КОНЦЕПТУАЛЬНІ ЗАСАДИ ПОСИЛЕННЯ ЦИФРОВОЇ РЕЗИЛЬЄНТНОСТІ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ НА ОСНОВІ ВІДМОВОСТІЙКИХ МОДУЛЬНИХ КОДІВ

Янко А.С., Глушко А.Д.
Національний університет «Полтавська політехніка імені Юрія Кондратюка», Полтава, Україна

Забезпечення стійкого цифрового розвитку України у 2026 році вимагає створення цілісної системи протидії кіберзагрозам на національному рівні. Особливої актуальності набуває питання цифрової резильєнтності (стійкості) критичної інфраструктури та державних інформаційних систем до атак на цілісність даних. Традиційні методи захисту часто мають надмірні часові затримки, що є критичним для систем реального часу. Ефективним рішенням є впровадження модульних кодів, які дозволяють інтегрувати функції контролю та виправлення помилок безпосередньо в арифметико-логічний базис системи для забезпечення економічної стійкості телекомунікаційних мереж [1, 2].

Метою доповіді є розробка практичних рекомендацій щодо посилення цифрової стійкості інформаційних систем держави через впровадження високопродуктивних засобів діагностування даних у модульних кодах.

У межах розробки концептуальної моделі цілісної системи протидії кіберзагрозам запропоновано використовувати внутрішні властивості модульних кодів для побудови самокоригувальних обчислювальних структур. Такий підхід дозволяє реалізувати механізм активного захисту на рівні протоколів автентифікації та виявлення гомології шкідливого програмного забезпечення [3, 4].

Основними рекомендаціями щодо посилення резильєнтності економічних суб'єктів та державних структур є:

1. Впровадження паралельних методів діагностування, а саме використання властивостей модульних кодів дозволяє поєднати в часі процеси обчислень та аналізу контрольних ознак (проекцій) чисел. Це забезпечує виявлення помилок (спричинених як збоями обладнання, так і навмисними спотвореннями) у реальному часі [2].

2. Динамічне керування надмірністю в структурі обчислювальних засобів. Концептуальна модель передбачає можливість адаптивної зміни кількості контрольних основ у модульних кодах залежно від рівня кіберзагрози. Це дозволяє підтримувати стабільність функціонування критичних вузлів навіть в умовах інтенсивних атак [3, 4].

Запропонована логічна організація відмовостійких вузлів обробки інформації на базі модульних кодів виступає як ефективний механізм управління в публічних організаціях з високим рівнем безпеки [5], дозволяючи державним інформаційним системам зберігати функціональність при відмові окремих обчислювальних каналів, що є фундаментом національної цифрової резильєнтності.

Реалізація запропонованих рекомендацій дозволить сформувати стійке цифрове середовище, де захищеність інформаційних систем держави базується на внутрішній стійкості модульних кодів.

Список літератури

1. Yanko A., Mychailichenko O., Hlushko A. Modern methods for protecting and storing data in computer systems to ensure their fault tolerance. *Theoretical and Applied Cyber Security*. 2024. Vol. 6, No. 1. P. 72–81. DOI: https://doi.org/10.20535/tacs.2664-29132024.1.315086

2. Янко А. С., Маслій О. А. Математична модель економічної стійкості телекомунікаційних систем з урахуванням показників відмовостійкості. *Цифрова економіка та економічна безпека*. 2025. № 4 (19). С. 461–468. DOI: https://doi.org/10.32782/dees.19-66

3. Sun H., Shu H., Kang F., Guang Y. ModDiff: Modularity Similarity-Based Malware Homologation Detection. *Electronics*. 2023. Vol. 12, No. 10. 2258. DOI: https://doi.org/10.3390/electronics12102258

4. Kalmykov I. A., Olenev A. A., Kononova N. V. et al. Improvement of the Cybersecurity of the Satellite Internet of Vehicles through the Application of an Authentication Protocol Based on a Modular Error-Correction Code. *World Electric Vehicle Journal*. 2024. Vol. 15, No. 7. 278. DOI: https://doi.org/10.3390/wevj15070278

5. Plevnik M. Communication and Information Systems User Support as a Governance Mechanism in a High-Security Public Organization. *Systems*. 2026. Vol. 14, No. 3. 288. DOI: https://doi.org/10.3390/systems14030288

SOFTWARE AND HARDWARE COMPLEX FOR AUTOMATED MONITORING OF IoT DEVICES OF A FIRE SAFETY SYSTEM

Rozhnova T.G., Kurylo A.V.
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine

The steady growth in the number of fires at residential, public and industrial facilities makes automated fire safety monitoring one of the most critical tasks of modern civil protection [1]. Traditional fire alarm systems based on stand-alone detectors have limited diagnostic capabilities, do not allow remote assessment of the technical state of the equipment, and in most cases react only to already developed hazardous factors of a fire. The rapid spread of the Internet of Things (IoT) paradigm opens new opportunities for building distributed monitoring systems capable of collecting, transmitting and analysing heterogeneous data from a large number of sensor nodes in real time [2].

The aim of the work is to develop a software and hardware complex for the automated monitoring of IoT devices of a fire safety system that provides continuous control over the operability of the sensor nodes, early detection of pre-emergency states and prompt notification of the responsible personnel.

The proposed complex has a three-tier architecture in accordance with the IoT reference model. The lower (perception) tier includes smoke, temperature, carbon monoxide and flame sensors connected to microcontroller nodes based on ESP32 modules with Wi-Fi and BLE interfaces. The middle (network) tier is built on an