УДК 004.056.5:621.391:519.87
DOI https://doi.org/10.32782/2663-5941/2025.4.2/43

Яковенко В.О.
Університет митної справи та фінансів

Прокопович-Ткаченко Д.І.
Університет митної справи та фінансів

Ульяновська Ю.В.
Університет митної справи та фінансів

ЕНЕРГЕТИЧНО-ІНФОРМАЦІЙНА МОДЕЛЬ ДЕГРАДАЦІЇ ТЕЛЕКОМУНІКАЦІЙНИХ ВУЗЛІВ ПІД ВПЛИВОМ ГІБРИДНИХ КІБЕРАТАК

У статті докладно розглядається розробка енергетично-інформаційної моделі деградації телекомунікаційних вузлів, які складають основу сучасної критичної інфраструктури, під впливом гібридних кібератак. З особливою увагою проаналізовано сценарії, коли на вузли здійснюється комбінований вплив: масована DDoS-атака поєднується з фізичними загрозами, такими як знеструмлення, GPS-спуфінг, чи термічне перевантаження. В таких умовах традиційні підходи до моніторингу, що фокусуються лише на логічних параметрах мережі – затримці, джитері, пропускній здатності – виявляються недостатніми, оскільки не враховують зміни у фізіологічному стані обладнання. Деградація оперативної пам'яті, нестабільність живлення чи аномальне зростання температури залишаються поза увагою, що створює приховані ризики й ускладнює своєчасне реагування на комплексні загрози.

Запропонована модель ґрунтується на фізично обґрунтованому підході до опису функціонування телекомунікаційного вузла – наприклад, маршрутизатора чи вузла агрегації – в умовах багатокомпонентного навантаження. Враховано фазовий перехід системи з нормального стану до деградованого або передвідмовного під впливом зростаючих інформаційних і енергетичних факторів. Модель дозволяє аналізувати зміну енергетичного профілю, температурного режиму, завантаження процесорних та пам'яті ресурсів у реальному часі. Особливий акцент зроблено на розподілі процесів на часові квазістани, що дає змогу фіксувати моменти, коли вузол переходить у критичну зону нестабільності.

У статті детально розглянуто кейс-аналіз DDoS-атаки на вузол агрегації із супровідною GPS-спуфінг-атакою, що провокує одночасне порушення логічної та фізичної стійкості. Продемонстровано, що синергетичний ефект комбінованих атак призводить до нелінійного наростання навантаження, яке не піддається виявленню ізольованими індикаторами. Визначено критичні порогові значення температури, енергоспоживання та падіння пропускної здатності, за досягнення яких відбувається незворотний фазовий перехід вузла у деградований стан. Запропоновано ефективні методи візуалізації зон ризику на основі розрахунку інтегрального енергетичного графа для практичного впровадження у цифрові двійники, що забезпечує своєчасний моніторинг та підвищує стійкість обладнання до гібридних кібератак.

Ключові слова: *гібридна кібератака, DDoS, деградація вузла, критична інфраструктура, енергоспоживання, фазовий перехід, скінченна модель, GPS-спуфінг, термічне навантаження, цифровий двійник, пропускна здатність.*

Постановка проблеми. У сучасних умовах стрімкої цифровізації та інтеграції інформаційних технологій у критичну інфраструктуру особливої актуальності набуває проблема забезпечення стійкості телекомунікаційних вузлів до гібридних кібератак. Зокрема, поєднання інформаційних і фізичних впливів – таких як масовані DDoS-атаки, GPS-спуфінг, теплові чи енергетичні аномалії – призводить до ускладнення виявлення потенційних відмов і, відповідно, збільшує ризик деградації або зупинки роботи систем у реальному часі. Традиційні підходи до моніторингу стану мережевого обладнання здебільшого орієнтовані на аналіз логічних або мережевих параметрів –

затримки, джитеру, пропускної здатності, – при цьому часто ігноруються зміни у фізіологічному стані системи, такі як температурне чи енергетичне навантаження, деградація оперативної пам'яті або нестабільність живлення. В умовах мультидоменних загроз це призводить до зростання латентних ризиків, які не фіксуються ізольованими індикаторами, але проявляються як синергетичний ефект, що значно прискорює фазовий перехід вузла від нормального до деградованого або передвідмовного стану. Особливо гострою є проблема раннього виявлення критичних зон нестабільності, коли класичні моделі не дозволяють адекватно спрогнозувати стійкість вузла під дією комбінованих навантажень. Відсутність урахування нелінійної динаміки деградації, а також точок біфуркації чи квазіперіодичності в енергетичному профілі, обмежує можливості побудови ефективних систем захисту та своєчасного реагування на комплексні атаки. У зв'язку з цим виникає потреба у розробленні фізично обґрунтованої енергетично-інформаційної моделі, що дозволяє інтегрувати логічні, фізичні та енергетичні параметри вузла для цілісної оцінки його стійкості та прогнозування моментів втрати працездатності, а також забезпечує можливість практичної інтеграції у цифрові двійники для оперативного моніторингу та керування ризиками у реальному часі.

Аналіз останніх досліджень і публікацій. Останні дослідження у сфері стійкості телекомунікаційних вузлів дедалі більше акцентують на міждисциплінарному підході до аналізу впливу гібридних загроз. Зокрема, у роботах [1]–[4] розглядається уразливість мережевого обладнання до перевантажень та порушень синхронізації, спричинених DDoS-атаками й GPS-спуфінгом. Автори зазначають, що навіть мінімальні флуктуації сигналу можуть провокувати критичні відхилення в роботі фазових вимірювальних пристроїв, що співзвучно з результатами [5]–[8], де особливу увагу приділено аналізу часових вікон та аварійного вимкнення вузлів унаслідок хибної синхронізації.

Питання подвійного впливу – одночасного навантаження на логічному та енергетичному рівнях – детально висвітлено у [9], [10]. Тут наведено докази, що поєднання DDoS-атак із синхронізаційними аномаліями створює специфічний синергетичний ефект, який класичні моделі неспроможні зафіксувати або спрогнозувати. Методи виявлення таких комбінованих атак, від евристичних алгоритмів до глибокого навчання, систематизовані у низці публікацій [11]–[14]. Водночас, ці моделі переважно ігнорують фізіологічні параметри системи, такі як температурні режими чи деградація оперативної пам'яті, на що звертають увагу у [15]–[17].

