УДК 004.052.42
DOI https://doi.org/10.26661/2413-6549-2020-2-07

НЕЙРОМЕРЕЖЕВА МОДЕЛЬ КОНТРОЛЮ АПАРАТНОЇ СУМІСНОСТІ КОМПОНЕНТІВ ІОТ-СИСТЕМИ

Тіменко А. В.
асистент кафедри комп'ютерних систем та мереж
Національний університет «Запорізька політехніка»
вул. Жуковського, 64, Запоріжжя, Україна
orcid.org/0000-0002-7871-4543
timenko.artur@gmail.com

Шкарупило В. В.
кандидат технічних наук, доцент,
доцент кафедри комп'ютерних систем і мереж
Національний університет біоресурсів і природокористування України
вул. Героїв Оборони, 15, Київ, Україна
orcid.org/0000-0002-0523-8910
shkarupylo.vadym@nubip.edu.ua

Смолій В. В.
кандидат технічних наук, доцент,
доцент кафедри комп'ютерних систем і мереж
Національний університет біоресурсів і природокористування України
вул. Героїв Оборони, 15, Київ, Україна
orcid.org/0000-0003-2834-6989
dr.v.smoliy@gmail.com

Ключові слова: *апаратна сумісність, інтернет речей, моделювання, нейронна мережа, пристрій, функціональна безпека.*

У наш час парадигма інтернету речей здобуває більш широке розповсюдження. Прикладна її реалізація в глобальному масштабі потребує залучення спеціалізованих технологій та засобів. Один із напрямів, що потребує опрацювання, є забезпечення сумісності компонентів відповідних систем. Цю роботу присвячено розвитку вказаного напряму. Для цього у роботі розв'язується завдання розроблення моделі контролю сумісності компонентів системи інтернету речей на рівні апаратного забезпечення, що дозволятиме своєчасно попереджувати відмови та/або виходи зі строю компонентів системи.

У межах роботи розкривається складник представленого комплексного підходу до контролю сумісності компонентів системи інтернету речей на рівнях як програмного, так і апаратного забезпечень. При цьому акцент робиться саме на апаратній сумісності компонентів системи.

Запропоновано модель контролю апаратної сумісності компонентів системи інтернету речей, що будується на основі математичного апарату нейронних мереж. Апаратна сумісність компонентів системи розглядається з позиції функціональної безпеки останньої. Компонентами розглянуто пристрої на базі мікроконтролерів ESP 8266 і ESP 8285, що набули значного поширення, зокрема, завдяки низькій вартості їх придбання.

Практична значущість отриманих у роботі результатів полягає у такому: запропоновано засіб оцінювання актуального стану компонентів системи

інтернету речей, що дозволяє своєчасно виявити й усунути загрозу функціональній безпеці системи в цілому на рівні окремого компонента системи; запропоновано засіб прогнозування кількості таких компонентів упродовж заданого інтервалу часу.
Перевірку розробленої моделі побудовано на розв'язанні завдань апроксимації й екстраполяції. Показано, що прикладне використання запропонованої моделі дозволяє виявляти компоненти системи, що потребують налаштування або заміни, тобто порушують функціональну безпеку системи в цілому. Розв'язання задачі екстраполяції дозволяє прогнозувати кількість таких компонентів через заданий час.

NEURAL NETWORK BASED MODEL FOR IOT-SYSTEM COMPONENTS HARDWARE INTEROPERABILITY CONTROL

Timenko A. V.
Assistant at the Department of Computer Systems and Networks
"Zaporizhzhia Polytechnic" National University
Zhukovskoho str., 64, Zaporizhzhia, Ukraine
orcid.org/0000-0002-7871-4543
timenko.artur@gmail.com

Shkarupylo V. V.
Candidate of Technical Sciences, Associate Professor,
Associate Professor at the Department of Computer Systems and Networks
National University of Life and Environmental Sciences of Ukraine
Heroiv Oborony str., 15, Kyiv, Ukraine
orcid.org/0000-0002-0523-8910
shkarupylo.vadym@nubip.edu.ua

Smolii V. V.
Candidate of Technical Sciences, Associate Professor,
Associate Professor at the Department of Computer Systems and Networks
National University of Life and Environmental Sciences of Ukraine
Heroiv Oborony str., 15, Kyiv, Ukraine
orcid.org/0000-0003-2834-6989
dr.v.smoliy@gmail.com

Key words: *hardware interoperability, Internet of Things, simulation, neural network, device, functional safety.*

