МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ТАРАСА ШЕВЧЕНКА

IX МІЖНАРОДНА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

«Проблеми кібербезпеки інформаційно-комунікаційних систем» (PCSICS)

24 квітня 2026 року

Збірник матеріалів доповідей та тез

Київ – 2026

УДК 621.39:351.861(06)
ББК 32.88:67.401.212.431
П 78

Редакційна колегія:
В.В. Ільченко, д.ф-м.н., проф., (голова);
І.І. Пархоменко, *к.т.н. доцент;* ***О.А. Лаптєв***, д.т.н., с.н.с.(голова організаційного комітету);

П78 Проблеми кібербезпеки інформаційно-комунікаційних систем: Збірник матеріалів доповідей та тез; м. Київ, 24 квітня 2026 року; Київський національний університет імені Тараса Шевченка / Редкол.: *В.В. Ільченко, д.ф-м.н., проф., (голова);* та ін. – К.: ВПЦ "Київський університет", 2026. – 194 с.

Тексти виступів і тез опубліковано в авторській редакції однією з робочих мов конференції: українською, англійською.

УДК 621.39:351.861(06)
ББК 32.88:67.401.212.431

© Київський національний університет імені Тараса Шевченка, 2026

Дескриптивне представлення подій кібербезпеки об'єктів критичної інфраструктури

Ярослав Дорогий[1], Владислав Ракович[2], Василь Цуркан[3]

1. Донецький національний технічний університет, УКРАЇНА, м. Дрогобич, вул. Самбірська, 76, E-mail: yaroslav.dorohyi@donntu.edu.ua

2. Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України, УКРАЇНА, м. Київ, вул. Олега Мудрака, 15, E-mail: covlad@ukr.net

3. Національний технічний університет України "Київський політехнічний інститут ім. Ігоря Сікорського", УКРАЇНА, м. Київ, Берестейський просп., 37, E-mail: v.v.tsurkan@gmail.com

Коротка анотація – The process of reporting cybersecurity events in organizations of both state and private ownership has been examined. Particular attention is paid to its relevance in preventing violations of the properties of information assets and the critical infrastructure facilities functioning. This is achieved through the existence of a structured approach to cybersecurity incident management. The feasibility of its implementation is determined by the completeness of the information collected about the event. Depending on this, the event may be classified as an incident. This underscores the importance of the descriptive representation of cybersecurity events involving critical infrastructure facilities. Among the components, the following have been identified: activity, information asset, control, tool, vulnerability, and threat. These components are characterized by their constant existence and manifestation depending on the presence of "favorable" conditions. Overall, they establish indicators of events and determine their attribution to the class of cybersecurity incidents.

Keywords – critical infrastructure facility, cybersecurity, event, incident, descriptive representation.

Вступ

Порушуваннями властивостей інформації та/або функційності заходів, засобів забезпечування кібербезпеки визначаються відповідні події. Їх настання може призводити до негативного впливання на інформаційні активи та, як наслідок, функціонування об'єктів критичної інфраструктури. Тому кожну з них можна класифікувати як або подію, або інцидент. Цим розмежовується успішність/не успішність кібератаки, відсутність/наявність порушень властивостей насамперед конфіденційності, цілісності та доступності інформаційних активів [1–4].

Запобігання і реагування на інциденти кібербезпеки досягається завдяки існуванню структурованого процесу планування і підготовляння, виявляння і звітування, оцінювання і вирішування. Цим може забезпечуватися належність класифікування подій. Воно реалізується шляхом збирання наявної інформації від виявляння до повідомляння про їх настання. Повнотою отриманих даних визначається оцінювання і класифікування подій як інцидентів кібербезпеки [1, 2].

Отже, дескриптивне представляння подій кібербезпеки об'єктів критичної інфраструктури є актуальним.

I Дескриптивне представлення складників подій кібербезпеки об'єктів критичної інфраструктури

З подією кібербезпеки об'єкта критичної інфраструктури асоціюються такі складники [2]: діяльність, інформаційний актив, захід, засіб, уразливість, загроза, інцидент. Залежно від ступеня їх урахування унеможливлюється завдання шкоди життєво важливим національним інтересам [3, 4]. Це реалізується завдяки забезпечуванню функційності, безперервності, відновлюваності, стійкості об'єкта критичної інфраструктури [3].