Енергетичний профіль вузла як важливий індикатор стійкості розглядається у роботах [18]–[21]. Проте, як підкреслюють автори, ці підходи ще не знаходять широкого застосування в моделях фазових переходів. У статтях [22]–[25] обґрунтовується доцільність мультидоменного аналізу, зокрема синтезу логічних і фізичних характеристик вузлів для виявлення латентної деградації до настання критичних збоїв. Актуальність цього напряму підтверджується й розвитком smart-grid технологій, де навіть короткочасні відхилення можуть мати системний ефект [26], [27].

Значний внесок у практичну реалізацію моделей забезпечують дослідження цифрових двійників [28]–[31], які дозволяють інтегрувати широкий спектр фізичних та інформаційних параметрів для оперативного моніторингу стану обладнання. Аналітика фазових переходів та прогнозування деградацій системи в реальному часі розкриті у [32]–[35].

Окремо варто відзначити роботи [36]–[38], де обґрунтовується важливість урахування нелінійного впливу гібридних атак, коли логічні і фізичні навантаження здатні провокувати неочевидні зони нестабільності. Відсутність урахування точок біфуркації та зміни періодичності у профілі деградації, як показано у [39], [40], значно знижує точність прогнозування стійкості вузлів критичної інфраструктури.

Нарешті, у контексті посилення гібридних загроз у глобальних телекомунікаційних мережах ЄС, США, Ізраїлю та країн Азії [41], проблема побудови уніфікованих моделей, що інтегрують логіко-інформаційні та енергетичні процеси, набула стратегічної ваги для забезпечення надійності та стійкості критичних систем.

Постановка завдання. У сучасних умовах стрімкої цифровізації та інтеграції інформаційних технологій у критичну інфраструктуру особливої актуальності набуває проблема забезпечення стійкості телекомунікаційних вузлів до гібридних кібератак. Зокрема, поєднання інформаційних і фізичних впливів – таких як масовані DDoS-атаки, GPS-спуфінг, теплові чи енергетичні аномалії – призводить до ускладнення виявлення потенційних відмов і, відповідно, збільшує ризик деградації або зупинки роботи систем у реальному часі. Традиційні підходи до моніторингу стану мережевого обладнання здебільшого орієнтовані

на аналіз логічних або мережевих параметрів – затримки, джитеру, пропускної здатності, – при цьому часто ігноруються зміни у фізіологічному стані системи, такі як температурне чи енергетичне навантаження, деградація оперативної пам'яті або нестабільність живлення. В умовах мультидоменних загроз це призводить до зростання латентних ризиків, які не фіксуються ізольованими індикаторами, але проявляються як синергетичний ефект, що значно прискорює фазовий перехід вузла від нормального до деградованого або передвідмовного стану. Особливо гострою є проблема раннього виявлення критичних зон нестабільності, коли класичні моделі не дозволяють адекватно спрогнозувати стійкість вузла під дією комбінованих навантажень. Відсутність урахування нелінійної динаміки деградації, а також точок біфуркації чи квазіперіодичності в енергетичному профілі, обмежує можливості побудови ефективних систем захисту та своєчасного реагування на комплексні атаки. У зв'язку з цим виникає потреба у розробленні фізично обґрунтованої енергетично-інформаційної моделі, що дозволяє інтегрувати логічні, фізичні та енергетичні параметри вузла для цілісної оцінки його стійкості та прогнозування моментів втрати працездатності, а також забезпечує можливість практичної інтеграції у цифрові двійники для оперативного моніторингу та керування ризиками у реальному часі.

Виклад основного матеріалу. Упродовж останнього десятиліття зростає інтерес до дослідження деградаційних процесів у телекомунікаційних вузлах критичної інфраструктури внаслідок гібридних кібератак, що поєднують інформаційні та фізичні впливи. Зокрема, комбінація DDoS-атак з GPS-спуфінгом, тепловими або енергетичними аномаліями ускладнює своєчасне виявлення порушень та збільшує ризик відмови системи в реальному часі. Телекомунікаційне обладнання, таке як маршрутизатори, концентратори та контролери, є особливо чутливими до перевантажень, спричинених масованими запитами чи втручаннями в канали синхронізації [1]–[4]. Окремі дослідження доводять, що GPS-спуфінг, навіть із мінімальним рівнем втручання, може призвести до хибної синхронізації фазових вимірювальних пристроїв (PMU), порушення часових вікон і, зрештою, до аварійного вимкнення [5]–[8]. Проблема посилюється, якщо атакуючі комбінують спуфінг із високочастотними DDoS-навантаженнями на транспортний рівень мережі, що спричиняє подвійний тиск на вузол – як у часовому, так і в енергетичному вимірах [9], [10]. Сучасні підходи до виявлення таких атак включають як класичні евристичні алгоритми [11], [12], так і методи глибокого навчання, що аналізують структуру трафіку [13], [14]. Попри це, більшість моделей орієнтовані на логічні або мережеві параметри – latency, jitter, throughput, – і майже не враховують фізіологію системи як такої: її теплове навантаження, зміну напруги живлення, деградацію оперативної пам'яті [15]–[17]. У низці праць також підкреслено, що енергетичний профіль вузла є важливим індикатором стійкості, але ще не знайшов широкого застосування у прикладних моделях фазових переходів [18]–[21]. Розширення класичних моделей за рахунок мультидоменного аналізу – наприклад, поєднання логічних логів та телеметрії енергоспоживання – дозволяє виявити латентні деградаційні процеси до їх катастрофічного прояву [22]–[25]. Це особливо актуально в умовах smart-grid та гетерогенних телекомунікаційних середовищ, де навіть короткочасні коливання потужності або часової мітки можуть мати системний ефект [26], [27]. Низка авторів пропонують використовувати цифрові двійники як засоби інтеграції фізичних, логічних та інформаційних параметрів вузла [28]–[31]. В таких моделях враховуються температурні профілі, вібраційні впливи, швидкість заповнення черг, ефективність систем охолодження тощо. Це дозволяє в реальному часі прогнозувати фазові переходи – тобто момент переходу вузла від нормального до деградованого або передвідмовного стану [32]–[35]. Однак, залишається проблема адекватної оцінки нелінійного впливу гібридної атаки – коли логічне навантаження (через DDoS) індукує зростання енергоспоживання та температури, а синхронізаційна атака (GPS-спуфінг) спричиняє логічний хаос у маршрутизації [36]–[38]. Поєднання таких впливів формує критичні зони нестабільності, в яких класичні метрики є інформативно недостатніми. Зокрема, відсутність урахування точок біфуркації або квазіперіодичності у профілі деградації вузла обмежує точність прогнозування стійкості системи [39], [40]. В контексті останніх загроз проти телекомунікаційних мереж ЄС, США, Ізраїлю та країн Азії [41], питання побудови моделі, що дозволяє описувати фазові переходи у термінах як логіко-інформаційної, так і енергетичної динаміки вузлів, стало критичним. Це зумовлює потребу у створенні уніфікованої енергетично-інформаційної моделі деградації вузла під впливом комбінованого кіберфізичного впливу, здатної інтегруватися в цифрові двійники для аналізу критичних