Nowadays, the Internet of Things paradigm is constantly becoming more and more widespread. Its implementation on a global scale requires the involvement of specialized technologies and tools. Among the directions to be worked out during that is to ensure the interoperability between the components of the corresponding systems. Given work is devoted to elaborate the specified direction. To this end, the following task is resolved: to develop the model of the Internet of Things system components interoperability control on a hardware plane – to provide an opportunity to detect the "potentially unsafe" components on time.
In presented work, the constituent of the proposed complex approach to the Internet of Things system components interoperability is revealed. Named approach encompasses the aspects of both software and hardware planes of interoperability. Within the given paper, the emphasis is put on a hardware plane though.
The model of hardware interoperability control between the components of the Internet of Things system has been proposed. The model is constructed on the basis of neural networks mathematical apparatus. Hardware interoperability between system components is approached from the standpoint of functional safety of a system as a whole. Devices based on ESP 8266 and ESP 8285 microcontrollers are considered as the components: in particular, due to being thoroughly widespread and accessible.

Practical significance of obtained results: proposed model allows identify and eliminate threats to the functional safety of the system as a whole at a component level by way of assessing the actual state of the latter. Moreover, an instrument for predicting the number of such components during a given time interval has been proposed.
Verification of the model proposed is based on solving the tasks of approximation and extrapolation. It has been demonstrated that implementation of the model allows to identify system components that need to be adjusted or replaced, i.e., violate the functional safety of the system as a whole. In turn, solving the extrapolation task makes it possible to predict the number of such components after a given time.

Вступ. Поточний характер застосування розподілених комп'ютерних систем можна охарактеризувати як всеохопний, адже тут мають місце чисельні сценарії успішної реалізації парадигми інтернету речей (IoT, Internet of Things) на практиці. Взаємодія компонентів відповідних систем здійснюється, зокрема, у межах концепцій «розумний дім», «розумне місто» тощо. Враховуючи специфіку названої парадигми, пристрої, призначені до взаємодії, мають бути сумісними на рівнях як програмного, так і апаратного забезпечень. При цьому питання програмної сумісності вирішуються, як правило, на рівні протоколів взаємодії [1]. На рівні контролю апаратної сумісності компонентів системи першорядного значення набуває питання забезпечення функціональної безпеки – режимів роботи, за яких система і відповідні компоненти функціонуватимуть згідно з очікуваннями, формалізованими у специфікації вимог, де регламентуються вимоги як до функціональних, так і до нефункціональних характеристик системи і компонентів.

Ідеєю, яка лежить в основі представленої роботи, є те, що апаратна сумісність компонентів IoT-системи розглядається з точки зору функціональної безпеки.

Згідно з положеннями стандарту ISO/IEC 21823-1:2019, сумісність (інтероперабельність) визначається як можливість двох або більше систем (компонентів систем) або додатків проводити обмін інформацією та спільно її використовувати [2]. При цьому виокремлюють, зокрема, такі площини функціональної сумісності компонентів IoT-системи: синтаксичну, семантичну, політики (взаємодії компонентів), поведінкову, транспортну. Однак варто зазначити, що проведено класифікацію саме на програмному рівні сприйняття системи. Водночас питання оцінювання рівню впливу чинників, що мають місце на апаратному рівні і є факторами, що порушують функціональну сумісність, потребує додаткового опрацювання. Сприянню вирішенню зазначеного питання і присвячено представлену роботу.

Центральна гіпотеза, що зумовлює актуальність проведених досліджень, – можливість реалізації функціональних характеристик IoT-системи будується, зокрема, на справності апаратного складника кожного з компонентів системи, тобто названа сумісність може бути порушена на апаратному рівні у зв'язку з виникненням збоїв та відмов обладнання. При цьому порушується питання забезпечення функціональної безпеки системи на рівні компонентів. Поняття «функціональна безпека» регламентується, зокрема, стандартом IEC 61508 [3]. Воно полягає у здатності системи виконувати свої функції та зберігати зазначені властивості в межах визначених режимів експлуатації.

Отже, питання сумісності розглядається з точки зору апаратного складника системи: зчитувані значення заданих показників функціонування компонентів системи використовуються як параметри розробленої моделі. У результаті застосування моделі робиться висновок про рівень критичності цих значень (критичний/некритичний).

Огляд літератури. Результати попередніх досліджень показали, що математичний апарат нейронних мереж є дієвим механізмом оцінювання і прогнозування стану компонентів розподіленої комп'ютерної системи [4]. Він забезпечує необхідний рівень гнучкості і масштабованості, надає зручний механізм варіювання складу параметрів моделі. Такими можуть виступати, зокрема, температура процесора, кількість обертів системи охолодження тощо [5].

