# НАПРЯМ 10. КІБЕРБЕЗПЕКА, ШТУЧНИЙ ІНТЕЛЕКТ ТА ЗАХИСТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ

DOI https://doi.org/10.36059/978-966-397-621-1-61

**Васьков О. В.,**
*студент ІІ курсу магістратури*
*кафедри комп'ютерної інженерії та інформаційних систем*
*Хмельницького національного університету*
*м. Хмельницький, Україна*

## КІБЕРФІЗИЧНА СИСТЕМА УПРАВЛІННЯ СИСТЕМАМИ ЕНЕРГОЗАБЕЗПЕЧЕННЯ ЦЕНТРІВ КОМУТАЦІЇ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

Сучасний стан телекомунікаційної інфраструктури України характеризується зростаючими вимогами до надійності та безперебійності функціонування в умовах цифрової трансформації та нестабільності зовнішнього електропостачання, зумовленої воєнним станом. Центри комутації телекомунікаційних мереж є критично важливими об'єктами, що безпосередньо визначають якість надання цифрових послуг. Ефективне управління системами енергозабезпечення таких об'єктів неможливе в рамках традиційних ізольованих підходів [7].

Концепція кіберфізичних систем (Cyber-Physical Systems, CPS) передбачає тісну інтеграцію обчислювальних компонентів із фізичними процесами через сенсорні мережі, вбудовані контролери та алгоритми інтелектуального управління. Застосування принципів CPS до задач управління енергозабезпеченням телекомунікаційних вузлів дозволяє підвищити ефективність функціонування обладнання, скоротити витрати на технічне обслуговування та мінімізувати час простою у разі аварійних ситуацій [5].

Стандарт EN 50600-2-2 визначає вимоги до систем електропостачання та розподілу об'єктів інформаційно-комунікаційних технологій, формуючи критерії надійності, резервування та безперервності роботи, що безпосередньо слугують методологічною основою при постановці задачі кіберфізичного управління енергозабезпеченням центрів комутації [1].

Аналіз предметної області виявив три взаємопов'язані площини об'єкта: енергетичну (зовнішнє електропостачання, ДБЖ, дизель-

генераторні установки, акумуляторні батареї); інформаційно-керуючу (контролери, шлюзи, SCADA/DCIM-рівні, аналітичні підсистеми); експлуатаційно-організаційну (регламенти обслуговування, процедури аварійного реагування, кібербезпека). Встановлено, що локальна оптимізація окремого вузла не гарантує стійкості системи загалом [3].

Порівняльний аналіз існуючих архітектурних підходів (централізованої AC, DC-орієнтованої та гібридної AC/DC архітектур) показав, що жоден з них в ізольованому вигляді не вирішує завдання комплексного кіберфізичного управління. Централізовані AC-системи мають зайві каскади перетворення енергії та критичну залежність від UPS як вузла концентрації ризику. DC-орієнтовані системи, хоча й оптимальні для телекомунікаційного навантаження, потребують додаткового AC-контуру для допоміжного обладнання. Гібридні архітектури є найбільш гнучкими, однак без єдиної інформаційної моделі перетворюються на набір ізольованих підсистем, які складно адмініструвати [2].

Запропонована архітектура кіберфізичної системи управління базується на взаємодоповнювальних підходах та включає три ієрархічні рівні: нижній (локальні контролери з гарантованим збором телеметрії в реальному часі та виконанням базових сценаріїв захисту навіть за втрати зв'язку), середній (нормалізація даних, координація між енергетичним та кліматичним контурами) та верхній (аналітика, довгострокове прогнозування та кореляція з мережевими платформами оператора). Така побудова поєднує локальну автономність з централізованою інтелектуальною підтримкою [3].

Ключовою особливістю запропонованого підходу є єдина інформаційна модель об'єкта з уніфікованим каталогом сутностей: ввід живлення, секція шин, випрямляч, батарейна гілка, генератор, АВР, кондиціонер, група критичного навантаження, датчик середовища. Для кожної сутності визначені атрибути, ідентифікатор, місце в ієрархії, критичність та зв'язки з іншими компонентами. Така модель є основою цифрового представлення об'єкта, що дозволяє перейти від простого опитування пристроїв до повноцінної кіберфізичної взаємодії [3].

Предиктивна аналітика реалізується через сукупний індикатор технічного стану батарейного контуру, що враховує температуру, струми заряду / розряду, внутрішній опір, історію циклів та вікові характеристики. Поряд із цим для кліматичних підсистем оцінюється тепловий ризик та здатність підтримувати допустимий температурно-вологісний режим. Координація енергетичного та кліматичного контурів є принциповою, оскільки перегрів суттєво прискорює старіння акумуляторів та може спричинити аварійне вимкнення частини навантаження [4].

Пріоритизація навантаження за рівнями критичності дозволяє продовжити роботу ядра мережі навіть у сценаріях критичного дефіциту енергоресурсів. Для типових аварійних сценаріїв (зникнення зовнішнього живлення, збій UPS-модуля, зростання температури, відмова

генератора) сформовані алгоритми реагування з визначенням дій, що виконуються автоматично, та дій, що рекомендуються оператору [7].

