальненні та розвитку логіки предикатів. Це можемо побачити з виразу (1), де в якості предметної змінної предиката виступає вирішальна функція $A_\mu : H_k$, тобто гіпотеза H_k про віднесення ситуації A_μ на підставі вектора діагностичних ознак X. Враховуючи, що результатом аналізу є якість гіпотези при прийнятті рішення, то ця якість може бути оцінена градієнтом характеристичної функції $\lambda(A_k X)$.

$$\lambda(A_\mu X) = \begin{cases} 1 \text{ при } x \in A_\mu; \\ 0 \text{ при } x \notin A_\mu. \end{cases}$$

Градієнт являє собою мінімальний вектор прирощення діагностичних ознак $X = \{x_1, ..., x_\mu\}$, який усуває помилку класифікації, пред'явлену в процесі навчання. При цьому характеристична функція $\lambda(A_\mu X)$ може бути отримана у процесі навчання:

$$\lambda(A_\mu X) = \prod_{i=1}^{N} R_i(A_i, X),$$

де $R_i(A_i, X) = \begin{cases} 1 \text{ при } A_\mu : H_k \neq 0; \\ 0 \text{ при } A_\mu : H_k = 0. \end{cases}$

При цьому N — це місцевий двозначний предикат зв'язку вектора діагностичних ознак X із ситуацією A_i, що розпізнається. Зазначимо, що на методах нечіткої логіки ґрунтуються неповні рішення, які або переростають у гіпотези, або відкидаються.

Отже, під діагностуванням будемо розуміти вирішення задачі перевірки (контролю) правильного функціонування мікропроцесорної системи, а також задачі виявлення та локалізації несправностей, що порушують її правильне функціонування. За такої постановки задача діагностування передбачає, по-перше, задання простору можливих технічних станів (найбільш ймовірна несправність) і, по-друге, наявність формалізованих методів побудови засобів діагностування, реалізація яких забезпечить виявлення (розпізнавання) несправностей із заданого простору з необхідною достовірністю правильного діагностування (ймовірність правильного розпізнавання).

Розпізнавання технічного стану термінальних компонент технологічної системи

Сучасні технологічні системи, як було зазначено вище, являють собою комплекс апаратно-програмних засобів, а також персоналу, призначені для організаційного управління або управління технологічними процесами, включно з промисловим, електронним, комунікаційним обладнанням, іншими технічними та технологічними засобами.

Якщо розглядати сучасні технологічні системи на прикладі Автоматизованої Системи Управління Технологічними Процесами (далі — АСУ ТП) з точки зору структурної ієрархії, то очевидним стає питання кібербезпеки цих систем. Це пов'язано з тим, що вони відносяться до об'єктів критичної інфраструктури, представляють собою типові, багаторівневі, розгалужені людино-машинні системи управління, які представлені на трьох рівнях:

- верхній рівень реалізується шляхом застосування системи диспетчерського управління та збору даних у режимі реального часу (SCADA-система — Supervisory Control And Data Acquisition);
- середній та нижній рівень (рівень термінальних компонентів) реалізується за допомогою застосування програмованих логічних контролерів (PLC — Programmable Logic Controller) та контрольно-вимірювальних приладів.

Так, щорічний аналіз [12], представлений компаніями в галузі кібербезпеки АСУ ТП, показав, що загальна кількість виявлених інцидентів постійно зростає. Так 29% випадків виявлення вразливостей були пов'язані з промисловим мережевим обладнанням, а також із програмним пакетом SCADA і людино-машинним інтерфейсом. Крім цього, 21% вразливостей виявили в програмованих логічних контролерах. У 22% і 13% випадків вразливості були знайдені відповідно у програмному забезпеченні АСУ ТП та числовому програмному управлінні устаткування, що використовується. Ще 15% цілей зазначені у звітах як «інші».

