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. 168 с.

В-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. 168 p.

© Автори публікацій, 2026
© ІПМЕ ім. Г.Є. Пухова НАН України, 2026

ОРГАНІЗАТОРИ КОНФЕРЕНЦІЇ

Інституті проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України
(м. Київ)

ПРОГРАМНИЙ КОМІТЕТ

Мохор Володимир Володимирович
член-кореспондент НАН України, доктор технічних наук, професор,
директор Інституту, голова програмного комітету

Чемерис Олександр Анатолійович
доктор технічних наук, професор,
заступник директора з наукової роботи

Чьочь Вікторія Володимирівна
кандидат технічних наук,
заступник директора з науково-технічної роботи

Артемчук Володимир Олександрвич
доктор технічних наук,
заступник директора з науково-організаційної роботи

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Артемчук Володимир Олександрвич
доктор технічних наук,
заступник директора з науково-організаційної роботи

Клименко Тетяна Михайлівна
завідувачка науково-організаційного відділу

Цуркан Оксана Володимирівна
молодший науковий співробітник

Я.Ю. Дорогий, В.С. Ракович, В.В. Цуркан

КОНЦЕПТУАЛЬНІ РІВНІ ПОВІДОМЛЯННЯ ПРО ПОДІЇ КІБЕРБЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Кібербезпека об'єктів критичної інфраструктури обумовлюється узгодженістю з міжнародними, регіональними та національними нормативними документами [1–6]. Перш за все це пов'язується з прагненнями України до європейського та євроатлантичного інтегрування. Крім того, кібербезпека об'єктів критичної інфраструктури забезпечується розроблянням відповідної національної системи [1]. В межах діяльностей її складників передбачається взаємодіяння з відповідними міжнародними структурами. Тож урахування найкращих світових практик доповнюється необхідністю гармонізування вітчизняного законодавства з нормативними документами міжнародної організації зі стандартизації [2–4], Європейського союзу [5], Національного інституту стандартів і технологій [6]. Тому формулювання концептуальних рівнів повідомляння про події кібербезпеки об'єктів критичної інфраструктури актуальне.

Міжнародний рівень визначається на основі серії нормативних документів ISO/IEC 27035 [3], а також [4]. При цьому поводження з інцидентами є одним з ключових організаційних заходів оброблянння неприйнятних ризиків. Він реалізується при розроблянні систем управління інформаційною безпекою [2]. У межах даного рівня об'єкт критичної інфраструктури інтерпретується як організація. Цим обумовлюється необхідність упроваджування механізму своєчасного повідомляння працівниками або відповідальної особи, або підрозділу кіберзахисту про події кібербезпеки встановленими каналами [1, 3]. Насамперед стосовно вірогідних або порушень властивостей інформації, або збоїв відповідних заходів і засобів. Тож подія кібербезпеки інтерпретується як один з визначальних об'єктів інциденту. З огляду на дескриптивне представлення потоку подій ініціюється отриманням інформації про неї [1]. За результатами виявляння і звітування подія кібербезпеки оцінюється. Як наслідок, приймається рішення стосовно її належності до інциденту.

Регіональний рівень визначається настановами директиви NIS 2 і насамперед узгоджується з прагненням України до європейського інтегрування [5]. Вони стосуються перш за все інформаційної інфраструктури (наприклад, мережевих та інформаційних систем). На регіональному рівні ключовим поняттям залишається «Інцидент», а також послідовність і дієвість поводження з повідомленнями про нього. Це спонукає до запроваджування «єдиного вікна» – механізму автоматичного та прямого звітування перед зацікавленими сторонами [5]. Його використанням передбачено врахування угод нерозголошення інформації за протоколом TLP. Таким підходом передбачається гармонізування шаблонів повідомлень про інциденти кібербезпеки. При цьому їх врегулювання покладається на групи реагування на інциденти комп'ютерної безпеки/комп'ютерні надзвичайні ситуації (CSIRT/CERT). Дане завдання виконується оброблянням великих обсягів інформації про вразливості, загрози, ризики.

Національний рівень визначається настановами директиви NIST SP 800-61:Rev. 3 і, за аналогією з регіональним, насамперед узгоджується з прагненням України до євроатлантичного інтегрування [6]. Основна увага зосереджується на несприятливих подіях кібербезпеки інформаційних систем. І, водночас, на реалізуванні єдиного підходу як при внутрішньому, так і при зовнішньому обміні інформацією між організаціями [6]. При цьому реагування на інциденти розглядається як критично важливий складник процесу управління ризиками. Його впроваджування ґрунтується на шести функціях фреймворку кібербезпеки CSF 2.0. Так [6], реалізування функції ідентифікування (англ. Identify) передбачає усвідомлювання потенційних несприятливих подій. З огляду на це вживаються відповідні заходи забезпечування кібербезпеки (англ. Protect). Виокремлені дії виконуються відповідно до встановлених стратегії і політики управління ризиками (англ. Govern). Тоді як реагування на інциденти починається у межах функції виявляння (англ. Detect).

Отже, концептуальні рівні повідомляння про події кібербезпеки об’єктів критичної інфраструктури формулюються з урахуванням, по-перше, прагнення України до європейського та євроатлантичного інтегрування. По-друге, необхідності взаємодіяння з відповідними міжнародними системам. Як наслідок, сформульовано міжнародний, регіональний і національній рівні повідомляння про події кібербезпеки об’єктів критичної інфраструктури. Характерною особливістю міжнародного рівня є зосередженість на події, встановленні ознак її належності до інциденту. Для обробляння події кібербезпеки передбачається розробляння і впроваджування в організації механізму повідомляння. Тоді як у межах двох інших рівнів основна увага зосереджується на діяльності стосовно поводження з інцидентами.

1. Цуркан В., Ракович В. Механізм повідомляння про події кібербезпеки об’єктів критичної інфраструктури. *Кібербезпека : освіта, наука, техніка*. 2026. Том 4, № 32. P. 1002–1014. DOI: https://doi.org/10.28925/2663-4023.2026.32.1200.
2. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection. Information security management systems. Requirements. [Valid from 2022-09-23]. URL: https://www.iso.org/standard/27001 (accessed on: 25.05.2026).
3. ISO/IEC 27035-1:2023. Information technology. Information security incident management. Part 1: Principles and process. [Valid from 2023-02-13]. URL: https://www.iso.org/standard/78973.html (accessed on: 25.05.2026).
4. ISO/IEC/IEEE FDIS 23612:2025. Software and systems engineering. Incident management. [Valid from 2025-11-18]. Geneva, 2025. 41 p.
5. Про заходи для високого спільного рівня кібербезпеки на всій території Союзу, внесення змін до Регламенту (ЄС) № 910/2014 та Директиви (ЄС) 2018/1972 та скасування Директиви (ЄС) 2016/1148 (Директива NIS 2) : Директива європейського парламенту і ради (ЄС) 2022/2555 від 14.12.2022. URL:https://zakon.rada.gov.ua/laws/show/9a3_001-22#Text (дата звернення: 25.05.2026).
6. NIST SP 800-61:2025 (Rev. 3). Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile. [Valid from 2025-04-03]. URL: https://csrc.nist.gov/pubs/sp/800/61/r3/final (accessed on: 25.05.2026).