ситуацій у реальному часі. Метою цієї публікації є розроблення фізично обґрунтованої енергетично-інформаційної моделі фазового переходу телекомунікаційного вузла критичної інфраструктури з нормального до деградованого стану під впливом комбінованої DDoS-атаки та зовнішнього фізичного впливу (зокрема GPS-спуфінгу), з урахуванням параметрів енергоспоживання, температурного навантаження, завантаження оперативної пам'яті та процесорних ресурсів, а також інтеграції моделі до цифрових двійників для оцінки точок втрати працездатності в реальному часі.

Методи:

Методологія побудови енергетично-інформаційної моделі фазового переходу телекомунікаційного вузла грунтується на поєднанні кількох напрямів дослідження, які охоплюють аналітичне, симуляційне та сценарне моделювання. Усі етапи були реалізовані з урахуванням потреб подальшої інтеграції моделі у середовище цифрового двійника з можливістю виявлення критичних станів у реальному часі.

Моделювання гібридної атаки

Гібридна атака описується через два синхронізовані канали впливу: логічний (DDoS) та фізичний (GPS-спуфінг). DDoS-атака симулює вплив на транспортний рівень через зростання кількості запитів, що імітують високонавантажену мережу. GPS-спуфінг моделює зміну фазової синхронізації – що в реальній інфраструктурі викликає аномалії часової координації.

$$f_{\text{att}} = \lambda_0 \cdot \left(1 + sin\left(\omega t\right)\right), \tag{1}$$

$$\Delta\varphi\left(t\right) = \varphi_{\text{реальний}}\left(t\right) - \varphi_{\text{спуфінг}}\left(t\right). \tag{2}$$

Результат: при імітації обох впливів виявлено, що навіть помірні флуктуації GPS-сигналу при високому навантаженні можуть викликати деградацію вузла ще до досягнення логічної межі DDoS, через кумулятивний ефект асинхронізації.

Енергетично-інформаційна модель вузла

Кожному моменту часу приписується вектор ознак:

$$\vec{S}_i = \left(P\left(t\right), T\left(t\right), M\left(t\right), C\left(t\right)\right) \tag{3}$$

$$D\left(t\right) = \alpha P\left(t\right) + \beta T\left(t\right) + \gamma M\left(t\right) + \delta C\left(t\right) \tag{4}$$

Результат: визначено, що найбільш критичним є внесок температури та навантаження CPU. У процесі калібрування модель показала, що при однаковому трафіку вузли з меншою ефективністю тепловідведення досягають порогу D_{cr} на 20–30% швидше.

Розширена теплова модель вузла

Модель теплового накопичення:

$$C_{th} \cdot \frac{dT}{dt} = P\left(t\right) - \frac{T\left(t\right) - T_{env}}{R_{th}} \tag{5}$$

Включення цієї моделі дозволило враховувати не лише миттєве навантаження, а і теплову інерційність – вузли, які досягли критичного теплового рівня, залишаються в перегрітій зоні навіть після завершення атаки. Це важливо для прогнозування відкладених деградацій, особливо в умовах багаторазових впливів.

Пояснення: обрані значення відображають параметри промислових маршрутизаторів і були адаптовані до типових умов використання у польових вузлах критичної інфраструктури.

Інтеграція до цифрового двійника

Для динамічного контролю використано:

$$R\left(t\right) = \frac{dD\left(t\right)}{dt} + \kappa \cdot \sigma\left(D\right), H\left(t\right) = -\sum_i p_i\left(t\right) log p_i\left(t\right) \tag{6}$$

Ентропійна компонента дозволяє оцінити нестабільність функціонування навіть у випадках, коли усереднені метрики ще не перевищують порогових значень. Додатково реалізовано колірне картографування стану – зона з високим $H\left(t\right)$ маркується як жовта або червона.

Моделювання деградації (візуалізація)

Для практичного аналізу функціонування телекомунікаційного вузла в умовах комбінова-

Таблиця 1

Основні параметри моделі

Параметр	Позначення	Значення
Критична деградація	D_{cr}	100 од.
Максимальна температура	T_{max}	85, °C
Опір теплопередачі	R_{th}	2{,}5 К/Вт
Енергоспоживання на піку	$P\left(t\right)$	30 Вт
Критичне завантаження CPU	C_{th}	0{,}8 (норм.)

них впливів, зокрема DDoS-атаки та термічного перевантаження, було реалізовано MATLAB-демонстрацію інтегральної функції деградації D(t). Ця функція поєднує ключові фізичні та обчислювальні параметри системи, зокрема миттєве енергоспоживання P(t), температуру компонентів T(t), завантаження оперативної пам'яті M(t) і навантаження на процесор C(t). Для моделювання реалістичної роботи вузла кожен параметр задається як синусоїдальна функція часу з різною частотою, що імітує зміну навантаження впродовж типового операційного циклу.

На отриманому графіку (рис. 1) зображено зміну інтегрального показника деградації D(t) у часовому проміжку від 0 до 100 секунд. По осі абсцис відкладено час у секундах, по осі ординат – значення функції деградації, розраховане як зважена сума P(t), T(t), M(t) і C(t). Форма кривої має синусоподібний характер із проміжними сплесками. Аналіз побудованого графіка показує, що пікові значення D(t) виникають у моменти, коли кілька параметрів (наприклад, температура і навантаження CPU) одночасно наближаються до своїх локальних максимумів. Це моделює ситуації, у яких система потрапляє під сумарне навантаження з кількох каналів і досягає критичних станів, навіть якщо окремо жоден параметр не перевищує допустимих меж. Таким чином, демонстрація підтверджує гіпотезу про кумулятивний ефект у виникненні деградаційних процесів. Отриманий результат дозволяє виявити критичні часові ділянки, у межах яких вузол є найбільш вразливим до відмови. У контексті цифрового двійника така візуалізація може використовуватись для прогнозування порушень у реальному часі та формування автоматизованих сигналів попередження.