Крім цього, проведений аналіз існуючих підходів щодо кіберзахисту АСУ ТП показав [13], що одним із перспективних напрямів забезпечення безпеки є створення інтелектуальних систем кібербезпеки, які будуть представляти частину загальної системи інформаційної безпеки. При цьому в основу побудови запропонованої системи має бути покладено поняття «еволюція (розвиток)», тобто здатність адаптації системи через зміну параметрів під впливом зовнішніх і внутрішніх кіберзагроз шляхом застосовуваних технологій протидії кібератакам протягом усього життєвого циклу.

При цьому передбачається, що система кібербезпеки АСУ ТП з елементами штучного інтелекту повинна забезпечити не тільки виявлення нових і невідомих кіберінцидентів і кібератак під час моніторингу (розвідки) кіберпростору, а й проведення аналізу виявлених кіберінцидентів і кібератак та автоматичний вибір параметрів функціонування АСУ ТП внаслідок несприятливих впливів без погіршення її основних характеристик.

Так, в роботі [14] з метою інтелектуалізації системи кібербезпеки АСУ ТП запропоновано застосування Експертної Системи (ЕС) шляхом інтеграції її в верхній рівень ієрархії, тобто в SCADA-систему. Крім цього основою середнього та нижнього рівня повинні стати ПЛІС, в якості систему контролю та діагностування яких запропоновано використовувати вбудовану в програмовану інтегральну логіку нейронну мережу. Вважається, що реалізація запропонованого підходу наділить АСУ ТП властивістю кіберстійкості через реалізацію активної відмовостійкості термінальних компонент технологічної системи, а саме виявлення та локалізація несправностей (кіберінцидентів та кібератак), а також відновлення правильного функціонування термінальних компонентів шляхом реконфігурації внутрішньої алгоритмічної структури за результатами самодіагностування.

Таким чином, на думку авторів, саме реалізація активної відмовостійкості термінальних компонент наділить технологічну систему властивістю кіберстійкісті за рахунок руйнування планів хакера на:

- створення прихованого захищеного каналу зовнішнього управління термінальними компонентами технологічної системи;
- довготривалий прихований збір внутрішньої інформації та приховане її виведення;
- прихована або явна модифікація (руйнування, знищення) інформації, параметрів технологічного процесу тощо.

При цьому слід розуміти, що головна ціль кібератаки — це задум, бажаний результат, форма набуття ефекту внаслідок виконання дій хакера. При цьому успішне досягнення кібератаки обумовлено необхідністю забезпечення певних обов'язкових умов, а саме:

- набуття хакером повноважень користувача та адміністратора для запуску на виконання в інфраструктурі технологічної системи зловмисних програм (скриптів, вірусів тощо);
- забезпечення відтворення повноважень запуску на виконання з правами користувача та адміністратора після перезавантаження, регламентних робіт для того чи іншого компонента технологічної системи;
- запобігання виявлення наявності у суб'єкта кібератаки повноважень в інфраструктурі технологічної системи шляхом відключення (блокування) захисних функцій.

Далі розглянемо більш детальніше питання щодо розпізнавання технічного стану термінальних компонент (мікропроцесорних систем) технологічної системи.

Як відомо, розпізнавання технічного стану визначається як комплекс задач, пов'язаних із перетворенням та обробкою вхідної інформації у вихідну. Вхідною інформацією служать портрети об'єкта контролю та діагностування (сигнали, параметри, ознаки об'єктів розпізнавання), а вихідною — прийняте рішення про віднесення об'єктів (образів), що розпізнаються, до деякого класу (діагнозу простору технічного стану).

Зазначимо, що процедура розпізнавання базується на математичному апараті теорії прийняття рішення про технічний стан об'єкта контролю та діагностування, і задача розпізнавання є, по суті, дискретним аналогом задачі пошуку оптимальних рішень.

Розглянута у загальному вигляді задача розпізнавання технічного стану може бути представлена у вигляді етапів її розв'язання (рис. 1).

