УДК 004.056.5
DOI: 10.31891/CSIT-2020-2-3

ЛИСЕНКО С. М., КОНДРАТЮК В. В.
Хмельницький національний університет

# МЕТОД ПРОГНОЗУВАННЯ РЕЗИЛЬЄНТНОСТІ КЛАУД-ОРІЄНТОВАНИХ КІБЕРФІЗИЧНИХ СИСТЕМ

*Застосування процесу прогнозування резильєнтності кіберфізичних систем за допомогою клауд-орієнтованих підвищує ефективну надійність та доступність КФС в її життєвому циклі за рахунок виявлення майбутніх збоїв та скорочення позапланового обслуговування. Процес прогнозування передбачає оцінку термінів корисної експлуатації, і здійснення пост прогностичного рішення щодо заходів з технічного обслуговування відповідно до заданих правил. Метод прогнозування резильєнтності клауд-орієнтованих кіберфізичних систем дозволяє визначити стан кіберфізичних систем із застосуванням хмарних обчислень. Механізм, що використовуються для зменшення витрат на обслуговуючі роботи та детального планування операцій з обслуговування, апарат генетичних алгоритмів.*

*Ключові слова: кіберфізична систем, резильєнтність, комп'ютерні системи, хмарні технології.*

LYSENKO S., KONDRATYUK V.
Khmelnytskyi National University, Khmelnytskyi, Ukraine

# METHOD FOR RESILIENCE FORECASTING OF THE CALAUD-ORIENTED CYBERPHYSICAL SYSTEMS

*Cyberphysical system is the integration of physical space (equipment, devices and people) with computing, communication and control systems (cyberspace). The National Institute of Standards and Terminology (NIST) has defined CFS as cyberphysical systems (CFS), which are designed systems built on the continuous integration of computational algorithms and physical components.*

*Improving the CFS provides greater opportunities for performance, adaptability, scalability, stability, security and usability, far exceeding today's simple embedded systems. CFS technology will transform the interaction of people with the engineering system [1, 2].*

*Today, cyberphysical systems exist in various fields, such as automotive, aerospace, civil, railway, medical. Large productions seek to increase the availability of the asset, while reducing maintenance costs through cyberphysical systems.*

*With the development of the industry and the use of systems in production, the proposed maintenance is used constantly to avoid failures. CFS maintenance is performed when certain indicators signal that the condition of the system has deteriorated. One way to solve this problem is to provide systems with resistance properties. Such systems are able to recover quickly and continue to function in changing conditions [3-9].*

*Therefore, the urgent task is to develop approaches that will predict the resilience of cyberphysical systems based on cloud computing. It is necessary to build methods and tools that will monitor the condition of the CFS and predict the timely replacement of their components that may fail.*

*The application of the process of predicting the resilience of cyberphysical systems using cloud-oriented increases the effective reliability and availability of cyberphysical systems in its life cycle by identifying future failures and reducing unscheduled maintenance. The forecasting process involves the assessment of the useful life, and the implementation of a post-forecast decision on maintenance measures in accordance with the rules. The method of predicting the resilience of cloud-oriented cyberphysical systems allows to determine the state of the cyberphysical systems using cloud computing. The mechanism used to reduce the cost of maintenance and detailed planning of maintenance operations, the apparatus of genetic algorithms.*

*Keywords: cyberphysical systems, resilience, computer systems, cloud technology.*

**Вступ.** Кіберфізична система – це інтеграція фізичного простору (обладнання, пристроїв та людини) з обчислювальними, комунікаційними та керуючими системами (кіберпростір). Національний інститут стандартів та термінології (NIST) дав визначення КФС як кіберфізичні системи (КФС) – це розроблені системи, побудовані з безперервної інтеграції обчислювальних алгоритмів та фізичних компонентів.

Удосконалення КФС надає більші можливості працездатності, адаптованості, масштабованості, стійкості, безпеки та зручності використання, що значно перевищує прості вбудовані сьогоднішні системи. Технологія КФС перетворить взаємодію людей з інженерною системою [1, 2].

На сьогодні кіберфізичні системи існують у різних галузях, таких як автомобільна, аерокосмічна, цивільна, залізнична, медична. Великі виробництва прагнуть збільшити доступність активу, одночасно знижуючи витрати на обслуговування за допомогою кіберфізичних систем.