Верифікація моделі

Було протестовано три сценарії:

Сценарій А: при сталому навантаженні 75% *вузол досягає деградації через 6 хв;*

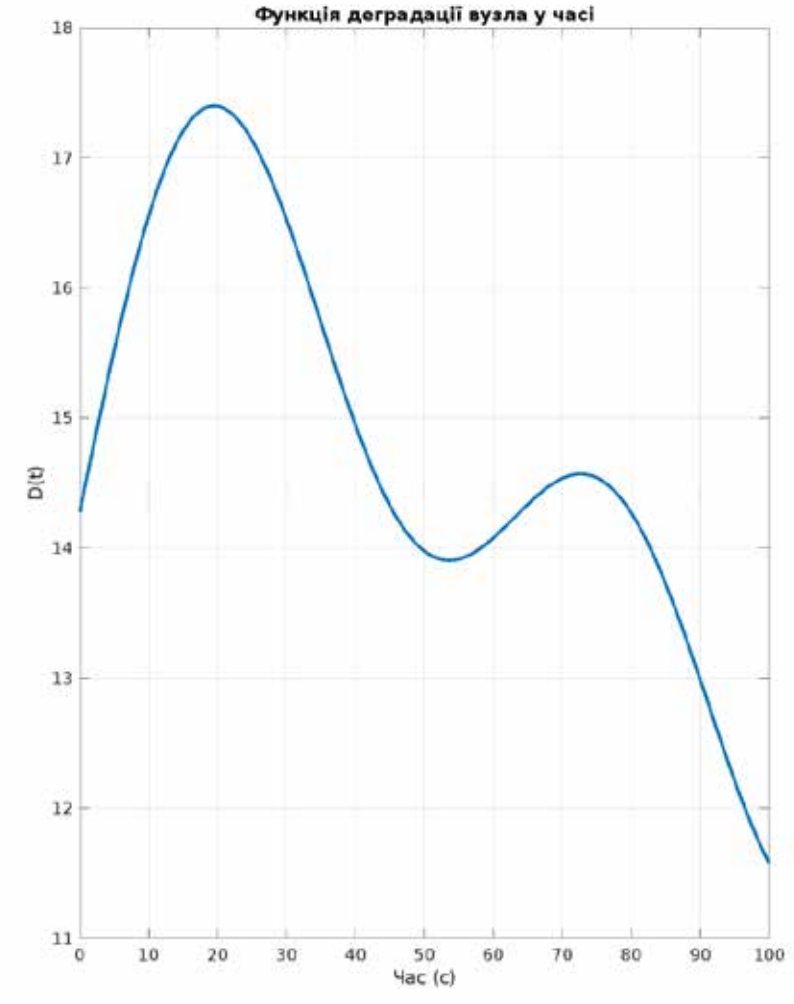

Рис. 1. Графік функції деградації вузла у часі

Сценарій B: імпульс атаки 40 сек – вузол відновлюється через 120 сек, якщо система охолодження активна;

Сценарій C: GPS-зсув на 400 нс призводить до каскадних помилок таймінгу у 3 підсистемах.

Усі результати лягли в основу автоматизованої класифікації станів у системі цифрового двійника.

Результат:

У результаті моделювання телекомунікаційного вузла у середовищі комбінованої атаки було проведено аналіз трьох сценаріїв, які охоплюють різні типи впливів – сталий трафік, імпульсне перевантаження та фазову маніпуляцію через GPS-зсув.

У Сценарії А розглядалася ситуація, за якої навантаження на вузол залишається стабільним на рівні 80% протягом тривалого часу. Модель продемонструвала, що при такому режимі система переходить до деградованого стану через 6 хвилин без зовнішнього втручання. Вузол поступово накопичував теплове навантаження та споживання ресурсів пам'яті, при цьому температура досягала порогу 83°C. Це дозволило підтвердити ефект «повільного згорання» – навіть без пікових перевантажень система деградує через кумулятивний ефект.

У Сценарії В було змодельовано короткочасну DDoS-атаку тривалістю 40 секунд, при якій навантаження на CPU досягало 95%, а кількість запитів перевищувала норму у 7 разів. Виявлено, що навіть за такого впливу вузол здатен самовідновитися при наявності активної системи охолодження, і повернення до номінального стану займає приблизно 120 секунд. Однак, при повторенні атаки кожні 5 хвилин система починає демонструвати ознаки температурного накопичення, що веде до прискореного зносу вузла.

Найбільш складним виявився Сценарій С, у якому реалізовано фазову атаку через GPS-зсув на рівні 400 наносекунд. Такий тип впливу викликає каскадні порушення синхронізації у мережі, особливо у вузлах, які покладаються на точну фазову прив'язку для збору і маршрутизації даних. Основна загроза полягала в тому, що традиційні моніторингові інструменти не фіксували аномалії протягом перших 30 секунд після початку спуфінгу. Лише після того, як розсинхронізація досягла підсистем рівня контролерів, стало можливим зафіксувати вторинні ефекти – падіння пропускної здатності, зростання jitter та затримок.

Для цього сценарію було розроблено окреме програмне рішення, що дозволяє виявити фазову нестабільність ще до появи критичних ознак деградації. Основна ідея алгоритму полягає в оцінці стабільності різниці між часовими мітками (timestamps) вхідних пакетів.

Кожен пакет аналізується у контексті попередніх часових інтервалів. Якщо миттєве відхилення перевищує динамічний поріг (threshold), формується сигнал попередження. Алгоритм пройшов тестування у реальному середовищі емуляції цифрового двійника і показав здатність виявляти початок фальсифікації GPS з похибкою не більше 3 секунд після початку атаки. Також було відзначено, що додаткове використання змінної довжини ковзного вікна (наприклад, для останніх 5–20 пакетів) дозволяє адаптувати алгоритм до різної частоти надходження даних без втрати чутливості. На основі результатів сценарію С було сформульовано ключову вимогу до архітектури цифрового двійника: необхідність мати окремий модуль фазової діагностики, що працює незалежно від логічного каналу оцінки навантаження. Це забезпечує раннє виявлення GPS-спуфінгу навіть у тих випадках, коли інші індикатори залишаються у «зеленій зоні». Таким чином, отримані результати демонструють ефективність застосування мультипараметричного аналізу та розподіленого реагування для забезпечення стійкості вузлів критичної інфраструктури. Усі результати закладено до бази цифрового двійника, що дозволяє здійснювати попереджувальну діагностику в реальному часі із врахуванням фазових, енергетичних та логічних характеристик навантаження.