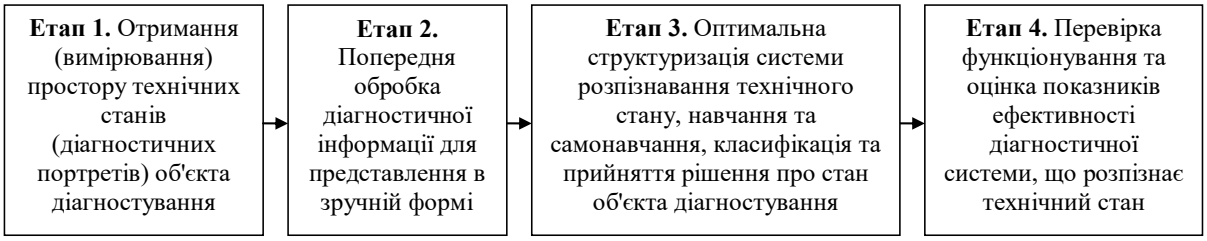

Рис. 1. Етапи вирішення задачі розпізнавання технічного стану

Так, враховуючи складність розпізнавання (визначення) технічного стану мікропроцесорних систем, в технічній діагностиці вже певний час чітко проявляється тенденція щодо використання елементів та компонентів штучного інтелекту як діагностичних систем. Зазначимо, що із загального переліку компонентів штучного інтелекту найбільший інтерес становлять експертні системи, нечітка логіка та штучні нейронні мережі. Розглянемо їх більш детальніше.

Експертні системи технічного діагностування являють собою програмні продукти, що виконують класифікацію мікропроцесорних систем та несправностей в них, проводять їхній аналіз та прогнозують поведінку мікропроцесорної системи в майбутньому [15]. В умовах невизначеності процесу діагностування або неповноти знань про мікропроцесорну систему, зокрема на структурному, функціональному чи алгоритмічному рівнях, ЕС можна використати для прийняття рішень щодо визначення технічного стану. В основу розробки ЕС діагностування мікропроцесорних систем

можуть бути покладені продукційні правила, фреймові та семантичні мережі, які підтримують увесь обсяг доступних знань про мікропроцесорну систему і процес діагностування.

Нечітка логіка. Правила нечіткої логіки дозволяють моделювати систему у разі неможливості застосування традиційних методів, а також замість точних математичних обчислень більш ефективно використовувати якісні оцінки технічного стану об'єкта діагностування. Однак методи нечіткої логіки не замінюють традиційні підходи, а навпаки, доповнюють їх. Для перетворення чітких вхідних значень діагностичних параметрів об'єкта діагностування на нечіткі вихідні, що характеризують його технічний стан, використовуються алгоритми Mamdani, Tsukamoto, Sugeno, Larsen, спрощений алгоритм нечіткого виведення, методи приведення до чіткості тощо.

Штучні нейронні мережі — це універсальний апроксиматор [16], що складається зі взаємопов'язаної сукупності простих обчислювальних елементів — нейронів. В результаті аналізу роботи нейронних механізмів мозку може бути відбудована множина моделей, які відрізняються одна від одної вихідними концепціями, рівнем узагальнень, запропонованих спрощень тощо. Схема використання нейронних мереж у багатьох випадках аналогічна схемі застосування ЕС, яка має як компонент придбання знань систему машинного навчання. В обох випадках за навчаючу вибірку використовується певна база емпіричних даних, після обробки яких система завдяки навчанню може успішно вирішувати важко формалізовані задачі. Однак, якщо в ЕС результат навчання буде представлений у базі даних в явному вигляді, то в нейронній мережі цей результат проявиться неявно і виразиться в зміні стану окремих нейронів і зв'язків між ними. На відміну від ЕС нейронні мережі не можуть давати пояснення з приводу отриманих результатів розв'язування важко формалізованих задач. Але висока швидкість навчання, завадостійкість до помилок роблять нейронну мережу альтернативою ЕС.