Виокремлені діяльності орієнтовані на надання життєво важливих функцій та/або послуг організаціями як державної, так і приватної форм власності. Кожною з них створюється, збирається, обробляється, зберігається, передається і знищується інформація [5–8]. Для організацій і, зокрема, об'єктів критичної інфраструктури вона характеризується цінністю і тлумачиться як актив. Тож забезпечуванням її безпеки обумовлюється досягненість встановленої мети діяльності. Наприклад [2, 3], надання життєво важливих функцій та/або послуг об'єктами критичної інфраструктури.

Уразливістю визначається слабкість інформатиційного активу та/або заходу, засобу забезпечування кібербезпеки. Їх існування призводить або може призводити до створювання обставин для реалізування загроз [1, 5, 7]. Серед типових різновидів уразливостей виокремлюються технічні, кадрові процедурні слабкості. Наприклад [1], застосовність операційної системи Windows 7, неналежність обізнаності користувачів про дії у випадку отримання підозрілих електронних листів, неправильність розподіляння прав доступу користувачам.

Потенційні причини виникання інциденту кібербезпеки узагальнюються поняттям загрози [5]. Її реалізування призводить або може призводити до настання шкоди як окремим інформаційним активам, так і об'єкту критичної інфраструктури загалом. Наприклад [1, 9], виконання зловмисниками довільного коду на комп'ютері жертви через віддалений робочий стіл, отримання електронного листа з підозрілим вкладенням (файли з розширеннями, наприклад, *.exe, *.docm), підвищування зловмисником своїх прав доступу до інформаційних активів.

Виниканню потенційних причин інциденту кібербезпеки запобігається розроблянням і впроваджуванням заходів і засобів у межах обраних варіантів обробляння ризиків [1, 2, 6–8]. Завдяки цьому модифікується їх величина через або вірогідність, або наслідки. Даний варіант прийнятний для двох критеріїв оцінювання ризиків. Наприклад [1, 6], оновлення операційної системи Windows 7 до версії 10 або 11, проведення навчань користувачів моделюванням надсилань електронних листів з підозрілими вкладеннями, встановлювання користувачам найменших привілеїв.

І вразливості, і загрози можуть призводити або призводять до настання однієї (декількох) небажаних або неочікуваних подій. З їх появою пов'язується виникання інцидентів кібербезпеки. Зокрема негативного впливання на діяльність об'єктів критичної інфраструктури. Наприклад [1, 10], змінювання даних користувачів в операційні системі Windows 7, підтверджування користувачем персональних даних за "посиланням" з отриманого електронного листа.

Наданням об'єктами критичної інфраструктури життєво важливих функцій та/або послуг задовольняються потреби людей, суспільства, держави [1, 2]. Порушування таких активностей може призвести до завдання шкоди важливим національним інтересам. Цим визначається вагомість об'єктів критичної інфраструктури для економіки, національної безпеки та оборони. Зазначене розкривається використанням поняття діяльності. Вона направлена на досягнення встановленої мети, наприклад, надання захищеного доступу до Інтернету.

II Дескриптивне представлення відношень між складниками подій кібербезпеки об'єктів критичної інфраструктури

Виокремлені складники діяльність, інформаційний актив, захід, засіб, уразливість, загроза асоціюються з об'єктом критичної інфраструктури [2]. Вони пов'язані між собою, можуть мати різний ступінь прояву, наприклад, існувати, не існувати, бути відомими або не відомими. І, залежно від цього призводити до виникання подій кібербезпеки. Тож розумінням відношень між складниками події кібербезпеки обумовлюються результати їх класифікування на фазі "Оцінювання і вирішування" [1, 2].