Архітектура підтримує інтеграцію різнорідних протоколів на нижньому рівні (Modbus RTU/TCP, SNMP, MQTT, OPC UA) при нормалізації даних на верхньому рівні. Це забезпечує поетапне підключення нових джерел даних без повного перепроєктування системи. Вимоги до кібербезпеки відповідають стандартам ISA/IEC 62443 та рекомендаціям NIST SP 800-82: зонування мереж, контроль доступу, захищений міжрівневий обмін даними, журналювання дій персоналу [3; 6].

Таким чином, запропонована кіберфізична система управління дозволяє подолати ключові проблеми традиційних підходів: фрагментарність моніторингу, реактивний характер технічної експлуатації та неузгодженість енергетичного і кліматичного контурів. Впровадження такої системи дозволить зменшити ризик раптових відмов, скоротити час виявлення та локалізації проблем, підвищити обґрунтованість експлуатаційних рішень та покращити використання енергетичних ресурсів критичної телекомунікаційної інфраструктури [5].

**Список використаних джерел:**

1. EN 50600-2-2:2019. Information technology. Data centre facilities and infrastructures. Part 2-2: Power supply and distribution. 2019. URL: https://knowledge.bsigroup.com/products/information-technology-data-centre-facilities-and-infrastructures-power-supply-and-distribution (дата звернення: 18.03.2026).

2. ETSI EN 300 132-3-1 V2.1.1. Environmental Engineering (EE); Power supply interface at the input to telecommunications and datacom (ICT) equipment; Part 3-1: Direct current source up to 400 V. 2012. URL: https://www.etsi.org/deliver/etsi_en/300100_300199/3001320301/02.01.01_60/en_3001320301v020101p.pdf (дата звернення: 20.03.2026).

3. Griffor E., Greer C., Wollman D., Burns M. Framework for Cyber-Physical Systems: Volume 1, Overview. NIST Special Publication 1500-201. Gaithersburg, 2017. 48 p. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-201.pdf (дата звернення: 18.03.2026).

4. ITU-T Recommendation L.1300. Best practices for green data centres. Geneva, 2014. URL: https://www.itu.int/rec/T-REC-L.1300/en (дата звернення: 20.03.2026).

5. Rajkumar R., Lee I., Sha L., Stankovic J. Cyber-Physical Systems: The Next Computing Revolution. Proceedings of the 47th Design Automation Conference (DAC). New York, 2010. P. 731–736. DOI: 10.1145/1837274.1837461.

6. Stouffer K., Pillitteri V., Lightman S., Abrams M., Hahn A. Guide to Industrial Control Systems (ICS) Security. NIST SP 800-82 Rev. 2. Gaithersburg, 2015. 247 p. URL: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-82r2.pdf (дата звернення: 20.03.2026).

7. Правила технічної експлуатації електроустановок споживачів. Затверджено наказом Міністерства енергетики України від 13.02.2012 р. № 91. Київ, 2012. 272 с.

DOI https://doi.org/10.36059/978-966-397-621-1-62

**Дубко В. О.,**
*доктор фізико-математичних наук, професор*
*Таврійського національного університету імені В. І. Вернадського*
*м. Київ, Україна*

**Распопов В. Б.,**
*кандидат фізико-математичних наук, доцент*
*Інституту кібернетики імені В. М. Глушкова*
*Національної академії наук України*
*м. Київ, Україна*

## ДИДАКТИЧНІ АСПЕКТИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ АКТИВІЗАЦІЇ НАВЧАЛЬНОЇ ДІЯЛЬНОСТІ СТУДЕНТІВ ПРИРОДНИЧИХ ДИСЦИПЛІН

**Вступ.** Сучасна вища освіта переживає епоху глибоких перетворень, зумовлених появою систем штучного інтелекту (ШІ), здатних аналізувати, виводити та пояснювати складні математичні співвідношення. Тож нині університетська дидактика має завдання не лише навчити студентів природничих дисциплін розв'язувати математичні задачі традиційними методами, а й заохотити творчу молодь співпрацювати зі штучним інтелектом як із новим когнітивним партнером. Викладач перестає бути лише джерелом знань – він стає тренером інтелектуальної взаємодії, який вчить майбутніх дослідників грамотно користуватися інструментами «машинного мислення». На прикладі адаптації авторського навчального курсу ***«Стохастичні диференційні рівняння»*** (СДР) для математичного аналізу та прогнозування у гідрометеорології в доповіді ілюструється, як можна реалізувати креативну співпрацю студентів і викладачів університету і НДІ НАН України, з метою підготовки фахівців для впровадження сучасних непрямих методів оперативної оцінки ГДК (гранично допустимих концентрацій) токсичними забрудненнями повітряного середовища. Ілюстрована презентація доповіді є за адресою: URL: https://drive.google.com/drive/folders/1rl7s2NGy8oo367VLXjhLIBP-aiq32F-z