Так, згідно з [17] новим витком розвитку та застосування штучних нейронних мереж стала поява ПЛІС, які своєю організацією дозволили не лише проєктувати адаптивні мікропроцесорні системи, а й апаратно-програмним шляхом реалізувати нейрони, об'єднуючи їх у мережу. Крім цього, архітектура ПЛІС дозволила за допомогою мов опису апаратури синтезувати нейронні процесори, а також реалізувати метод Built-Inself-Test, шляхом розміщення нейронної мережі разом із мікропроцесорною системою на одному кристалі програмованої інтегральної схеми.

Розглянемо узагальнену структурну схему системи контролю та діагностування мікропроцесорної системи, яка реалізує метод Built-Inself-Test (рис. 2).

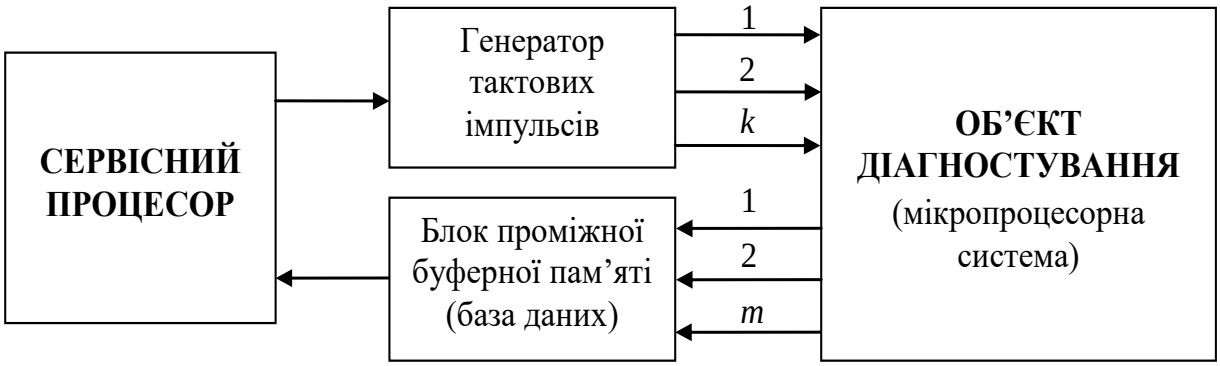

Рис. 2. Структурна схема системи самодіагностування

До складу системи самодіагностування мікропроцесорної системи входять: сервісний процесор, який формує блок тест-векторів і записує їх у генератор тактових імпульсів; блок проміжної буферної пам'яті для запам'ятовування відповідних реакцій; об'єкт діагностування (мікропроцесорна система). Принцип дії системи самодіагностування можемо інтерпретувати наступним чином. Генератор тактових імпульсів за сигналом сервісного процесора на основі записаного блоку тест-векторів формує тестові впливи, які через паралельні незалежні канали $1,...,k$ подаються на об'єкт діагностування. При подачі на об'єкт діагностування тестових впливів на його виходах з'являються сигнали відповідних реакцій, які в подальшому через канали $1,...,m$ фіксуються в блоці проміжної буферної пам'яті (база даних) та зчитуються сервісним процесором у вигляді векторів відповідних реакцій для подальшого аналізу. Так, в роботі [18] запропоновано структуру і приклад реалізації генератора тактових імпульсів системи діагностування на базі одношарової штучної мережі Хопфілда (рис. 3).