У межах організацій державної і приватної форм власності інформація є цінністю. Нею як активом визначається досягненість мети діяльності об'єктів критичної інфраструктури. Попри це впродовж життєвого циклу інформаційним активам притаманні слабкості. Їх існування може призводити до порушування властивостей насамперед конфіденційності, цілісності та доступності. Це означає, що уразливості наражають інформаційні активи на небезпеку. Зокрема створюються обставини для використання слабкостей загрозами. Вони реалізуються з метою порушування властивостей інформаційних активів і, як наслідок, завдання шкоди об'єктам критичної інфраструктури. Так унеможливлюється задоволення потреб людей, суспільства, держави. Запобігання цьому досягається обиранням і впроваджуванням заходів і засобів забезпечування кібербезпеки. Разом з тим, їм також приманні вразливості як потенційні точки входу загроз. В обох випадках для інформаційних активів, заходів, засобів забезпечування кібербезпеки і вразливості, і загрози можуть бути або відомі, або невідомі [1, 2, 5–8]. Тому важливо бути обізнаним стосовно появляння емерджентних (нових) ризиків [10]. Дані рекомендації поширюється і на заходи та засоби забезпечування кібербезпеки.

Реалізування загроз, використання уразливостей інформаційних активів, заходів, засобів може спричиняти виникання подій. Тож важливо на фазі "Планування і підготовлення" визначити як індикатори настання, так і потенційні джерела (наприклад, працівника, команди спостережування об'єкта критичної інфраструктури) з механізмом повідомлення про них. Його використання дозволить у межах фази "Виявляння і звітування" зосередитися на збиранні відомостей про подію (події) кібербезпеки. До того ж шляхом оцінювання отриманих результатів визначити чи вона (вони) впливають на діяльність об'єкта критичної інфраструктури та, як наслідок, класифікувати її (їх) як інциденту кібербезпеки [1, 2, 5–8].

Висновок

Отже, дескриптивне представляння дозволяє виокремити та встановити відношення між складниками подій кібербезпеки об'єктів критичної інфраструктури. Серед них виокремлено перш за все діяльність, інформаційний актив, захід, засіб, уразливість, загроза. Кожен зі складників характеризується постійністю існування і проявляється залежно від наявності "сприятливих" причин. Насамперед це актуально для встановлювання індикаторів виникання подій. Оскільки від цього залежить класифікованість/не класифікованість їх як інциденту кібербезпеки. До того ж ефективність управління ними, запобігання порушенням діяльності об'єктів критичної інфраструктури та, як наслідок, завдання шкоди важливим національним інтересам

Література

[1] 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: 30.03.2026).

[2] Цуркан В. В., Ракович В. С. Механізм повідомляння про події кібербезпеки об'єктів критичної інфраструктури. *Кібербезпека : освіта, наука, техніка*. 2026. Том 4 № 32. DOI: https://doi.org/ 10.28925/2663-4023.2026.32.1200.

[3] Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-20. Дата оновлення: 21.09.2024. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 30.03.2026).

[4] Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-19. Дата оновлення: 19.10.2025. URL: https://zakon.rada.gov.ua/ laws/show/2163-19#Text (дата звернення: 30.03.2026).

[5] ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection. Information security management systems. Requirements. [Valid from 2022-10-25]. URL: https://www.iso.org/ru/standard/ 27001 (accessed on: 30.03.2026).

[6] ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection. Information security controls. [Valid from 2022-02-15]. URL: https://www.iso.org/standard/ 75652.html (accessed on: 30.03.2026).

[7] ISO/IEC 15408-1:2022. Information security, cybersecurity and privacy protection. Evaluation criteria for IT security. Part 1: Introduction and general model. [Valid from 2022-08-09; revised 2023-10-27]. URL: https://www.iso.org/standard/72891.html (accessed on: 30.03.2026).

[8] ISO/IEC 27032:2023. Cybersecurity. Guidelines for Internet security. [Valid from 2023-06-28]. URL: https://www.iso.org/standard/76070.html (accessed on: 30.03.2026).

[9] Критична вразливість в старих версіях ОС Windows. URL: https://cert.gov.ua/article/2661 (дата звернення: 30.03.2026).

[10] Мохор, В. В., Бакалинський, О. О., Дорогий, Я. Ю., Цуркан В. В. Парадигма нових ризиків кібербезпеки. *Кібербезпека енергетики* : науково-практична конференція (Київ, 29 травня 2024 р.). Київ : ІПМЕ ім. Г. Є. Пухова НАН України, 2025. С. 116–117. DOI: https://doi.org/10.5281/zenodo.14601760.