doi: https://doi.org/10.15407/visn2025.08.059

КОРЧЕНКО
Олександр Григорович —
член-кореспондент НАН України, перший проректор Державного університету інформаційно-комунікаційних технологій

МЕТОДИ ТА МОДЕЛІ ОЦІНЮВАННЯ СТАНУ КІБЕРЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ДЕРЖАВИ

Стенограма доповіді на засіданні Президії НАН України 18 червня 2025 року

У доповіді акцентовано увагу на тому, що розроблення та впровадження ефективних засобів і систем оцінювання стану кіберзахисту об'єктів критичної інфраструктури держави й рівня гібридних загроз є актуальним науковим завданням. Розглянуто отримані в Державному університеті інформаційно-комунікаційних технологій, у межах розробок наукової школи «Кібербезпека», теоретичні та практичні результати, спрямовані на створення нових, гнучких та адаптивних методів захисту об'єктів критичної інфраструктури і розроблення ефективних систем оцінювання кіберзагроз.

Шановний пане президенте!
Шановні члени Президії! Шановні колеги!
Кібербезпека має вирішальне значення для функціонування держави, економіки та суспільства, особливо в умовах підвищеного впливу кіберзагроз. Стан кіберзахисту об'єктів критичної інфраструктури визначається проведенням оцінки рівня готовності, спроможності та ефективності заходів, які здійснюють для забезпечення безпеки критичних систем, з метою виявлення вразливостей в інфраструктурі об'єкта, оцінювання відповідності впроваджених заходів національним стандартам і вимогам Державної служби спеціального зв'язку та захисту інформації України, прийняття рішень щодо підвищення рівня кіберзахисту, підготовки до інцидентів та зменшення ризиків.

У Стратегії кібербезпеки України одним із головних завдань визначено проведення постійного моніторингу стану кіберзахисту об'єктів критичної інфраструктури.

Загалом до об'єктів критичної інфраструктури належать об'єкти (фізичні або віртуальні), порушення функціонування яких може призвести до загроз національній безпеці, значних економічних втрат, порушення життєдіяльності населення тощо.

Інтенсивний розвиток сучасних інформаційних технологій та штучного інтелекту супроводжується появою нових кіберзагроз та збільшенням кількості кіберінцидентів. За одну добу кількість таких подій в Україні може перевищувати один мільйон. Так, за даними Державної служби спеціального зв'язку та захисту інформації України, 25 травня 2025 р. сталося 1 436 154 кіберінциденти. Крім того, в умовах війни спостерігається стрімке зростання гібридних загроз у секторі цивільної безпеки.

Гібридні загрози в контексті кібербезпеки виникають через поєднання різних видів впливів — технологічних, соціальних, інформаційних, і це ускладнює їхню ідентифікацію, прогнозування та нейтралізацію. Такі загрози є багатовимірними — кібератаки, дезінформаційні кампанії, маніпуляції соціальними процесами, і породжують виклики не лише для інформаційної безпеки, а й для стабільності функціонування державних, економічних і технічних систем. Тому питання оцінювання стану кіберзахисту об'єктів критичної інфраструктури держави та ризиків гібридних загроз набуває особливої актуальності.

Розглянемо основні проблеми, які виникають у процесі оцінювання стану кіберзахисту. Насамперед вони пов'язані з тим, що:

- наявні методики не охоплюють усього спектра сучасних загроз;
- вихідні дані часто залишаються неповними, фрагментованими або суперечливими;
- для підвищення точності прогнозів необхідна інтеграція професійних суджень експертів;
- у процесі управління ризиками виникає невизначеність, що унеможливлює ефективне використання традиційних підходів до оцінювання загроз і стану кіберзахисту об'єктів критичної інфраструктури держави;
- класичні моделі оцінювання зосереджені на вузьких технічних аспектах і не враховують синергетичну природу гібридних впливів;
- неоднорідність гібридних загроз ускладнює інтегрування їх у єдину модель;
- через недостатнє розуміння гібридного контексту інформаційно-психологічні, соціальні, фізичні загрози, які є частиною гібридного впливу, залишаються поза межами оцінки;
- суб'єкти, що здійснюють шкідливі впливи, дедалі частіше використовують інноваційні технології та штучний інтелект;
- є брак кваліфікованих фахівців (нестача кіберекспертів із глибоким розумінням загроз штучного інтелекту й технічних та нормативних аспектів).

Шляхи вирішення цих проблем і, відповідно, основні напрями наукових досліджень у цій галузі пов'язані з оцінюванням таких чинників:

- ризики втрати інформаційних ресурсів;
- стан кіберзахисту об'єктів критичної інфраструктури;
- рівень гібридних загроз у секторі цивільної безпеки держави;
- можлива шкода національній безпеці України в разі витоку державної таємниці;
- відповідність оцінювання шкоди європейському регламенту GDPR щодо захисту персональних даних.