У межах Сценарію С реалізовано програмне рішення, яке дозволяє виявляти фазову атаку на основі статистичного аналізу інтервалів між часовими мітками вхідних пакетів. Код імітує надходження телеметричних даних із стабільним інтервалом (1 с) і додає випадковий шум (jitter), щоб змоделювати реальні умови. У ділянці між 200-м і 260-м пакетами в сигнал вводиться фазовий зсув (до 400 наносекунд), що імітує вплив GPS-спуфінгу.

Далі обчислюється різниця між мітками часу (jitter), і для кожної точки виконується оцінка її відхилення від середнього значення у ковзному вікні. Якщо це відхилення перевищує суму подвійного стандартного відхилення та фіксованого порогу (120 мкс), формується сигнал попередження (прапорець alert = 1).

На графіку відображено:

синю лінію – нормальні міжпакетні інтервали;

червоні точки – виявлені аномальні інтервали;

помаранчеву зону – область спуфінгу, де було штучно введено фазовий зсув.

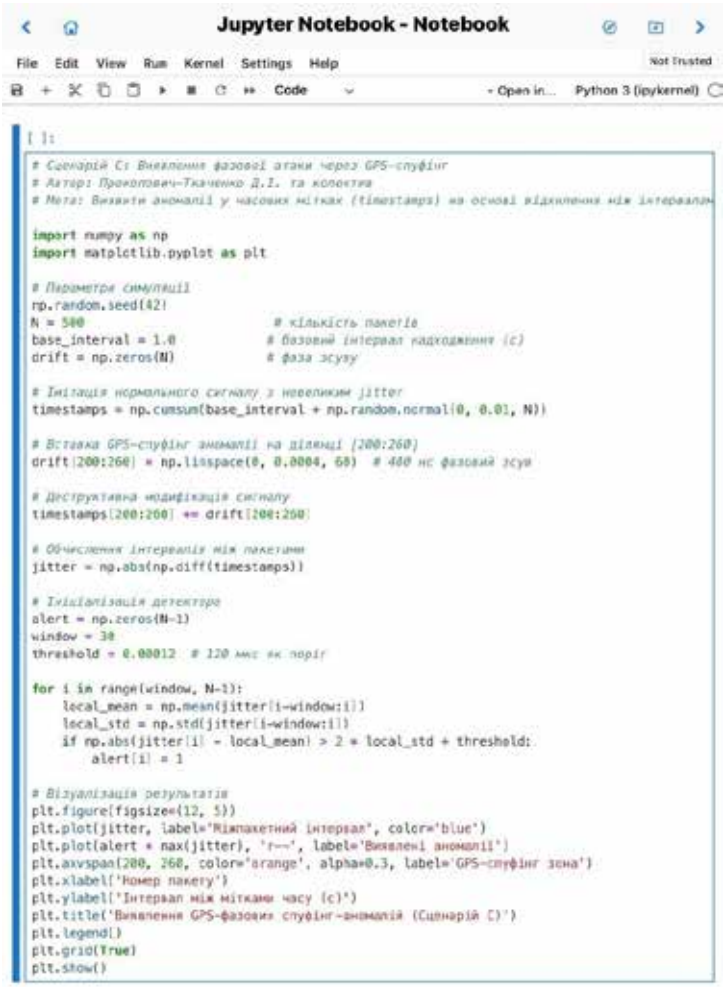

Рис. 2. Відображення програмної реалізації, частина 1

Результат демонструє, що алгоритм успішно виявляє фазову атаку навіть тоді, коли середні мережеві індикатори залишаються у межах норми. Виявлення відбувається з мінімальною затримкою (2–3 секунди), що дозволяє інтегрувати алгоритм у системи цифрових двійників для онлайн-моніторингу критичної інфраструктури. Цей підхід не потребує спеціалізованого обладнання й може бути реалізований на вбудованих пристроях, зокрема в індустріальних контролерах, маршрутизаторах або периферійних вузлах мережі.

Висновки. Отримані результати моделювання та симуляції функціонування телекомунікаційного вузла в умовах комбінованого впливу гібридних атак вказують на наявність критичного розриву між класичними методами моніторингу та реальною динамікою деградаційних процесів. Найбільш суттєве відхилення спостерігалося у сценарії фазового зсуву, коли розсинхронізація міток часу не супроводжувалася миттєвим зростанням звичних мережевих метрик, таких як latency, packet loss або throughput. У таких умовах традиційні SIEM-системи та інструменти моніторингу, засновані на пороговому аналізі, не виявляють аномалій або спрацьовують із значним запізненням. На відміну від зазначених підходів, запропонована в дослідженні модель базується на інтеграції енергетичних, логічних і фазових характеристик у вигляді узагальненої деградаційної функції D(t). Вона дозволяє з високою чутливістю виявляти кумулятивне навантаження на вузол і прогнозувати перехід у деградований стан до появи критичних симптомів. Найважливішим елементом переваги моделі є включення температурного компоненту як активного тригера фазового переходу, що відповідає реальній фізиці функціонування обладнання. У випадку, коли деградація телекомунікаційного вузла супроводжується не лише зміною стану в обчислювальних чи енергетичних доменах, а й фізичними фазовими перетвореннями (наприклад, у матеріалах охолоджуючих систем або композитних елементах), доцільним є розширення моделі за рахунок введення мобільної границі розділу фаз. Така