У загальному сенсі забезпечення сумісності компонентів системи реалізується шляхом стандартизації (наприклад протокол IPv6, технологія RFID (Radio Frequency Identification)) [6].

Водночас вагомий внесок у напрямі розв'язання проблеми забезпечення сумісності компонентів IoT-системи викладається у нижченаведених підходах. Наприклад, для забезпечення сумісності пропонується залучати спеціалізовані програмні шлюзи (засоби сполучення) [7; 8], використовувати семантичні засоби [9; 10]. Однак такий підхід характеризується як прив'язкою до заданої предметної сфери, що суперечить парадигмі IoT, так і необхідністю ускладнення програмного складника, що породжує труднощі в масштабуванні системи. Перший зазначений недолік пропонується усувати шляхом забезпечення сумісності на рівні предметно орієнтованих застосунків [11]. Альтернативний підхід, у якому оминається останній зазначений недолік, базується на застосуванні спеціалізованих засобів трансляції протоколів взаємодії компонентів системи [12]. Це може створити перешкоди для реалізації сценаріїв взаємодії, сприйнятливих до

пропускної спроможності каналів обміну даними між пристроями.

Підсумувати доробок вищерозглянутих праць можна так: питання забезпечення сумісності охоплюється на програмному рівні. На противагу цьому серед нечисленних вітчизняних публікацій з окресленої тематики можна виокремити роботи професора Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського» В.В. Пілінського, де проблема сумісності компонентів IoT-системи розглядається з точки зору електромагнітної сумісності пристроїв у складі системи, тобто вирішується вже на рівні апаратного забезпечення [13].

Узагальнити розглянуті підходи можна так: сумісність компонентів IoT-системи не розглядається з позиції функціональної безпеки. Це породжує сумніви стосовно тривалості реалізації функціональних характеристик результувальною системою у заданих режимах роботи, з огляду на вимушену тимчасову несумісність певних компонентів системи, зумовленою апаратним складником відповідних компонентів. Зважаючи на це, в межах представленої роботи окреслена специфіка опрацьовується на рівні апаратного забезпечення: поточний стан апаратного забезпечення окремо взятого компонента системи розглядається як чинник, що зумовлює результувальну функціональну безпеку системи в цілому. Для комплексного оцінювання названого стану залучається математичний апарат нейронних мереж.

Як предметну сферу розглянемо бездротову сенсорну мережу (WSN, Wireless Sensor Network), що є фундаментальним складником глобальної IoT-системи [14]. Як апаратне забезпечення компонентів системи розглянемо пристрої на базі мікроконтролерів ESP 8266 і ESP 8285, що набули значного поширення [15].

Методи. В основі роботи лежить математичний апарат нейронних мереж, що застосовується як засіб отримання кількісних оцінок показників апаратної сумісності компонентів системи інтернету речей.

Для перевірки розробленої моделі в роботі застосовано метод дискретно-подійного імітаційного моделювання, а також виконано задачу апроксимації й екстраполяції. Вирішення задачі апроксимації дозволило одержати апроксимальну функцію, що є базисом для розв'язання задачі екстраполяції. Розв'язання задачі екстраполяції дозволило прогнозувати кількість компонентів системи, що перешкоджатимуть реалізації функціональних характеристик останньої через заданий відрізок часу.

На підставі вищезазначеного стверджуємо, що розв'язуване в роботі завдання формулюється так: розробити модель контролю сумісності компонентів IoT-системи на рівні апаратного забезпечення, що дозволятиме своєчасно попереджувати відмови та/або виходи зі строю компонентів системи.

Ухвалено рішення сприяти розв'язанню завдання забезпечення сумісності на апаратному рівні в межах розробленого підходу на основі математичного апарату нейронних мереж шляхом оцінювання та прогнозування кількості відмов компонентів системи за заданий інтервал часу.

Результати. Поданий у роботі матеріал є викладенням складника запропонованого комплексного підходу до контролю сумісності компонентів IoT-системи та є присвяченим апаратному рівню останніх (рис. 1).