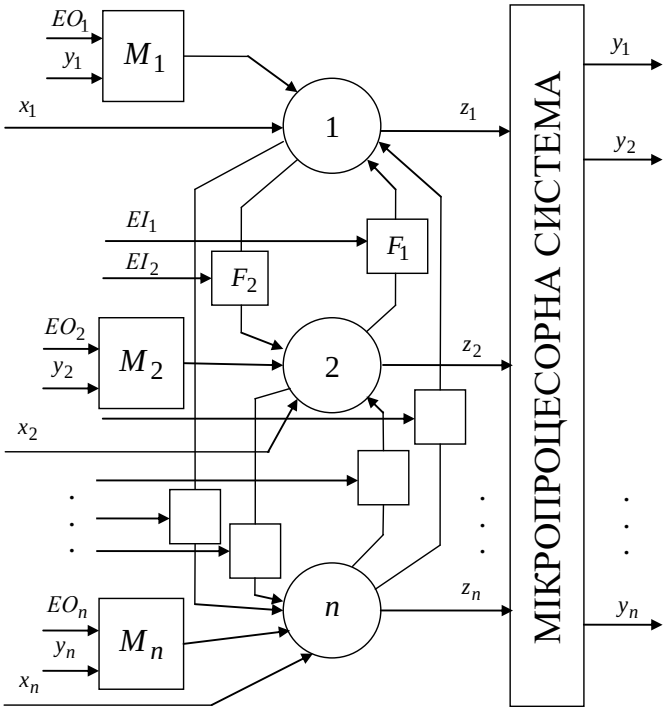

Рис. 3. Фрагмент структури генератора тактових імпульсівна нейронній мережі Хопфілда

При цьому принцип роботи генератора тактових імпульсів полягає в наступному. З виходів мікропроцесорної системи $y_1,...,y_n$ сигнали відповідних реакцій через елементи $M_1,...,M_n$, які виконують функцію дозволу чи заборони проходження сигналів, поступають для підсумовування на входи одиниць, які обробляються (нейрони) $1,...,n$. Вхідний сигнал кожної такої одиниці складається із зовнішнього по відношенню до замкнутої системи «Генератор тактових імпульсів — Мікропроцесорна системи» сигналу x_1 та зваженого «синаптичного» сигналу, який є результатом дії сигналу відповідної реакції з мікропроцесорної системи, і суми сигналів $\sum_{j=1}^{n-1} w_j$, що поступають із дозволених виходів

інших одиниць. З урахуванням початкового внутрішнього стану одиниць T, що обробляються, вихідний сигнал i-ї одиниці, що обробляється, визначається рівнянням:

$$f_i = x_i + \sum_{i=1}^{n} T_i + \sum_{j=1}^{n-1} w_j \ .$$

Діагностування мікропроцесорної системи закінчується при ітераційному повторенні сталого стану нейронної мережі. При збіганні стану нейронної мережі із станом для еталонної мікропроцесорної системи — мікропроцесорна система, яка діагностується, вважається справною, в іншому випадку вважається несправною. При цьому аналіз розбіжностей еталонного стану та стану мікропроцесорної системи, яка діагностується, дає інформацію про тип і місце прояву несправності.

Так, на сьогодні існує велика кількість штучних нейронних мереж, які можемо класифікувати як: одношарові та багатошарові мережі, нейронні мережі з прямим зв'язком (односпрямовані) та мережі з оберненим зв'язком (рекурентні), гетероасоціативні мережі Коско та автоасоціативні нейронні мережі Хопфілда, радіально-базисні нейронні мережі та самоорганізаційні карти Кохонера. Але серед всього різноманіття особливий інтерес для діагностування мікропроцесорних систем становлять нейронні мережі з оберненими зв'язками. Застосування таких мереж дає діагностичній системі можливість самонавчатись, використовуючи еталон. При цьому суть самонавчання зводиться до того, що маючи еталонну мікропроцесорну систему, система самодіагностування сама генерує тест. Якщо мікропроцесорна система несправна, система самодіагностування вказує місце прояву несправностей та заносить ознаки несправностей в блок проміжної буферної пам'яті (база даних), а також заносить і ті несправності, які проявилися вперше.

Таким чином, розглянутий підхід до розпізнавання технічного стану, в основі якого лежить принцип самодіагностування, що реалізований за допомогою нейронної мережі, значно підвищує ефективність процесу контролю і діагностування (реагування на кіберінциденти та кібератаки) мікропроцесорних систем (термінальних компонентів) технологічної системи та відкриває нові можливості щодо автоматизації операції знаходження місця прояву несправностей (кіберінцидентів та кібератак) та поповнення бази даних про несправності (кіберінциденти та кібератаки).