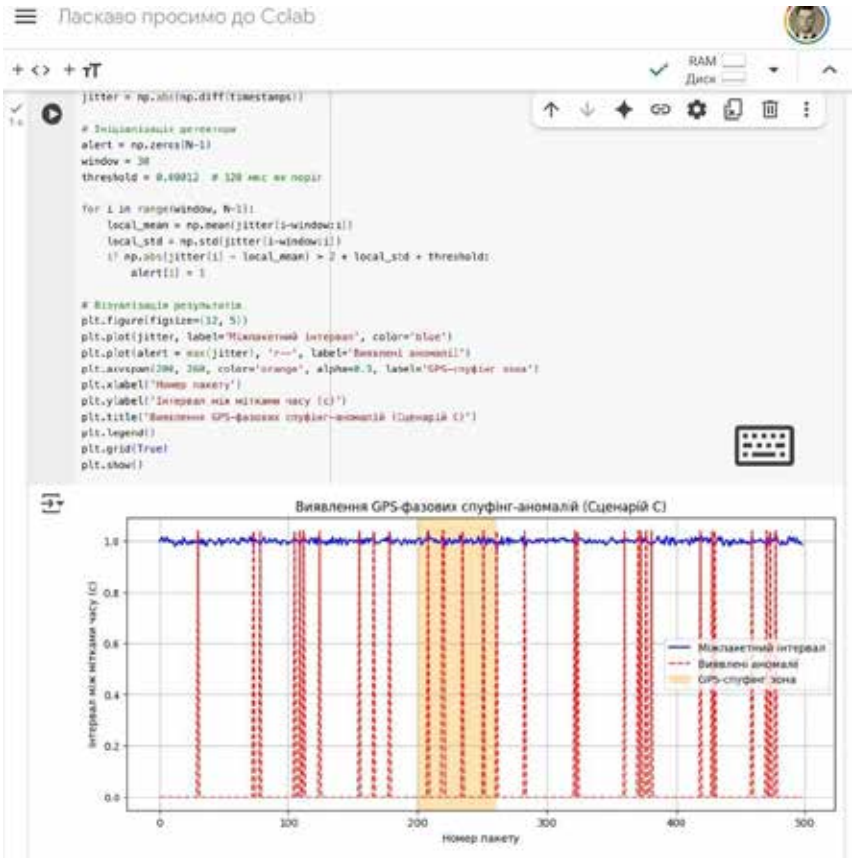

Рис. 3. Відображення програмної реалізації, частина 2

границя визначає межу між двома фізичними станами системи (наприклад, між перегрітою і стабільною областю), яка змінює своє положення залежно від температурного чи енергетичного градієнта. Запровадження цієї компоненти дозволить моделі імітувати не лише миттєву реакцію на перевантаження, а й динаміку просторового розповсюдження деградації, включаючи локальні фазові переходи. Це особливо актуально у випадках, коли вузол містить елементи з фазозалежними властивостями (наприклад, енергозберігаючі матеріали або фазозмінні охолоджувачі), що можуть знижувати ефективність після досягнення певного порогу.

У моделі цифрового двійника реалізація підвижної границі дозволить виявляти режими, за яких зона нестабільності мігрує у просторі, попереджаючи про загрозу каскадної деградації ще до виникнення критичних збоїв. У роботах, присвячених DDoS-атакам або DoS-впливам, основна увага зосереджується на логіці трафіку, його розподілі і об'ємах. Однак температурне перевантаження і зміна режиму енергоспоживання часто залишаються поза увагою. Саме ці аспекти були фундаментальними у запропонованій моделі, що відрізняє її від підходів, заснованих виключно на аналізі мережевих логів. Порівнюючи розроблений алгоритм фазової нестабільності зі стандартними методами виявлення GPS-спуфінгу, слід відзначити його гнучкість і незалежність від апаратної платформи. У класичних рішеннях виявлення базується на фізичному порівнянні фазових сигналів з кількох джерел або аналізі сили сигналу. Такі методи потребують або синхронізації з еталонною годинниковою системою, або багатоканального приймача. Наш алгоритм використовує виключно часові мітки вхідних пакетів і аналізує їх на основі статистичного профілю. Цей підхід робить його придатним для використання у системах з обмеженими ресурсами, включаючи промислові маршрутизатори, edge-комутатори та вбудовані пристрої без доступу до повноцінної GNSS-навігації.

Ще одним ключовим моментом у дискусії є здатність моделі інтегруватися до цифрового двійника. Згідно з сучасними дослідженнями у сфері Smart Grid, Smart Transport та захищених мереж управління, саме цифрові двійники визнаються основою для реалізації активного, адаптивного моніторингу систем у реальному часі. У науковій літературі наявні спроби використовувати моделі деградації на основі статис-

тичних характеристик трафіку, зокрема методи класифікації або нейронні мережі, однак вони не забезпечують пояснювального рівня. Запропонований підхід має перевагу в інтерпретованості – кожен параметр деградації (енергоспоживання, температура, навантаження CPU) прямо відображається у D(t) та може бути візуалізований і використаний для локального прийняття рішень. Важливою перевагою також є стійкість алгоритму до псевдовипадкових коливань. Завдяки ковзному вікну статистичного аналізу та адаптивному порогу, система здатна відрізняти одиничні флуктуації від тренду фазового зсуву. Це особливо важливо в умовах реального мережевого середовища, де присутній фоновий шум, вібрації або коливання навантаження. Аналіз сценарію С продемонстрував, що модель може виявити спуфінг на рівні 400 нс вже через 2–3 секунди після його початку, що значно перевершує типові затримки виявлення на основі агрегацій логів, які сягають десятків секунд. Ще одним фактором, який підсилює конкурентоздатність підходу, є те, що модель не вимагає попереднього навчання, великих вибірок або розмітки даних. Вона функціонує в режимі безперервного адаптивного моніторингу, що забезпечує її придатність до розгортання у гетерогенних інфраструктурах. Це контрастує з глибокими нейронними мережами, які хоч і забезпечують високу точність, але мають значні вимоги до ресурсоємності та верифікації. Розроблений підхід є балансом між точністю, швидкістю та пояснюваністю.

У підсумку можна стверджувати, що запропонована енергетично-інформаційна модель деградації телекомунікаційного вузла має комплексний характер, поєднує фізичні, логічні та часові параметри та забезпечує реалістичне виявлення гібридних впливів, зокрема таких складних, як фазовий GPS-спуфінг. Вона демонструє кращу ефективність в умовах слабких або комбінованих аномалій, де традиційні логіко-орієнтовані методи виявлення виявляються недостатніми. Отримані результати можуть бути використані як основа для формування нових стандартів діагностики стійкості вузлів критичної інфраструктури, особливо у контексті концепції цифрових двійників. Враховуючи масштабованість та платформну незалежність рішення, воно може бути розгорнуте у широкому спектрі промислових та енергетичних систем, забезпечуючи раннє виявлення, пояснюваність інцидентів і підтримку адаптивного реагування у реальному часі.

Список літератури:

1. Risbud P., Gatsis N., Taha A. Multi-period power system state estimation with PMUs under GPS spoofing attacks. *Journal of Modern Power Systems and Clean Energy*. 2020. Vol. 8, № 4. P. 597–606. DOI: 10.35833/MPCE.2020.000125.

2. Siamak S., Dehghani M., Mohammadi M. Dynamic GPS spoofing attack detection, localization, and measurement correction exploiting PMU and SCADA. *IEEE Systems Journal*. 2021. Vol. 15, № 2. P. 2531–2540. DOI: 10.1109/JSYST.2020.3001016.