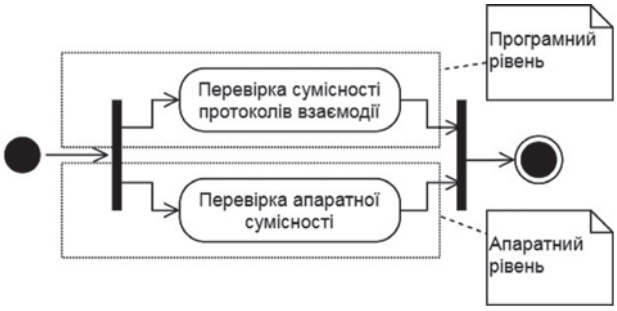

Рис. 1. Концептуальне подання розробленого підходу

Згідно із запропонованим підходом (рис. 1), контроль сумісності на програмному рівні має забезпечуватися шляхом здійснення формальної верифікації методом перевірки на моделі в автоматизованому режимі [1]. Як засіб контролю сумісності на апаратному рівні пропонується застосовувати математичний апарат нейронних мереж. Архітектуру побудованої мережі подано на рис. 2.

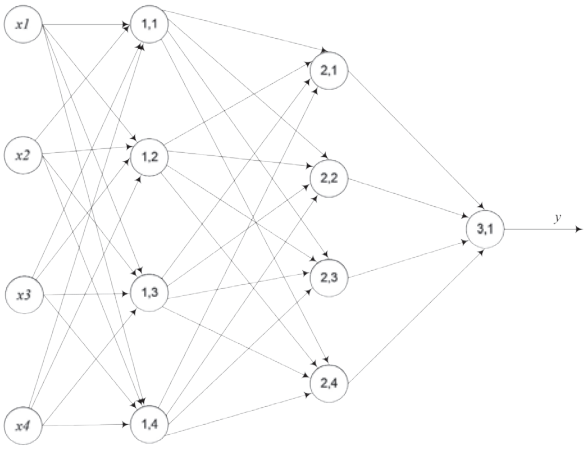

Рис. 2. Архітектура розробленої моделі

На рис. 2 на кожен елемент вхідного шару мережі подається по чотири параметри: значення температури

навколишнього середовища (x_1), рівнів вологості (x_2), вібрації (x_3), а також куту нахилу IoT-пристрою (x_4). При цьому кожен елемент кожного з трьох шарів мережі пронумеровано парою значень, де перше значення є порядковим номером шару мережі, друге – номером елемента в межах заданого шару. Результат роботи мережі зчитується на виході елемента $(3,1)$. Відповідна математична модель представлена системою рівнянь такого вигляду:

$$\begin{cases} Y_{NN} = \lambda_{(3,1)} = \left(1 + e^{-\left(-12.21+18.86\lambda_{(2,1)}-7.32\lambda_{(2,2)}+16.74\lambda_{(2,3)}-6.51\lambda_{(2,4)}\right)}\right)^{-1}; \\ \lambda_{(2,1)} = \left(1 + e^{-\left(-5.83+8.97\lambda_{(1,1)}-4.97\lambda_{(1,2)}-5.53\lambda_{(1,3)}+5.89\lambda_{(1,4)}\right)}\right)^{-1}; \\ \lambda_{(2,2)} = \left(1 + e^{-\left(-4.03+5.32\lambda_{(1,1)}+1.12\lambda_{(1,2)}+6.09\lambda_{(1,3)}-6.21\lambda_{(1,4)}\right)}\right)^{-1}; \\ \lambda_{(2,3)} = \left(1 + e^{-\left(-5.05+6.12\lambda_{(1,1)}-4.74\lambda_{(1,2)}+2.32\lambda_{(1,3)}+2.34\lambda_{(1,4)}\right)}\right)^{-1}; \\ \lambda_{(2,4)} = \left(1 + e^{-\left(-1.12+5.09\lambda_{(1,1)}+2.34\lambda_{(1,2)}-0.95\lambda_{(1,3)}+5.74\lambda_{(1,4)}\right)}\right)^{-1}; \\ \lambda_{(1,1)} = \left(1 + e^{-\left(1.73+0.27x_1-4.27x_2-4.15x_3-2.07x_4\right)}\right)^{-1}; \\ \lambda_{(1,2)} = \left(1 + e^{-\left(4.42-0.81x_1+0.36x_2-3.42x_3+5.39x_4\right)}\right)^{-1}; \\ \lambda_{(1,3)} = \left(1 + e^{-\left(-2.32-5.39x_1+1.89x_2+1.42x_3-1.89x_4\right)}\right)^{-1}; \\ \lambda_{(1,4)} = \left(1 + e^{-\left(6.09+2.13x_1-2.73x_2-1.12x_3-2.07x_4\right)}\right)^{-1}, \end{cases} \quad (1)$$

де Y_{NN} – результат роботи вихідного шару нейронної мережі, представленої єдиним елементом $(3,1)$ (рис. 2).

