НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ

ІНСТИТУТ ПРОБЛЕМ МОДЕЛЮВАННЯ В ЕНЕРГЕТИЦІ ІМ. Г.Є. ПУХОВА

НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ «КІБЕРБЕЗПЕКА ЕНЕРГЕТИКИ»

Матеріали

03 червня 2026 року

Київ – 2026

УДК [621.3+620.9]::[004[056.53+42+94] + 504.06]
ББК 31
Б-39

Рекомендовано до друку Вченою радою Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України (протокол № 06 від 28 травня 2026 р.)

Б-39 **Кібербезпека енергетики,** науково-практична конференція Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України : матеріали, 03 червня 2026 р. Київ : ІПМЕ ім. Г.Є.Пухова НАН України, 2026. 175 с.

B-39 **Cybersecurity of energy**, scientific-practical conference of the G.E. Pukhov Institute for Modeling in Energy Engineering National Academy of Sciences of Ukraine : materials, June 03, 2026. Kyiv: PIMEE NAS of Ukraine, 2026. 175 p.

В.М. Мацука

УПРАВЛІННЯ КІБЕРРИЗИКАМИ В SMART GRID ТА ЦИФРОВИХ ЕНЕРГЕТИЧНИХ МЕРЕЖАХ

Сучасний енергетичний сектор активно впроваджує цифрові технології, автоматизовані системи управління та мережі Smart Grid. Це підвищує ефективність енергосистем, оптимізує споживання ресурсів і покращує якість енергопостачання, але водночас створює нові кіберризики для критичної інфраструктури. Проблема кібербезпеки особливо актуальна в умовах гібридних загроз і кібератак на енергетичний сектор. Оскільки енергетика є основою функціонування держави та економіки, забезпечення її кіберзахисту стає одним із ключових напрямів державної безпеки [1].

Управління кіберризиками в Smart Grid передбачає комплекс заходів, спрямованих на виявлення, оцінку, мінімізацію та контроль кіберзагроз. Ефективна система управління ризиками повинна поєднувати організаційні, технічні, технологічні та управлінські рішення.

Smart Grid – це інтелектуальна енергетична мережа, яка використовує сучасні цифрові технології для автоматизованого управління процесами генерації, передачі, розподілу та споживання електроенергії. Основною особливістю Smart Grid є двосторонній обмін інформацією між усіма учасниками енергетичної системи.

До структури Smart Grid входять: автоматизовані системи диспетчерського управління (SCADA); інтелектуальні лічильники; цифрові підстанції; IoT-пристрої; сенсори моніторингу; хмарні сервіси; системи аналізу великих даних [2].

Використання цифрових технологій дозволяє здійснювати оперативний контроль за станом енергомережі, прогнозувати навантаження, зменшувати втрати електроенергії та підвищувати енергоефективність. Однак інтеграція великої кількості цифрових компонентів одночасно збільшує кількість потенційних вразливостей.

Сучасні енергетичні мережі фактично перетворюються на кіберфізичні системи, де порушення роботи інформаційної інфраструктури може спричинити фізичні наслідки: аварії, знеструмлення об’єктів або пошкодження обладнання [3].

Кіберризики в інтелектуальних енергетичних мережах є багаторівневими та складними. Найпоширенішими загрозами є: несанкціонований доступ до систем управління; атаки на SCADA-системи; DDoS-атаки; зараження шкідливим програмним забезпеченням; компрометація IoT-пристроїв; фішингові атаки; перехоплення каналів передачі даних; внутрішні загрози з боку персоналу.

Особливо небезпечними є атаки на операційні технології (OT), оскільки вони безпосередньо впливають на функціонування енергетичного обладнання. Порушення роботи диспетчерських систем може призвести до масштабних аварій та економічних збитків.

Зростання кількості підключених пристроїв у Smart Grid збільшує поверхню атак. Багато IoT-пристроїв мають низький рівень захисту, що робить їх потенційною точкою проникнення до енергетичної мережі.

Одним із найвідоміших прикладів кібератак на критичну інфраструктуру стала атака на українські енергетичні компанії у грудні 2015 року. Унаслідок втручання хакерів було тимчасово відключено електропостачання для сотень тисяч споживачів.

Зловмисники отримали доступ до корпоративних мереж через фішингові листи та шкідливе програмне забезпечення BlackEnergy. Після проникнення в систему вони змогли дистанційно керувати SCADA-системами та вимикати електропідстанції.

Цей випадок продемонстрував: критичну важливість сегментації мереж; необхідність багатофакторної автентифікації; потребу у постійному моніторингу кіберзагроз; важливість підготовки персоналу до кіберінцидентів.

У 2016 році було зафіксовано ще одну масштабну атаку на українську енергетичну інфраструктуру із застосуванням шкідливого програмного забезпечення Industroyer (CrashOverride). Особливістю цього вірусу була його здатність взаємодіяти з промисловими протоколами управління енергетичними системами.

Програма автоматично виконувала команди відключення енергетичного обладнання, що свідчить про високий рівень підготовки кіберзлочинців.

Після інциденту енергетичні компанії почали активніше впроваджувати: SOC-центри; системи виявлення вторгнень; резервне копіювання; процедури реагування на кіберінциденти.

У 2021 році кібератака на компанію Colonial Pipeline стала однією з найрезонансніших у світі. Внаслідок ransomware-атаки було тимчасово зупинено найбільший паливний трубопровід США [4].

Хоча атака була спрямована переважно на IT-інфраструктуру компанії, керівництво ухвалило рішення тимчасово припинити роботу операційних систем для уникнення подальших ризиків.

Цей кейс підтвердив: взаємозалежність IT- та OT-систем; необхідність резервування критичних даних; важливість планів безперервності бізнесу; значення кризового менеджменту в умовах кібератак.