З розвитком галузі та використанням систем на виробництві, передбачуване технічне обслуговування використовується постійно, щоб уникнути збоїв. Технічне обслуговування КФС проводиться тоді, коли певні показники дають сигнал про те, що стан системи погіршився. Одним із способів вирішення зазначеної проблеми є надання систем властивості резильєнтності. Такі системи здатні швидко відновлюватися та продовжувати функціонувати в умовах зміни стану [3–9]. Тому актуальною задачею є розроблення підходів, які дозволять здійснювати прогнозування резильєнтності кіберфізичних систем на основі залучення хмарних обчислень. Необхідним є побудоа методів та засобів, які будуть стежити за станом КФС та прогнозувати своєчасну заміну їх компонентів, які можуть вийти з ладу.

**Пов'язані роботи.** В [10] запропоновано мережну архітектуру виявлення втручань на мережній структурі ebbits. При такому підході можливим є прослуховувати або контролювати трафіку КФС засобами 6LoWPAN. Використано гібридний підхід для розміщення КФС. Менеджер моніторингу є основним компонентом пропонованої системи, яка генерує попередження, використовуючи інформацію, доступну на компоненті мережного менеджера.

В [11] запропоновано інформаційну технологію виявлення вторгнень в реальному часі SVELTE. У системі є три основних централізованих елементи: 6LoWPAN Mapper (картограф), який збирає інформацію

про протокол RPL і перебудовує мережі в 6BR; елемент виявлення змін, який виявляє вторгнення шляхом аналізу даних, що нанесені на карту, та розподілений міні-брандмауер, який фільтрує трафік, перш ніж він досягне мережі.

В [12] запропоновано КФС, яка включає систему моніторингу та механізм виявлення змін в мережній структурі. Система моніторингу складається з диспетчера частотної гнучкості (FAM) та системи управління інцидентами і інтегрує широкий спектр інструментів безпеки в рамках однієї системи моніторингу. Це зводить до мінімуму помилкові спрацювання. FAM (Frequency Agility Manager) забезпечує 6LoWPAN можливістю перебудови частоти. Тестування системи на проникнення продемонстрували здатність виявлення та мітігації змін свого стану.

В [13] запропоновано інформаційну технологію виявлення вторгнень шляхом реалізації полегшеного протоколу Heartbeat. Протокол RPL вразливий для різних атак маршрутизації, він має вбудовані механізми для протидії атакам і пом'якшення наслідків атак. IDS для КС можуть бути доповнені новими механізмами безпеки в протоколі IPv6. Їх техніка використовується для виявлення і запобігання атак вибіркової переадресації.

В [14] запропоновано технологія, що заснована на обробці подій для вирішення проблеми вторгнень в КФС. У рамках цього підходу розроблено архітектуру IDS на основі моделі обробки подій (EPM). Це заснована на правилах IDS, в якій правила зберігаються в репозиторії шаблонів правил і приймають SQL і EPL Epser в якості посилання.

В [15] запропоновано метод оцінювання стану систем. Він представляє собою схему захисту, включаючи виявлення Sibil атаки на основі соціальних графів (SGSD) та виявлення Sibil атаки на основі класифікації поведінки (BCSD).

В [16] подано технологію виявлення Sinkhole атака INTI (Intrusion Detection of Sinkhole attacks on 6LoWPAN). Інформаційна технологія INTI прагне зменшити негативний вплив атаки на КФС, поєднує в собі стратегії спостереження, репутації та довіри для виявлення зловмисників шляхом аналізу поведінки пристроїв. Отримані результати показують продуктивність INTI і її ефективність по відношенню до швидкості виявлення атак, кількості помилкових позитивних і негативних результатів.

В [17] описано інформаційну технологію радіочастотної ідентифікації в RFID – ключовому протоколі шифрування, який забезпечує безпеку зв'язку та аутентифікацію між міткою і сервером.

В [18] описана інформаційна технологія захисту CloudEyes від атак мережного типу, яка надає ефективні та надійні служби безпеки для пристроїв з обмеженими ресурсами. CloudEyes виявляє підозрілу фільтрацію, заснована на структурі зворотніх ескізів і забезпечує точне створення фрагментів злоякісної сигнатури.