Отримані експериментальні дані подано в табл. 1. При цьому варто зазначити, що в табл. 1 наведено лише 5 із $1,92 \cdot 10^2$ проведених замірів, аби підкреслити найбільш показовий випадок (№ 5 з/п), за якого $x_4 = 149\,°$. Така ситуація демонструє випадок, коли положення пристрою в просторі порушено (як результат впливу вібрації). Установлено, що це стало наслідком неякісної фіксації пристрою в просторі.

Як наслідок, відповідний пристрій охарактеризовано як «несумісний», з огляду на те, що він є джерелом недостовірних даних. Недостовірними при цьому вважаються дані, що виходять за межі встановлених лімітів. Ужитими заходами є відновлення положення пристрою в просторі.

Таблиця 1

Вихідні дані та результати роботи моделі

№ з/п	Значення показників				Y_{NN}
	x_1, °C	x_2, %	x_3, Гц	x_4, °	
1	70	11	4	3	1
2	46	31	10	5	1
3	39	33	9	3	1
4	41	39	16	4	1
5	92	10	10	149	0

Із табл. 1 видно, що у випадку № 5 з/п одержуємо значення $Y_{NN} = 0$. Воно означає, що відповідний пристрій є несумісним, адже потребує налагодження або заміни. Фрагмент матриці вагових коефіцієнтів – співмножників показників $x_1, ..., x_4$ – подано в табл. 2.

Таблиця 2

Елементи матриці вагових коефіцієнтів

№ шару мережі	№ нейрона у шарі	Значення зміщення w_0	Параметри мережі та вагові коефіцієнти	
			Параметр	Значення w
1	1	1,73	x_1	0.27
			x_2	-4,27
			x_3	-4,15
			x_4	-2,07
	2	4,42	x_1	-0,81
			x_2	0,36
			x_3	-3,42
			x_4	-5,39

У табл. 2 значення коефіцієнтів w_0 і w отримано в результаті налаштування мережі.

Побудована нейромережева модель є ієрархічною структурою, елементами кожного з трьох ієрархічних рівнів якої є нейрони. При цьому верхній ієрархічний рівень представлений єдиним елементом $(3,1)$ (рис. 2). Прикладне застосування моделі дозволяє отримати оціночне значення агрегованого показника придатності заданого IoT-пристрою до використання як компонента цільової системи з позиції його апаратної сумісності. Значення середньоквадратичної помилки навчання склало $1,41 \cdot 10^{-14}$. Для тестової вибірки значення помилки склало вже $2,84 \cdot 10^{-5}$.

Проведене дослідження полягало в такому: впродовж року розроблена модель щомісяця застосовувалася як засіб аналізу параметрів кожного з компонентів. У результаті цього модель продукувала значення 1 або 0 для кожного із 16 компонентів щомісяця. Упродовж року щомісяця фіксувалася сума значень y за всіма компонентами. На основі одержаних даних вирішено задачу апроксимації (рис. 3).

На рис. 3 довірчі інтервали побудовано для довірчої імовірності 0,95. Із рис. 3 видно, що впродовж року безперервної роботи IoT-системи на основі 16 IoT-пристроїв вже на восьмому місяці експлуатації характеристики двох компонентів системи не відповідали штатному режиму їх функціонування. Застосування розробленої моделі дозволило виявити ці компоненти і виробити комплекс заходів, спрямованих на повернення зазначених компонентів до штатного режиму роботи.

До того ж розроблену модель можна застосовувати для прогнозування кількості компонентів сис-

