

Секція 4  
**Особливості розвитку національної економіки  
в умовах глобальних викликів**

**МЕТОЛИЧНІ АСПЕКТИ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ  
ЕНЕРГЕТИЧНОЇ ІНФРАСТРУКТУРИ**

*Клименко І.В.*

*Науковий керівник: Мордовцев О.С., к.е.н., доцент  
Харківський національний автомобільно-дорожній університет*

Енергетична безпека це стан захищеності від загроз енергетичній безпеці, а також порушень стабільності та безперервності. Ці загрози визначаються як зовнішніми (геополітичними, макроекономічними, кон'юнктурними) факторами, так і власне станом і функціонуванням енергетичного сектора країни. Загрози енергетичній безпеці традиційно об'єднуються в п'ять основних груп. Останнім часом список загроз був розширений загрозами кібербезпеки, реалізація яких може спровокувати серйозні екстремальні ситуації в енергетиці, чреваті значним зниженням можливостей забезпечення енергоресурсами споживачів. Кіберзагрози розглядаються як один з найважливіших сучасних видів загроз енергетичній безпеці.

Позаштатні ситуації в енергетичному секторі такі, як критичні або надзвичайні, є предметом досліджень енергетичної безпеки. Загрозами енергетичної безпеки є дефіцит потреб в ресурсах прийнятної якості в нормальних умовах і екстремальних ситуаціях, порушення стабільності і безперервності енергозабезпечення

З одного боку, стрімке поширення комп'ютерного середовища, розвиток інформаційних технологій і тенденція переходу до інтелектуальної енергетики роблять кіберзагрози однією з найважливіших тактичних і стратегічних загроз енергетичній безпеці. З іншого боку, на об'єктах критичної інфраструктури на фоні військової агресії та інших зовнішніх чинників спостерігається недооцінювання необхідності проведення систематичних превентивних заходів щодо запобігання кіберзагроз і постійного оновлення засобів захисту, що, в свою чергу, може вплинути на виникнення значного і тривалого дефіциту енергоресурсів в залежності від масштабу і наслідків кібератак.

Аналіз інцидентів показує, що критична інформаційна інфраструктура може бути уразливою для кібератак, здатних привести до руйнування фізичних систем і мереж. Також на фоні війни спостерігається збільшення зловмисних атак на автоматизовані системи управління технологічними процесами. Такі атаки вже не є гіпотетичними, і, відповідно, це вимагають ефективного захисту не тільки від випадкових збоїв, але і подібного виду загроз і небезпек, які є більш складними для прогнозування

Процес «цифровізації» енергетичних мереж, використання інтелектуальних технологій, датчиків і сенсорів Інтернету речей в роботі

енергетичних систем підвищують ризики в області кібербезпеки енергетичних підприємств. При реалізації концепцій інтелектуальної та цифрової енергетики необхідно враховувати наступні потенційні ризики використання сучасних інформаційних технологій, зокрема:

- підвищена складність інформаційної мережі підвищує кількість вразливостей для потенційних атак і ненавмисних помилок;
- мережі, взаємопов'язані з іншими мережами, які також можуть займати кілька «розумних» доменів мережі, збільшують ймовірність каскадних аварій;
- велика кількість взаємозв'язків програмних компонентів збільшує вразливість програмного коду, що спрощує зловмисникам впровадження в програмний код шкідливого коду і вразливостей;
- у міру збільшення вузлів мережі збільшується і число точок входу в систему для зловмисників.

При вирішенні проблеми переходу до інтелектуальної енергетики виділяють дві взаємопов'язані області – технологічна інфраструктура та інформаційно-комунікаційна інфраструктура. Успіх створення системи безпеки багато в чому залежить від успішного застосування сучасних інформаційних технологій. У свою чергу, говорити про застосування останніх має сенс при наявності розвиненої сучасної технологічної інфраструктури. Рішення щодо розвитку технологічної інфраструктури, безумовно, належать до класу стратегічних рішень. Для обґрунтування та підтримки прийняття таких рішень доцільно залучення інтелектуальних інформаційних технологій.

## **СТАТИСТИЧНИЙ АНАЛІЗ ДИСПРОПОРЦІЙ У ФОРМУВАННІ ТА ВИКОРИСТАННІ КРЕДИТНИХ РЕСУРСІВ БАНКІВ**

*Коваленко М.О.*

*Науковий керівник: Непран А. В., к.е.н., доцент  
Харківський національний автомобільно-дорожній університет*

Банківський сектор відіграє важливу роль у розвитку національної економіки. Станом на 1.12.2023 р. обсяг банківських кредитів становив 1007,6 млрд грн, або 19,2 % від ВВП. Стабільний розвиток банківської системи України у значній мірі залежить від формування та використання ресурсів позикового капіталу. Практика розвитку банківської системи в Україні засвідчила, що вітчизняні банки мають низький рівень фінансової стійкості.

Однією із причин порушення фінансової стійкості банківської системи України є наявність диспропорцій у формуванні та використанні ресурсної бази банків. Сутність диспропорції полягає в тому, що ресурсна база банків формується у значній мірі за рахунок короткострокових депозитів, тоді як кредити надаються переважно довгострокові. Такі розриви у формуванні та використанні ресурсної бази банків загрожують фінансовій стабільності банків. Це підтверджується даними табл. 1.