**Метод прогнозування резильєнтності клауд-орієнтованих кіберфізичних систем.** В роботі пропонується метод прогнозування резильєнтності клауд-орієнтованих кіберфізичних систем. В основі методу передбачається здійснення моніторингу системи з метою виявлення майбутні збоїв у роботі КФС.

Згідно методу необхідно здійснити оцінку як поточного стану системи, так і її можливий термін роботи. Це дозволяє ефективно здійснювати планування заходів з технічного обслуговування КФС, що може вплинути на надійність, доступність, безпеку та якість функціонування системи.

Метод базується на моделі КФС, яку можна представити як багатошарову структуру:

– фізичний рівень включає в себе множину компонентів системи та множину давачів;

– обчислювальний рівень включає в себе підсистему, яка реалізована за допомогою хмарних обчислень і яка здійснює аналізу даних, прогнозування корисного терміну використання КФС, детального планування її технічного обслуговування тощо.

Робота методу починається зі збору даних від різних датчиків, необхідних для моніторингу стану КФС. Отримані дані аналізуються, фільтруються та синхронізуються для використання на етапі прогнозування. Цей крок передбачає оцінку стану компонентів (чи компонента) системи та оцінки її стану. Це дозволяє виявлення раннього попередження у випадку несправності компонента.

Так попередження буде використано на кроці пост прогностичного рішення для подальшого прийняття заходів щодо планового обслуговування КФС та уможливлення уникнення передбачуваних та непередбачених експлуатаційних проблем [19].

Пост прогностичний процес прийняття рішень використовує інформацію стану системи з метою прийняття оптимальне рішення щодо того, яке технічне обслуговування потрібно провести для визначеної КФС. Також прогнозування дозволяє отримати інструкції щодо того, коли і хто повинен виконувати обслуговування КФС.

**Вимоги до реалізації прогнозування.** Результати прогностичного та постпрогностичного прийняття рішень не залежать лише від вибору методів чи способу обробки даних [20]. Але також, з багатьох інших моментів, як:

1. Загальний моніторинг усієї множини компонентів системи.
2. Зберігання та обробка великої кількості інформації.
3. Управління знаннями, яке буде використовуватися в майбутніх випадках та в оцінці стану системи.

4. Застосування надійних та оптимальних алгоритмів для оцінка стану системи та для прийняття рішень з високим рівнем достовірності.

5. Вимога мінімізації часу реакції від моменту збору даних до прийняття відповідного прогностичного рішення.

**Процес здійснення прогнозування на основі залучення хмарних обчислень.** Хмарні обчислення є потужним інструментом, який дозволяє безпечно і в простий спосіб здійснювати зберігання та обробку великої кількості даних [21]. При цьому обробка може виконуватися як в онлайн, так і офлайн.

У хмарних обчисленнях усі розподілені ресурси реалізуються у вигляді хмарних сервісів:

1. SaaS (програмне забезпечення як сервіс) [22].
2. PaaS (платформа як сервіс) [23].
3. IaaS (інфраструктура як сервіс) [24].

Ефективність та зручність перерахованих сервісів підтверджується можливостями, та адаптивністю до вимог систем.

Хмарні сервіси, з боку користувачів, можуть замовлятися як послуги проектування, виготовлення, тестування, управління та всіх інших етапів життєвого циклу систем.

Хмарні обчислення мають суттєві переваги в процесі їх залучення до вирішення задач різного спрмування та складності.

Перевагами хмарних обчислень вважають:

1. Можливість зниження витрат на підтримку кіберфізичної системи;
2. Адаптивність ресурсного використання в частині необхідних обчислювальних можливостей;
3. Здатність заощадження витрат на ІТ, використовуючи ресурси постачальника хмарних обчислень.

Мінімізація робочого часу, який витрачається на необхідність встановлення та технічне обслуговування компонент КФС.

Здатність одночасного доступ до хмарних ресурсів. Сервіс географічно є незалежним та доступним з будь-якої точки.

Диверсність хмарного ресурсу дозволяє використовувати його постійне, і не турбуватися про можливі збої в наанні сервісів.

З метою здійснення ефективного процесу прогнозування стану КФС, доцільним є застосування апарату хмарних обчислень, які дозволять перенести обчислення процесу прогнозування, що, в свою чергу, уможливить мінімізувати часові витрати.

**Приклад роботи.** У роботі пропонується реалізувати хмарний сервіс, що дозволить здійснити пост прогностичне прийняття рішення щодо стану КФС [23].