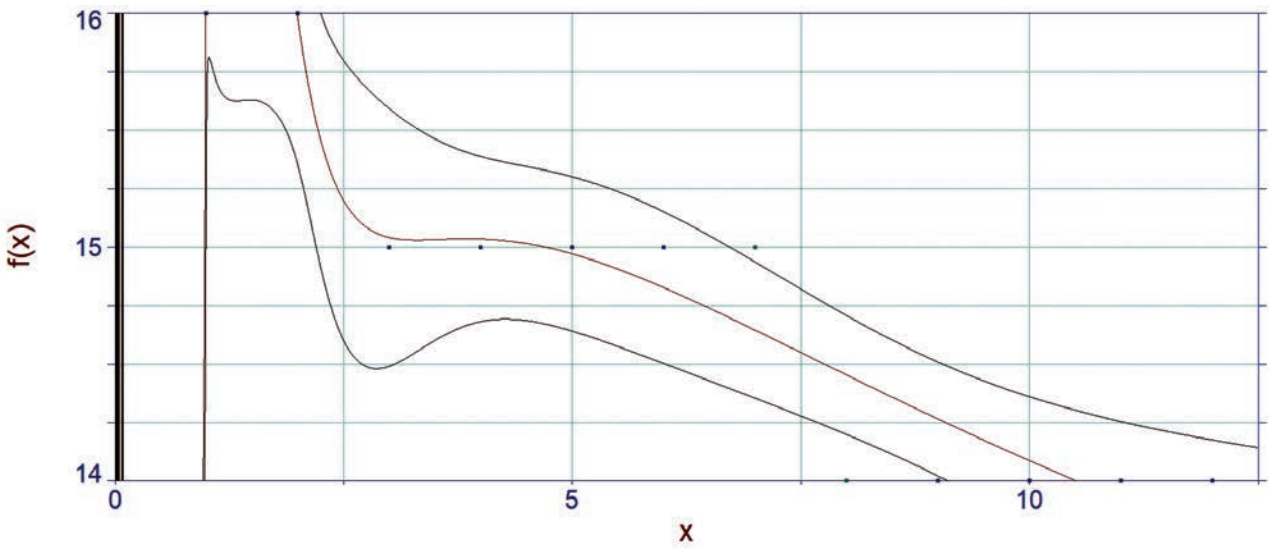

Рис. 3. Результат вирішення задачі апроксимації

теми, що вийдуть із ладу за заданий проміжок часу. Для дослідженого випадку апроксимувальну функцію представлено поліномом четвертого порядку:

$$f(x) = a + \frac{b}{x} + \frac{c}{x^2} + \frac{d}{x^3} + \frac{e}{x^4}, \qquad (2)$$

де $a = 11{,}0009$; $b = 47{,}5262$; $c = -198{,}7787$; $d = 338{,}4551$; $e = -182{,}2033$; x – порядковий номер місяця від початку відліку. Значення коефіцієнта детермінації при цьому таке: $R^2 = 0{,}92$. Для прогнозування кількості компонентів системи, ознаки функціонування яких не відповідатимуть штатному режиму, створено відповідний програмний засіб на основі апроксимувальної функції $f(x)$. Результат його застосування показав, що через 18 місяців безперервної роботи системи вже три її компоненти функціонуватимуть не в штатному режимі. Такий результат можна охарактеризувати як індикативний засіб для вироблення комплексу заходів, напрямлених на усунення змушувальних чинників потенційних збоїв у роботі IoT-системи.

Висновки. Таким чином, у роботі розроблено модель контролю сумісності компонентів IoT-системи на апаратному рівні, що базується на математичному апараті нейронних мереж.

Було отримано такі результати:

1) продемонстровано дієвість використання запропонованої моделі як засобу оцінювання придатності апаратного складника компонентів IoT-системи до цільового застосування для виявлення компонентів, що є несумісними з рештою компонентів системи за рівнем функціональної безпеки. При цьому як предметну сферу розглянуто сценарій згідно з концепцією «розумний дім». Для проведення дослідження залучено 16 пристроїв на основі мікроконтролерів ESP 8266 і ESP 8285. У результаті було виявлено один несумісний пристрій;

2) у результаті розв'язання завдань апроксимації й екстраполяції встановлено, що впродовж 18 місяців експлуатації системи вже три пристрої з 16 матимуть незадовільне значення показника сумісності. Отримане значення коефіцієнта детермінації для результату розв'язання задачі апроксимації – 0,92.

Запропонована модель на основі математичного апарату нейронних мереж є засобом оцінювання і прогнозування сумісності компонентів IoT-системи на апаратному рівні (з позиції функціональної безпеки). Особливістю представленого рішення є безпосередня залежність результату такого оцінювання як від складу вихідних даних (параметрів оцінювання), так і від установлених обмежень на допустимі значення цих параметрів.

Подальша робота орієнтована на узагальнення отриманих результатів шляхом розширення спектра охоплених сценаріїв прикладного використання досліджуваної IoT-системи.

ЛІТЕРАТУРА

1. Timenko A.V., Shkarupylo V.V., Oliinyk A.O., Hrushko S.S. Formal Model for Checking the Interoperability Between the Components of the IoT system. *Problemele Energeticii Regionale*. 2019. Vol. 40, No. 1-1. P. 69–78. DOI: https://doi.org/10.5281/zenodo.3239196
2. ISO/IEC 21823-1:2019 Internet of things (IoT) - Interoperability for IoT systems - Part 1: Framework. [Active since 2019-02]. URL: https://www.iso.org/standard/71885.html (access date: 05.01.2021).