Як свідчить досвід, застосування теорії нечітких множин забезпечує побудову методів та моделей оцінювання в слабоформалізованому нечітко визначеному довкіллі в умовах складних загроз. Подібні дослідження вже проводили в таких сферах, як енергетика, транспорт, цивільна оборона, фінансовий сектор, військова інфраструктура, авіація, інформаційно-комунікаційна інфраструктура, промислова автоматизація, хімічна промисловість, освітній сектор тощо. Однак усі ці дослідження переважно були пов'язані з конкретними системами: інфраструктурою управління підприємствами, розподіленими сенсорними мережами, системами електронного урядування, освітніми мережами, кіберфізичними системами з відкритим доступом, системами цивільної авіації, системами у банківській сфері, системами кіберзахисту об'єктів ЗСУ, промисловими контролерами, автоматизованими системами управління інфраструктурою метрополітену та ін., які функціонують на нижніх рівнях ієрархії в системі оцінювання стану кіберзахисту і не придатні для реалізації завдань на глобальному рівні.

Науковці Державного університету інформаційно-комунікаційних технологій у межах наукової школи «Кібербезпека» розробили концепцію і заклали теоретичне підґрунтя для побудови систем оцінювання. Зокрема, було отримано такі результати:

- розроблено узагальнені формальні моделі параметрів та системи характеристик даних підмножин групи чинників та показників;
- запропоновано методи оцінювання ризиків безпеки ресурсів інформаційних систем;
- запропоновано методи оцінювання шкоди від втрати інформаційних ресурсів з обмеженим доступом;
- розроблено методи оцінювання стану кіберзахисту об'єктів критичної інфраструктури держави;
- запропоновано метод оцінювання ризиків гібридних загроз у секторі цивільної безпеки;
- розроблено структурно-параметричну модель системи оцінювання шкоди від втрат персональних даних згідно з регламентом GDPR;
- запропоновано структурні моделі систем оцінювання ризику та стану кіберзахисту об'єктів критичної інфраструктури.

Крім того, в рамках розвитку теорії нечітких множин, яка є перспективним інструментом для оброблення суб'єктивних і нечітких даних, отримано такі результати:

- розроблено методи реалізації м'яких обчислень;
- створено базові методи варіювання порядку лінгвістичних змінних;
- запропоновано базові аналітичні вирази верифікації трансформованих лінгвістичних змінних;
- розроблено методи фазифікації інтервалів.

За результатами цих робіт було опубліковано сім монографій.

Отже, на основі теоретико-множинного та логіко-лінгвістичного підходу розроблено узагальнені формальні моделі параметрів та системи характеристик даних, запропоновано методи і моделі оцінювання ризиків безпеки ресурсів інформаційних систем та оцінювання ризиків гібридних загроз у сфері цивільної безпеки, а також оцінювання рівня кіберзахисту та рівня підвищення стану кіберзахисту об'єктів критичної інфраструктури держави.

Завдяки запропонованому методологічному підходу на підставі суджень експерта можна оцінювати стан захищеності об'єктів критичної інфраструктури, який має важливе значення не лише для підвищення ефективності управління ризиками, а й для забезпечення стабільності функціонування суспільних та критичних систем, зниження їхньої вразливості до гібридних загроз та оптимального розподілу ресурсів з огляду на сучасні виклики безпеки.

На особливу увагу заслуговує запропонована система оцінювання ризиків у режимі реального часу, система оцінювання рівня кіберзахисту, а також система оцінювання рівня підвищення стану кіберзахисту об'єктів критичної інфраструктури. Ці системи ґрунтуються на використанні експертних та CVSS-оцінок, процедурах фазифікації даних, математичних методах аналізу ризиків і дають змогу проводити порівняльне оцінювання стану захищеності різних об'єктів.

Практична реалізація моделей оцінювання, в тому числі програмна візуалізація результатів, має перспективи в контексті впровадження цих розробок у державні та відомчі системи управління кібербезпекою. Отримані результати використано в системі Держспецзв'язку та МВС України.

З урахуванням нинішньої складної безпекової ситуації в країні, пов'язаної з бойовими діями, розроблені моделі оцінювання можуть становити підґрунтя для гарантування кібербезпеки та забезпечення сталого розвитку України.

Дякую за увагу!

За матеріалами засідання
підготувала О.О. Мележик

Oleksandr G. Korchenko
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: https://orcid.org/0000-0003-3376-0631

METHODS AND MODELS FOR ASSESSING THE STATE OF CYBER DEFENSE OF CRITICAL INFRASTRUCTURE FACILITIES OF THE STATE

Transcript of scientific report at the meeting of the Presidium of NAS of Ukraine, June 18, 2025

The report emphasizes that the development and implementation of effective tools and systems for assessing the state of cyber security of critical infrastructure facilities of the state and the level of hybrid threats is a relevant scientific task. The theoretical and practical results obtained at the State University of Information and Communication Technologies are considered. These are aimed at creating new, flexible and adaptive methods for protecting critical infrastructure facilities and developing effective cyber threat assessment systems.

Cite this article: Korchenko O.G. Methods and models for assessing the state of cyber defense of critical infrastructure facilities of the state (transcript of scientific report at the meeting of the Presidium of NAS of Ukraine, June 18, 2025). *Visn. Nac. Akad. Nauk Ukr*. 2025. (8): 59—62. https://doi.org/10.15407/visn2025.08.059