В основі обробки даних є застосування методи оптимізації витрат на технічне обслуговування КФС, які уможливлюють ефективне планування завдань з обслуговування КФС.

Результуюча вартість, необхідна для технічного обслуговування КФС, залежить від множини параметрів:

– витрати на компоненти КСФ, які необхідно замінити;

– витрат на здійснення робіт з обслуговування;

– транспортні витрати тощо.

Пропонований сервіс для пост прогностичного прийняття рішень реалізує процес оптимізації одного або багатьох пунктів витрат.

Для мінімізації транспортних витрат необхідним є мінімізація відстані, яку має подолати служба технічного обслуговування для відновлення робочого стану КФС. Кожен компонент характеризується місцем розташування та множиною значень рівня стану справності компонентів КФС, отримані системою прогнозування. Також кіберфізична система обслуговується командою технічного обслуговування. Вона починає поїздку з центру технічного обслуговування і повинна відвідати всі компоненти до виходу з ладу. Задача полягає у ошуку найкоротшої відстані, яку долатиме команда з техобслуговування для усіх компонентів, що можуть вийти з ладу.

Для вирушення означеної задачі в роботі було використано – це еволюційний алгоритм пошуку, що використовується для вирішення задач оптимізації шляхом послідовного підбору, комбінування і варіації шуканих параметрів з використанням механізмів, аналогічних природньому відбору живих організмів [25].

В роботі механізми нашій роботі генетичний алгоритм використовується для оптимізації значень відстані, пройденої командою технічного обслуговування КФС.

**Висновки.** Застосування процесу прогнозування резильєнтності кіберфізичних систем за допомогою клауд-орієнтованих підвищує ефективну надійність та доступність КФС в її життєвому циклі за рахунок виявлення майбутніх збоїв та скорочення позапланового обслуговування.

Процес прогнозування передбачає оцінку термінів корисної експлуатації, і здійснення пост прогностичного рішення щодо заходів з технічного обслуговування відповідно до заданих правил.

Метод прогнозування резильєнтності клауд-орієнтованих кіберфізичних систем дозволяє визначити стан КСФ із застосуванням хмарних обчислень.

Механізм, що використовуються для зменшення витрат на обслуговуючі роботи та детального планування операцій з обслуговування, апарат генетичних алгоритмів.