3. IEC 61508 Edition 2.0. Functional safety of electrical/electronic/programmable electronic safety-related systems. [Approved: April 2010]. URL: https://www.iec.ch/functionalsafety/standards/page2.htm. (access date: 05.01.2021).
4. Tang J., Liu F., Zhang W., Ke R. Zoue Y. Lane-changes prediction based on adaptive fuzzy neural network. *Expert Systems with Applications*. 2018. Vol. 91. P. 452–463. DOI: https://doi.org/10.1016/j.eswa.2017.09.025
5. Тіменко А.В., Скрупська Л.С. Нейромережева модель прогнозування ймовірності безвідмовної роботи CPU на основі вимірювання температурних показників. *Наукові праці ДонНТУ: серія «Інформатика, кібернетика та обчислювальна техніка»*. 2018. № 1 (26). С. 106–111.
6. Al-Fuqaha A., Guizani M., Mohammadi M., Aledhari M., Ayyash M. Internet of things: a survey on enabling technologies protocols and applications. *IEEE Communications Surveys & Tutorials*. 2015. Vol. 17, No. 4. P. 2347–2376. DOI: http://www.arpnjournals.org/jeas/research_papers/rp_2020/jeas_1220_8427.pdf
7. Blackstock M., Lea R. IoT interoperability: A hub-based approach. *Internet of Things (IOT)*: proc. 2014 International Conference (Cambridge, MA, USA, 6–8 Oct. 2014). 2014. P. 79–84. DOI: https://doi.org/10.1109/IOT.2014.7030119
8. Pereira C., Pinto A., Aguiar A., Rocha P., Santiago F., Sousa J. IoT interoperability for actuating applications through standardised m2m communications. *A World of Wireless, Mobile and Multimedia Networks (WoWMoM)*: proc. 2016 IEEE 17th International Symposium (Coimbra, Portugal, 21–24 June 2016). 2016. P. 1–6. DOI: https://doi.org/10.1109/WoWMoM.2016.7523564
9. Desai P., Sheth A., Anantharam P. Semantic Gateway as a Service Architecture for IoT Interoperability. *Mobile Services*: proc. 2015 IEEE International Conference (New York, NY, USA, 27 June – 2 July 2015). 2015. P. 313–319. DOI: https://doi.org/10.1109/MobServ.2015.51
10. Aloi G., Caliciuri G., Fortino G., Gravina R., Pace P., Russo W., Savaglio C., Enabling IoT interoperability through opportunistic smartphone-based mobile gateways. *Journal of Network and Computer Applications*. 2017. Vol. 81, No. C. P. 74–84. DOI: https://doi.org/10.1016/j.jnca.2016.10.013
11. Soursos S., Podnar-Zarko I., Zwickl P., Gojmerac I., Bianchi G., Carrozzo G. Towards the Cross-Domain Interoperability of IoT Platforms. *Networks and Communication (EUCNC 2016)*: proc. 2016 European Conference (Athens, Greece, 27–30 June 2016). 2016. DOI: https://doi.org/10.1109/EuCNC.2016.7561070
12. Derhamy H., Eliasson J., Delsing J. Iot interoperability: On-demand and low latency transparent multiprotocol translator. *IEEE Internet of Things Journal*. 2017. Vol. 4, No. 5. P. 1754–1763. DOI: https://doi.org/10.1109/JIOT.2017.2697718
13. Пілінський В. В., Ратушний О. С., Тітков Д. В. Аналіз електромагнітної обстановки пристроїв Інтернету речей у приміщенні. *Вісник Національного технічного університету «ХПІ». Серія : Техніка та електрофізика високих напруг*. 2019. № 27 (1352). С. 50–54. URL: http://nbuv.gov.ua/UJRN/vcpitevn_2019_27_10 (дата звернення: 20.12.2020).
14. Kocakulak M., Butun I. An overview of Wireless Sensor Networks towards Internet of Things. *Proc. 2017 IEEE 7th Annual Computing and Communication Workshop and Conference, CCWC* (Las Vegas, NV, USA, 9-11 Jan. 2017). 2017. P. 1–6. DOI: https://doi.org/10.1109/CCWC.2017.7868374
15. Mesquita J., Guimaraes D., Pereira C., Santos F., Almeida L. Assessing the ESP8266 WiFi module for the Internet of Things. *Proc. 2018 IEEE 23rd International Conference on Emerging Technologies and Factory Automation, ETFA* (Turin, Italy, Sept. 4-7, 2018). 2018. DOI: https://doi.org/10.1109/ETFA.2018.8502562