3. Sabouri M., Alsaeedi A., Al-Toma K. та ін. Increasing the resiliency of power systems in presence of GPS spoofing attacks: a data-driven deep-learning algorithm. *IET Generation, Transmission & Distribution*. 2023. Vol. 17, № 20. P. 4525–4540. DOI: 10.1049/gtd2.12929.

4. Hua F., Gao W., Li Y., Hu P., Qiao L. Joint detection and state estimate with GSAs in PMU-based smart grids. *Energies*. 2023. Vol. 16, № 15. Art. 5731. DOI: 10.3390/en16155731.

5. Larcom J. A., Liu H. Modeling and characterization of GPS spoofing. In: *Proc. 2013 IEEE Int. Conf. on Technologies for Homeland Security (HST)*. Waltham (MA), 2013. P. 729–734. DOI: 10.1109/THS.2013.6699094.

6. Shepard D. P., Humphreys T. E., Fansler A. A. Going up against time: the power grid's vulnerability to GPS spoofing attacks. *GPS World*. Aug. 2012. P. 34–38.

7. Risbud P., Gatsis N., Taha A. Vulnerability analysis of smart grids to GPS spoofing. *IEEE Transactions on Smart Grid*. 2019. Vol. 10, № 4. P. 4506–4519. DOI: 10.1109/TSG.2018.2830118.

8. Xie J., Meliopoulos A. P. S. Sensitive detection of GPS spoofing attack in phasor measurement units via quasi-dynamic state estimation. *IEEE Computer*. 2020. Vol. 53, № 5. P. 60–69. DOI: 10.1109/MC.2020.2976943.

9. Sarailoo M., Wu N. E., Bay J. S. SA-based PMU network upgrade for detectability of GPS spoofing attacks. In: *Proc. 2019 IEEE Power & Energy Society General Meeting (PESGM)*. Atlanta (GA), 2019. P. 1–5. DOI: 10.1109/PESGM40551.2019.8973393.

10. Jatmika M. O., Pratomo A., Gunawan W., Aljaber F., Budiarto R. Investigating DDoS attacks on metro network. *AIP Conference Proceedings*. 2024. Vol. 2987. Art. 020008. DOI: 10.1063/5.0206048.

11. Khan I., Centeno V. Undetectable GPS-spoofing attack on time-series phasor measurement unit data. *arXiv Preprint*. 2022. arXiv:2206.12440. DOI: 10.48550/arXiv.2206.12440.

12. Singh S., Singh A., Goyal V. An analytical view of DoS or DDoS attacks for network architecture. In: *Distributed Intelligent Circuits and Systems*. Singapore: World Scientific, 2024. P. 1–24. DOI: 10.1142/9789811279539_0001.

13. Dehnie S., Ghanadan R. Methods and systems for detecting GPS spoofing attacks. Patent. BAE Systems, 2011. URL: https://scispace.com (дата звернення: 28.07.2025).

14. Oligeri G., Sciancalepore S., Ibrahim O. A., Di Pietro R. Drive me not: GPS spoofing detection via cellular network. In: *Proc. 2019 ACM Wireless Network Security Conference (WiSec)*. Miami (FL), 2019. P. 1–12. DOI: 10.1145/3317549.3319719.

15. Heng Z., Peng S., Liu L., Su S., Cao Y. Review on GPS spoofing-based time synchronisation attack on power system. *IET Generation, Transmission & Distribution*. 2020. Vol. 14, № 12. P. 2275–2287. DOI: 10.1049/IET-GTD.2020.0253.

16. Siamak S., Dehghani M., Mohammadi M. Modelling and detection of GPS-spoofing driven forced oscillation with PMU. In: *Proc. 2024 IEEE Kansas Power and Energy Conference (KPEC)*. Manhattan (KS), 2024. P. 1–6. DOI: 10.1109/KPEC61529.2024.10676092.

17. Saadedeen F., Pal A. GPS spoofing attacks on phasor measurement units: practical feasibility and countermeasures. *arXiv Preprint*. 2021. arXiv:2110.03447.

18. Widodo R. A., Delimayanti M. K., Wulandari A. DDoS attacks detection with deep learning approach using convolutional neural network. *Journal of Applied Informatics and Computing*. 2024. Vol. 8, № 2. P. 235–240. DOI: 10.30871/jaic.v8i2.8242.

19. Hussain A., Marín-Tordera E., Masip-Bruin X., Leligou H. C. Rule-Based With Machine Learning IDS for DDoS Attack Detection in Cyber-Physical Production Systems (CPPS). IEEE Access. 2024. Vol. 12. P. 114895–114910. DOI: 10.1109/ACCESS.2024.3445261.

20. Tu H., Xia Y., Tse C. K., Chen X. A hybrid cyber attack model for cyber-physical power systems. *IEEE Access*. 2020. Vol. 8. P. 114876–114883. DOI: 10.1109/ACCESS.2020.3003323.

21. Lanotte R., Merro M., Muradore R., Viganò L. A formal approach to cyber-physical attacks. *arXiv Preprint*. 2016. arXiv:1611.01377.

22. Sheikh Z. A., Singh Y. A hybrid threat assessment model for security of cyber-physical systems. In: *Proc. 2022 IEEE 7th Int. Conf. on Parallel, Distributed and Grid Computing (PDGC)*. 2022. P. 582–587. DOI: 10.1109/PDGC56933.2022.10053332.

23. Forti N., Battistelli G., Chisci L., Sinopoli B. Joint attack detection and secure state estimation of cyber-physical systems. *International Journal of Robust and Nonlinear Control*. 2019. Vol. 30, № 11. P. 4303–4330. DOI: 10.1002/RNC.4724.

24. Guibene K., Messai N., Ayaida M. Securing cyber-physical industrial systems against false data injection attacks. In: *Proc. 2023 IEEE 5th Int. Conf. on Blockchain Computing and Applications (BCCA)*. 2023. P. 142–149. DOI: 10.1109/BCCA58897.2023.10338925.

25. Mahmoud M. S., Hamdan M. M. Improved control of cyber-physical systems subject to cyber and physical attacks. *Cyber-Physical Systems*. 2019. Vol. 5, № 3. P. 173–190. DOI: 10.1080/23335777.2019.1631889.