## Література


1. DerlerP., LeeE.A.and Sangiovanni-VincentelliA.Modeling Cyber-Physical System. Proceedings of the IEEE (special issue on CPS), 13-28, January 2012. – No. 100 (1).
2. J. Lee, H. D. Ardakani, S. Yang, and B. Bagheri. Industrial big data analytics and cyber-physical systems for future maintenance & service innovation. Procedia CIRP, vol. 38, pp. 3–7, 2015.
3. Лисенко С. М. Метод забезпечення резильєнтності комп'ютерних систем в умовах кібер-загроз на основі самоадаптивності. Радіоелектронні і комп'ютерні системи. 2019. № 4. С. 4–16.
4. Лисенко С. М., Харченко В. С., Бобровнікова К. Ю., Щука Р. Резильєнтність комп'ютерних систем в умовах кіберзагроз: Онтологія та таксономії. Радіоелектронні і комп'ютерні системи. 2020. №1. С. 17–28.
5. Лисенко С. М. Моделі опису здійснення кібер-атак на інформаційно-комунікаційні системи. Вимірювальна та обчислювальна техніка в технологічних процесах. 2019. № 2. С. 173–179.
6. Lysenko S., Savenko O., Bobrovnikova K., Kryshchuk A. Self-adaptive system for the corporate area network resilience in the presence of botnet cyberattacks. Communications in Computer and Information Science, ISSN: 1865–0929 (Scopus, Web of Science). 2018. Pp. 385–401.
7. Lysenko S., Bobrovnikova K., Nicheporuk A., Shchuka R. SVM-based Technique for Mobile Malware Detection. CEUR-WS, ISSN: 1613–0073 (Scopus). 2019. Vol. 2353. Pp. 85–97.
8. Savenko O., Nicheporuk A., Hurman I., Lysenko S. Dynamic signature-based malware detection technique based on API call tracing. CEUR-WS. ISSN: 1613–0073 (Scopus). 2019. Vol. 2393. Pp. 633–643.
9. Lysenko S., Bobrovnikova K., Savenko O., Kryshchuk A. BotGRABBER: SVM-Based Self-Adaptive System for the Network Resilience Against the Botnets' Cyberattacks. Communications in Computer and Information Science, ISSN: 1865-0929 (Scopus, Web of Science). 2019. Pp. 127–143.
10. Pasqualetti F., Dörfler F., Bullo F. Attack detection and identification in cyber– physical systems, IEEE Trans. Autom. Control. 2013. Vol. 58. No. 11. Pp. 2715–2729.
11. Raza S., Wallgren L., Voigt T. SVELTE: Real-time intrusion detection in the Internet of Things. Ad Hoc Networks. 2013. Vol. 11. No. 8. Pp. 2661–2674. doi:10.1016/j.adhoc.2013.04.014
12. Arrington B., Barnett L., Rufus R., Esterline A. Behavioral Modeling Intrusion Detection System (BMIDS) Using Internet of Things (IoT) Behavior-Based Anomaly Detection via Immunity-Inspired Algorithms. In 25th International Conference on Computer Communication and Networks (ICCCN) (August 2016). 2016. Pp. 1-6.
13. Hao J., Piechocki R.J., Kaleshi D., Chin W., Fan Z., Sparse malicious false data injection attacks and defense mechanisms in smart grids, IEEE Trans. Ind. Inform. 2015. Vol. 11. No. 5. Pp. 1198–1209.
14. Jun C., Chi C. Design of complex event-processing IDS in internet of things. In Sixth International Conference on Measuring Technology and Mechatronics Automation (ICMTMA)(January 2014). 2014. Pp. 226-229.
15. Zhang J., Blum R.S., Lu X., Conus D. Asymptotically optimum distributed es- timation in the presence of attacks, IEEE Trans. Signal Process. 2015. Vol. 63. No. 5. Pp.1086–1101.
16. Cervantes C., Poplade D., Nogueira M., Santos A. Detection of sinkhole attacks for supporting secure routing on 6lowpan for internet of things. In IFIP/IEEE International Symposium on Integrated Network Management (IM)(May, 2015). 2015. Pp. 606-611.
17. An R., Feng H., Liu Q., Li L. Three elliptic curve cryptography-based RFID authentication protocols for Internet of Things. In International Conference on Broadband and Wireless Computing, Communication and Applications. Springer International Publishing (November 2016). 2016. Pp. 857-878.
18. Pang Z.-H., Liu G.-P., Dong Z. Secure networked control systems under denial of service attacks, IFAC Proc., 2011. Vol. 44. No. 1. Pp. 8908–8913.
19. S. Chre´tien, N. Herr, J.-M. Nicod, and C. Varnier A post-prognostics decision approach to optimize the commitment of fuel cell systems in stationary applications. Prognostics and Health Management (PHM), 2015 IEEE Conference on. IEEE, 2015, pp. 1–7.
20. M. Xia, T. Li, Y. Zhang, and C. W. de Silva Closed-loop design evolution of engineering system using condition monitoring through internet of things and cloud computing. Computer Networks, vol. 101, pp. 5–18, 2016.
21. S. Meraghni, L. S. Terrissa, N. Zerhouni, C. Varnier, and S. Ayad. A post-prognostics decision framework for cell site using cloud computing and internet of things. Cloud Computing Technologies and Applica- tions (CloudTech), 2016, pp. 310–315.
22. Yiling Zhou, Tao Hu, Jianjun Yang. Design and Implementation of PHM System Framework for Unmanned Surface Vehicles. IEEE, 2019, pp. 1-6.
23. X. Yue, H. Cai, H. Yan, C. Zou, and K. Zhou. Cloud-assisted industrial cyber-physical systems: An insight. Microprocessors and Microsystems, vol. 39, no. 8, pp. 1262–1270, 2015.
24. P. Leitao, S. Karnouskos, L. Ribeiro, J. Lee, T. Strasser, and A. W. Colombo. Smart agents in industrial cyber–physical systems. IEEE, vol. 104, no. 5, pp. 1086–1101, 2016.
25. A.P. Engelbrecht Computational Intelligence An Introduction Wiley, New York, 2002.


Надійшла / Paper received: 17.09.2020
Надрукована / Paper Printed : 03.11.2020