Управління кіберризиками є безперервним процесом, спрямованим на забезпечення кіберстійкості енергетичної інфраструктури. Основними етапами цього процесу є:

На першому етапі визначаються критичні активи системи та потенційні джерела загроз. Особлива увага приділяється SCADA-системам, каналам зв'язку, серверному обладнанню та системам диспетчеризації.

Оцінка ризиків передбачає визначення ймовірності реалізації кіберзагроз та масштабу можливих наслідків. Для цього застосовуються міжнародні стандарти ISO/IEC 27001, ISO/IEC 27005 та NIST Cybersecurity Framework.

До основних заходів мінімізації ризиків належать: сегментація мережі; шифрування даних; контроль доступу; багатофакторна автентифікація; регулярне оновлення програмного забезпечення; резервне копіювання; використання IDS/IPS-систем.

Системи моніторингу забезпечують виявлення аномалій та оперативне реагування на кіберінциденти. Для цього використовуються SOC-центри та SIEM-платформи, які здійснюють аналіз подій безпеки в режимі реального часу.

Ефективність кіберзахисту залежить не лише від технічних рішень, але й від якості управління. Організаційна складова включає: розроблення політики кібербезпеки; розподіл відповідальності; проведення аудиту безпеки; навчання персоналу; створення планів реагування на інциденти; управління безперервністю діяльності [5].

Людський фактор залишається одним із головних джерел кіберризиків, тому регулярне навчання працівників є важливою умовою забезпечення кіберстійкості.

Крім того, важливого значення набуває формування культури кібербезпеки на підприємствах енергетичного сектору.

Серед сучасних технологій захисту Smart Grid можна виділити: системи SIEM; IDS/IPS; Zero Trust Architecture; технології штучного інтелекту; блокчейн; системи резервування даних; засоби криптографічного захисту.

Особливо перспективним є використання штучного інтелекту для автоматичного виявлення аномальної активності в енергетичних мережах. AI-системи здатні аналізувати великі обсяги даних та прогнозувати потенційні загрози.

Концепція Zero Trust передбачає перевірку кожного користувача та пристрою незалежно від місця їхнього підключення, що значно зменшує ризик несанкціонованого доступу.

Подальший розвиток Smart Grid супроводжуватиметься збільшенням кількості цифрових компонентів, IoT-пристроїв та хмарних сервісів. Це вимагатиме створення адаптивних систем кіберзахисту, здатних оперативно реагувати на нові загрози.

Одним із ключових напрямів розвитку є впровадження концепції кіберстійкості (Cyber Resilience), яка передбачає не лише захист від атак, але

й здатність швидко відновлювати функціонування системи після інциденту [6].

Для України питання кібербезпеки енергетики має стратегічне значення, оскільки стабільне функціонування енергосистеми безпосередньо впливає на національну безпеку та економічну стабільність держави.

Управління кіберризиками в Smart Grid та цифрових енергетичних мережах є одним із ключових напрямів забезпечення безпеки критичної інфраструктури. Активна цифровізація енергетичного сектору створює нові можливості для підвищення ефективності енергосистем, але водночас збільшує кількість потенційних кіберзагроз.

Практичні кейси кібератак на енергетичну інфраструктуру України та інших держав демонструють необхідність комплексного підходу до кіберзахисту. Ефективна система управління кіберризиками повинна поєднувати сучасні технології захисту, ефективний менеджмент, підготовку персоналу та міжнародні стандарти інформаційної безпеки.

Забезпечення кіберстійкості Smart Grid є необхідною умовою стабільного функціонування енергетики та гарантування енергетичної безпеки держави в умовах сучасних кіберзагроз.

1. Медвідь, В. Ю., Дячков, Д. В., Галич, О. А., Калініченко, О. В., & Лесюк, В. С. (Ред.). (2026). Вплив воєнного стану та політика повоєнного відновлення України: національні стратегії, регіональна безпека та стійкість громад [Колективна монографія]. ПП «Астрая». https://repository.mu.edu.ua/jspui/handle/123456789/10696.
2. Костюк, Ю. В., Складанний, П. М., Рзаєва, С. Л., Самойленко, Ю. О., & Коршун, Н. В. (2025). Інтелектуальні системи керування та захисту в кіберфізичних і хмарних середовищах Smart Grid. Кібербезпека: освіта, наука, техніка, 2(30), 125–156.
3. Стойка, А. В., Верительник, С. М., & Мацука, В. М. (2025). Діджиталізація управління проєктами і вплив на світову економіку та інвестиції. Вчені записки, 39(2), 45–58. http://doi.org/10.33111/vz_kneu.39.25.02.04.026.032.
4. Cherep, A. V., Dashko, I. M., Ohrenych, Yu. O., Cherep, O. H., & Helman, V. M. (Eds.). (2025). European experience in the use of digital technologies in the economy [Collective monograph]. Baltija Publishing. European Experience Monograph. https://dspace.znu.edu.ua/xmlui/bitstream/handle/12345/26563/0063121.pdf?sequence=3#page=193.
5. Cherep, A. V., Dashko, I. M., Ohrenych, Yu. O., & Cherep, O. H. (Eds.). (2024). Theoretical and methodological foundations for the use of digital technologies in Ukraine through the implementation of EU experience [Collective monograph]. Publisher of FOP Mokshanov V.V. Digital Technologies in Ukraine Monograph https://dspace.znu.edu.ua/xmlui/handle/12345/24080.
6. Information Technology Laboratory. Computer Security Resource Center. (2014). Guidelines for Smart Grid Cybersecurity https://csrc.nist.gov/pubs/ir/7628/r1/final.