REFERENCES

1. Timenko, A.V., Shkarupylo, V.V., Oliinyk, A.O., & Hrushko, S.S. (2019). Formal Model for Checking the Interoperability Between the Components of the IoT system. *Problemele Energeticii Regionale*, 40(1-1), 69–78. https://doi.org/10.5281/zenodo.3239196
2. International Organization for Standardization (2019). *Internet of things (IoT) - Interoperability for IoT systems - Part 1: Framework* (ISO/IEC Standard No. 21823-1:2019). https://www.iso.org/standard/71885.html
3. International Electrotechnical Commission (2010). *Functional safety of electrical/electronic/programmable electronic safety-related systems* (IEC 61508 Edition 2.0). https://www.iec.ch/functionalsafety/standards/page2.htm
4. Tang, J., Liu, F., Zhang, W., Ke, R. & Zoue, Y. (2018). Lane-changes prediction based on adaptive fuzzy neural network. *Expert Systems with Applications*, 91, 452–463. https://doi.org/10.1016/j.eswa.2017.09.025
5. Timenko, A.V., & Skrupskaya, L.S. (2018). Neural network model for predicting the probability of the CPU failure-free operation based on the measured temperature indicators. *Scientific papers of Donetsk National Technical University. Series: "Informatics, Cybernetics and Computer Science"*, 1(26), 106–111.

6. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: a survey on enabling technologies protocols and applications. *IEEE Communications Surveys & Tutorials*, 17(4), 2347–2376. https://doi.org/10.1109/COMST.2015.2444095
7. Blackstock, M., & Lea, R. (Oct. 2014). IoT interoperability: A hub-based approach. *Proc. 2014 International Conference on the Internet of Things (IOT)*, Cambridge, MA, USA. https://doi.org/10.1109/IOT.2014.7030119
8. Pereira, C., Pinto, A., Aguiar, A., Rocha, P., Santiago, F., & Sousa, J. (June 2016). IoT interoperability for actuating applications through standardised m2m communications. *Proc. 2016 IEEE 17th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM),* Coimbra, Portugal. https://doi.org/10.1109/WoWMoM.2016.7523564
9. Desai, P., Sheth, A., & Anantharam, P. (July 2015). Semantic Gateway as a Service Architecture for IoT Interoperability. *Proc. 2015 IEEE International Conference on Mobile Services*, New York, NY, USA. https://doi.org/10.1109/MobServ.2015.51
10. Aloi, G., Caliciuri, G., Fortino, G., Gravina, R., Pace, P., Russo, W., & Savaglio, C. (2017). Enabling IoT interoperability through opportunistic smartphone-based mobile gateways. *Journal of Network and Computer Applications*, 81(C), 74–84. https://doi.org/10.1016/j.jnca.2016.10.013
11. Soursos, S., Podnar-Zarko, I., Zwickl, P., Gojmerac, I., Bianchi, G., & Carrozzo, G. (June 2016). Towards the Cross-Domain Interoperability of IoT Platforms.: *Proc. 2016 European Conference on Networks and Communication (EUCNC 2016),* Athens, Greece. https://doi.org/10.1109/EuCNC.2016.7561070
12. Derhamy, H., Eliasson, J., & Delsing, J. (2017). Iot interoperability: On-demand and low latency transparent multiprotocol translator. *IEEE Internet of Things Journal*, 4(5), 1754–1763. https://doi.org/10.1109/JIOT.2017.2697718
13. Pilinsky, V.V., Ratushnyi, O.S., & Titkov, D.V. (2019). Analysis of the electromagnetic environment of internet of things devices indoors. *Bulletin of the National Technical University "KhPI". Ser. : Technique and Electrophysics of High Voltage*. 27(1352), 50–54. http://repository.kpi.kharkov.ua/handle/KhPI-Press/43637 (in Ukrainian)
14. Kocakulak, M., & Butun, I. (Jan. 2017). *An overview of Wireless Sensor Networks towards Internet of Things*. 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA. https://doi.org/10.1109/CCWC.2017.7868374
15. Mesquita, J., Guimaraes, D., Pereira, C., Santos, F., & Almeida, L. (Sept. 2018). *Assessing the ESP8266 WiFi module for the Internet of Things*. 2018 IEEE 23rd International Conference on Emerging Technologies and Factory Automation (ETFA), Turin, Italy. https://doi.org/10.1109/ETFA.2018.8502562