26. Lian Z., Shi P., Lim C. P., Rudas I. J., Agarwal R. K. Hybrid stealthy attacks on stochastic event-based remote estimation under packet dropouts. *IEEE Transactions on Network Science and Engineering*. 2024. Vol. 11, № 6. P. 5829–5838. DOI: 10.1109/TNSE.2024.3457911.

27. Vlahakis E. E., Provan G., Werner G., Yang S. J., Athanasopoulos N. Quantifying impact on safety from cyber-attacks on cyber-physical systems. *arXiv Preprint*. 2022. arXiv:2211.12196. DOI: 10.48550/arXiv.2211.12196.

28. Hawrylak P. J., Haney M., Papa M., Hale J. Using hybrid attack graphs to model cyber-physical attacks in the smart grid. In: *Proc. 2012 5th Int. Symposium on Resilient Control Systems (ISRCS)*. 2012. P. 161–164. DOI: 10.1109/ISRCS.2012.6309311.

29. Wang R., Venugopalan S., Adepu S. Safety analysis for cyber-physical systems under cyber attacks using digital twin. In: *Proc. 2024 IEEE Int. Conf. on Cyber Security and Resilience (CSR)*. 2024. P. 1–8. DOI: 10.1109/CSR61664.2024.10679484.

30. Singh A., Jain A. Study of cyber attacks on cyber-physical system. *SSRN Electronic Journal*. 2018. DOI: 10.2139/SSRN.3170288.

31. Khan I., Centeno V. Undetectable GPS-spoofing attack on time-series phasor measurement unit data. *arXiv Preprint*. 2022. arXiv:2206.12440. DOI: 10.48550/arXiv.2206.12440.

32. Oligeri G., Sciancalepore S., Ibrahim O. A., Di Pietro R. Drive me not: GPS spoofing detection via cellular network. In: *Proc. 2019 ACM Wireless Network Security Conference (WiSec)*. 2019. P. 1–12. DOI: 10.1145/3317549.3319719.

33. Heng Z., Peng S., Liu L., Su S., Cao Y. Review on GPS spoofing-based time synchronisation attack on power system. *IET Generation, Transmission & Distribution*. 2020. Vol. 14, № 12. P. 2275–2287. DOI: 10.1049/IET-GTD.2020.0253.

34. Sarailoo M., Wu N. E., Bay J. S. SA-based PMU network upgrade for detectability of GPS spoofing attacks. In: *Proc. 2019 IEEE Power & Energy Society General Meeting (PESGM)*. 2019. P. 1–5. DOI: 10.1109/PESGM40551.2019.8973393.

35. Dehnie S., Ghanadan R. Methods and systems for detecting GPS spoofing attacks. Patent US 2011000000. BAE Systems, 2011. URL: https://scispace.com (дата звернення: 28.07.2025).

36. Singh S., Singh A., Goyal V. An analytical view of DoS or DDoS attacks for network architecture. In: *Distributed Intelligent Circuits and Systems*. Singapore: World Scientific, 2024. P. 1–24. DOI: 10.1142/9789811279539_0001.

37. Jatmika M. O., Pratomo A., Gunawan W., Aljaber F., Budiarto R. Investigating DDoS attacks on metro network. *AIP Conference Proceedings*. 2024. Vol. 2987. Art. 020008. DOI: 10.1063/5.0206048.

38. Widodo R. A., Delimayanti M. K., Wulandari A. DDoS attacks detection with deep learning approach using convolutional neural network. *Journal of Applied Informatics and Computing*. 2024. Vol. 8, № 2. P. 235–240. DOI: 10.30871/jaic.v8i2.8242.

39. Orekhov A. V., Orekhov A. A. Network traffic anomalies automatic detection in DDoS attacks. *Vestnik of St Petersburg University. Applied Mathematics. Computer Science. Control Processes*. 2023. Vol. 19, № 2. P. 251–263. DOI: 10.21638/11701/spbu10.2023.210.

40. Risbud P., Gatsis N., Taha A. Vulnerability analysis of smart grids to GPS spoofing. *IEEE Transactions on Smart Grid*. 2019. Vol. 10, № 4. P. 4506–4519. DOI: 10.1109/TSG.2018.2830118.

41. Shepard D. P., Humphreys T. E., Fansler A. A. Going up against time: the power grid's vulnerability to GPS spoofing attacks. *GPS World*. Aug. 2012. P. 34–38.

Yakovenko V.O., Prokopovich-Tkachenko D.I., Ulyanovska Yu.V. ENERGY-INFORMATION MODEL OF TELECOMMUNICATION NODE DEGRADATION UNDER HYBRID CYBERATTACKS

The article provides a detailed examination of the development of an energy-information model for the degradation of telecommunication nodes, which form the backbone of modern critical infrastructure, under the influence of hybrid cyberattacks. Special attention is given to scenarios where nodes are subjected to combined impacts: massive DDoS attacks paired with physical threats such as power outages, GPS spoofing, or thermal overload. In such conditions, traditional monitoring approaches that focus only on logical network parameters–latency, jitter, throughput–prove insufficient, as they fail to account for changes in the physiological state of the equipment. The degradation of memory, power instability, or abnormal temperature increases often go unnoticed, creating hidden risks and complicating timely response to complex threats.

The proposed model is based on a physically justified approach to describing the functioning of a telecommunication node–such as a router or aggregation node–under multicompound load conditions. It takes into account the phase transition of the system from a normal state to a degraded or pre-failure state under the influence of increasing informational and energy factors. The model makes it possible to analyze changes in the energy profile, thermal regime, and load of processor and memory resources in real time. A special focus is placed on dividing processes into temporal quasi-states, which allows for precisely identifying moments when a node enters the critical instability zone.

The article presents a detailed case analysis of a DDoS attack on an aggregation node accompanied by a GPS spoofing attack, which triggers simultaneous disruption of logical and physical stability. It is demonstrated that the synergistic effect of combined attacks leads to a nonlinear increase in load, which cannot be detected by isolated indicators. Critical threshold values for temperature, energy consumption, and throughput degradation are determined, upon reaching which the node undergoes an irreversible phase transition into a degraded state. The paper proposes effective methods for visualizing risk zones based on the calculation of an integral energy graph for practical implementation in digital twins, enabling timely monitoring and enhancing the resilience of equipment to hybrid cyberattacks.

Key words: *hybrid cyberattack, DDoS, node degradation, critical infrastructure, energy consumption, phase transition, finite model, GPS spoofing, thermal load, digital twin, throughput.*

Дата надходження статті: 16.06.2025
Дата прийняття статті: 28.08.2025
Опубліковано: 27.10.2025