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Запропоновано підхід до визначення технічного стану мікропроцесорних систем в базисі програмно-реконфігурованої логіки, які є основою термінальних компонентів технологічної системи. З метою автоматизації системи контролю та діагностування мікропроцесорних систем запропоновано реалізувати принцип самодіагностування, в основу якого покладено ідеї штучного інтелекту. При цьому синергізм мікропроцесорної системи та системи діагностування з елементами інтелектуалізації відкриває нові можливості щодо підвищення кіберстійкості термінальних компонентів технологічної системи завдяки реалізації принципу активної відмовостійкості мікропроцесорних систем, який полягає в виявленні та локалізації несправностей (реагуванні на кіберінциденти та кібератаки), а також у відновленні правильного функціонування мікропроцесорної системи шляхом реконфігурації її внутрішньої алгоритмічної структури за результатами самодіагностування.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Furber, S. (2017). Microprocessors: the engines of the digital age. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences, 473(2199),* 20160893. https://doi.org/10.1098/rspa.2016.0893
2. Про основні засади забезпечення кібербезпеки України, Закон України № 2163-VIII (2022) (Україна). https://zakon.rada.gov.ua/laws/show/2163-19#Text.
3. Штаненко, С., Самохвалов, Ю., & Толюпа, С. (2023). Методичний підхід до відновлення правильного функціонування вбудованих систем на рівні програмованої елементної бази. *Системи і технології зв'язку, інформатизації та кібербезпеки, (3),* 171–181.
4. Pena-Fernandez, M., Lindoso, A., Entrena, L., Lopes, I., & Pouget, V. (2021). Microprocessor Error Diagnosis by Trace Monitoring Under Laser Testing. *IEEE Transactions on Nuclear Science, 68(8),* 1651–1659. https://doi.org/10.1109/tns.2021.3067554
5. Barboza, E., Jacob, S., Ketkar, M., Kishinevsky, M., Gratz, P., & Hu, J. (2021). Automatic Microprocessor Performance Bug Detection. *2021 IEEE International Symposium on High-Performance Computer Architecture (HPCA).* IEEE. https://doi.org/10.1109/hpca51647.2021.00053
6. Хаханов, В., Сысенко, И., Джахирул, Х., & Мехеди, М. (2001). Кубическое моделирование неисправностей цифровых проектов на основе FPGA, CPLD. *Радиоэлектороника, информатика, управление, (1),* 123–129.
7. Shtanenko, S., Samokhvalov, Y., Iohov, O., & Maliuk, V. (2022). Microprocessor systems based on programmable logic devices as an object of diagnostics. *Advanced Information Systems, 6(1),* 81–87. https://doi.org/10.20998/2522-9052.2022.1.14
8. Пинкевич, В., & Платунов, А. (2018). Тестирование и отладка встраиваемых вычислительных систем на основе уровневых моделей. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics, 18(5 (117)),* 801–808.
9. Иыуду, К. (1989). *Надежность, контроль и диагностика вычислительных машин и систем*.
10. Локазюк, В., & Заєць, О. (2000). Тестове комбіноване діагностування персональних комп'ютерів. *Вимірювальна та обчислювальна техніка в технологічних процесах*, 160–163.
11. Герасимов, Б., Камишин, В., & Самойлов, І. (2007). Інтелектуальне діагностування складних технічних систем. *Науково-технічна інформація, (1),* 3–7.
12. *Australian Cyber Security Centre, Annual-Threat-Report. jule 2021 - june 2022.* (б. д.). https://www.cyber.gov.au/sites/default/files/2023-03/ACSC-Annual-Cyber-Threat-Report-2022_0.pdf.
13. Бородакий, Ю. (2013). Кибербезопасность как основной фактор национальной и международной безопасности XXI века (Часть 1). *Вопросы кибербезопасности, (1 (2)),* 2–9.
14. Толюпа, С., Самохвалов, Ю., & Штаненко, С. (2021). Забезпечення кібербезпеки АСУ ТП шляхом застосування ПЛІС технології. *Безпека інформаційних систем і технологій, (1),* 45–54.
15. Поморова, О. (2007). *Теоретичні основи, методи та засоби інтелектуального діагностування комп'ютерних систем* [Неопубл. автореф. автореф. дис. … д-ра техн. наук.].
16. Герасимов, Б., Локазюк, В., Оксіюк, О., & Поморова, О. (2007). *Інтелектуальні системи підтримки прийняття рішень*. Видавництво Європейського університету.
17. Shtanenko, S., Samokhvalov, Y., Toliupa, S., & Silko, O. (2023). The Approach to Assessment of Technical Condition of Microprocessor Systems that Are Implemented on Integrated Circuits with a Programmable Structure. *Emerging Networking in the Digital Transformation Age, 965*. https://doi.org/10.1007/978-3-031-24963-1_28
18. Локазюк, В., Поморова, О., & Домінов, А. (2001). *Інтелектуальне діагностування мікропроцесорних пристроїв та систем. Навчальний посібник для вузів*.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (22), 2023
ISSN 2663 - 4023

Serhii Toliupa
Doctor of Sciences, professor, professor of the Department of Cyber Security and Information Protection
Taras Shevchenko National University, Kyiv, Ukraine
ORCID 0000-0002-1919-9174
tolupa@i.ua

Yurii Samokhvalov
Doctor of Sciences, professor, professor of the Department of Intellectual Technologies
Taras Shevchenko National University, Kyiv, Ukraine
ORCID 0000-0001-5123-1288
yu1953@ukr.net

Pavlo Khusainov
PhD, associate professor, professor of the Department of Cyber Security
Heroes of Kruty Military Institute of Telecommunications and Informatization, Kyiv, Ukraine
ORCID 0000-0002-0675-0369
indesys@ukr.net

Serhii Shtanenko
PhD, associate professor, associate professor of the Department of Telecommunication Systems and Networks
Heroes of Kruty Military Institute of Telecommunications and Informatization, Kyiv, Ukraine
ORCID 0000-0001-9776-4653
sh_sergei@ukr.net

SELF-DIAGNOSIS AS A WAY TO INCREASE THE CYBER RESISTANCE OF TERMINAL COMPONENTS OF A TECHNOLOGICAL SYSTEM

Abstract. The article proposes an approach to determine the technical condition of the terminal components of the technological system, the basis of which are microprocessor systems implemented on software-reconfigurable logic. The existing methods and methods of testing programmable logic integrated circuits are analyzed, the shortcomings and advantages are revealed. It has been proven that the most effective method of using self-diagnosis schemes is BIST — Built-Inself-Test, which in the future can become the basis for monitoring and diagnosing microprocessor systems implemented on a software-reconfigurable element base. The existing methods of determining the technical condition of microprocessor systems implemented on large/very large integrated circuits with rigid architecture are considered, and the mathematical basis of their technical diagnosis is presented. In order to increase the cyber resistance of the terminal components of the technological system, it is proposed to use programmable logic integrated circuits as an element base, which are able to change the internal algorithmic structure by reprogramming as a result of cyber incidents and cyber attacks. At the same time, the reconfiguration of the algorithmic structure of the microprocessor system on the basis of program-reconfigurable logic is proposed to be carried out based on the results of self-diagnosis, that is, by using a diagnostic system with elements of artificial intelligence, which implements the BIST — Built-Inself-Test method. It is assumed that the synergy of the microprocessor system and the diagnostic system with elements of artificial intelligence will allow the implementation of the principle of active fault tolerance (cyber resilience), which consists in the detection and localization of malfunctions (response to cyber incidents and cyber attacks), as well as the restoration of the correct functioning of the terminal components of the technological system by reconfiguring their internal algorithmic structure according to the results of self-diagnosis.

Keywords: cyber resilience, technological system, terminal component, microprocessor system, software-reconfigurable logic, self-diagnosis, artificial intelligence.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Furber, S. (2017). Microprocessors: the engines of the digital age. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences, 473(2199),* 20160893. https://doi.org/10.1098/rspa.2016.0893.
2. On the Basic Principles of Cybersecurity in Ukraine, Law Of Ukraine No. 2163-VIII (2022) (Ukraine). https://zakon.rada.gov.ua/laws/show/2163-19#Text.
3. Shtanenko, S., Samokhvalov, Y., & Toliupa, S. (2023). A methodical approach to restoring the correct functioning of embedded systems at the level of the programmable element base. *Systems and technologies of communication, informatization and cyber security, (3),* 171–181.
4. Pena-Fernandez, M., Lindoso, A., Entrena, L., Lopes, I., & Pouget, V. (2021). Microprocessor Error Diagnosis by Trace Monitoring Under Laser Testing. *IEEE Transactions on Nuclear Science*, *68*(8), 1651–1659. https://doi.org/10.1109/tns.2021.3067554.
5. Barboza, E. C., Jacob, S., Ketkar, M., Kishinevsky, M., Gratz, P., & Hu, J. (2021). Automatic Microprocessor Performance Bug Detection. *2021 IEEE International Symposium on High-Performance Computer Architecture (HPCA)*. IEEE. https://doi.org/10.1109/hpca51647.2021.00053/
6. Khakhanov, V., Sysenko, I., Dzhakhyrul, Kh., & Mekhedy, M. (2001). Cubic fault modeling of digital projects based on FPGA, CPLD. *Radio electronics, computer science, control, (1),* 123–129.
7. Shtanenko, S., Samokhvalov, Y., Iohov, O., & Maliuk, V. (2022). Microprocessor systems based on programmable logic devices as an object of diagnostics. *Advanced Information Systems*, *6(1),* 81–87. https://doi.org/10.20998/2522-9052.2022.1.14.
8. Pinkevich, V., & Platunov, A. (2018). Testing and debugging of embedded computing systems based on level models. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics, 18(5(117)),* 801–808.
9. Iyudu, K. (1989). Reliability, control and diagnostics of computers and systems.
10. Lokaziuk, V., & Zaiets, O. (2000). Test combinations for diagnosing personal computers. Vimirival and computational technology in technological processes,160–163.
11. Herasymov, B., Kamyshyn, V., & Samoilov, I. (2007). Intelligent diagnostics of folding technical systems. *Scientific and technical information, (1),* 3–7.
12. *Australian Cyber Security Centre, Annual-Threat-Report. jule 2021 - june 2022.* https://www.cyber.gov.au/sites/default/files/2023-03/ACSC-Annual-Cyber-Threat-Report-2022_0.pdf.
13. Borodakii, Yu. (2013). Cybersecurity as a major factor in national and international security in the 21st century (Part 1). *Cybersecurity issues, (1 (2)),* 2–9.
14. Toliupa, S., Samokhvalov, Y., & Shtanenko, S. (2021). Cyber security of automated process control systems is based on the use of FPLI technology. *Security of information systems and technologies, (1),* 45–54.
15. Pomorova, O. (2007). Theoretical foundations, methods and features of intelligent diagnostics of computer systems [Unpublished. abstract abstract dis. ...Dr.Tech. sciences.].
16. Herasymov, B., Lokaziuk, V., Oksiiuk, O., & Pomorova, O. (2007). Intelligent support systems make decisions. Fellowship of the European University.
17. Shtanenko, S., Samokhvalov, Y., Toliupa, S., & Silko, O. (2023). The Approach to Assessment of Technical Condition of Microprocessor Systems that Are Implemented on Integrated Circuits with a Programmable Structure. *Emerging Networking in the Digital Transformation Age*, *965*. https://doi.org/10.1007/978-3-031-24963-1_28.
18. Lokaziuk, V., Pomorova, O., & Dominov, A. (2001). Intelligent diagnostics of microprocessor devices and systems. Study guide for universities.