DOI: 10.18372/2310-5461.68.20768
УДК: 004.056:004.89:351.86

С. В. Казмірчук**,** д-р техн. наук, професор
Державний університет інформаційно-комунікаційних технологій
orcid.org/0000-0001-6083-251
e-mail: s.kazmirchuk@duikt.edu.ua

В. П. Шульга, д-р іст. наук, професор
Державний університет інформаційно-комунікаційних технологій
orcid.org/0000-0003-4356-7288
e-mail: v.shulha@duikt.edu.ua

СИСТЕМА ОЦІНЮВАННЯ КІБЕРБЕЗПЕКОВОГО СТАНУ НА ІНДИКАТОРАХ КІБЕРДИПЛОМАТІЇ

Вступ

У сучасних умовах глобальної цифровізації, інтенсифікації гібридних загроз та трансформації кіберпростору на повноцінний вимір міждержавного протиборства проблема оцінювання рівня кібербезпеки держави виходить за межі суто технічного або інфраструктурного підходу. Для держав, що перебувають у стані воєнної агресії та постійного зовнішнього кібертиску, зокрема України, кібербезпека набуває системного, стратегічного та зовнішньополітичного виміру, тісно пов'язаного з реалізацією стратегії кібердипломатії.

Проведений у попередніх дослідженнях [1] аналіз міжнародних індексів і моделей оцінювання кібербезпеки (Global Cybersecurity Index, National Cyber Security Index, NIS2 Directive, OECD Digital Security Risk Management Framework, Cybersecurity Capacity Maturity Model) показав, що наявні підходи орієнтовані переважно на фіксацію формальної наявності політик, інституцій або технічних спроможностей, але не забезпечують комплексного оцінювання реального стану кіберзахищеності держави з урахуванням воєнного контексту, динаміки загроз та міжнародного виміру. Більшість моделей мають жорстку структуру, обмежену гнучкість і не дозволяють інтегрувати експертні оцінки в умовах невизначеності та неповноти інформації.

Разом з тим, у роботі [1], присвячених формуванню системи критеріїв оцінювання кіберзахищеності України в аспекті кібердипломатії, було обґрунтовано доцільність переходу від вузькоспеціалізованих індикаторів до інтегрованої багатовимірної системи критеріїв, що охоплює правові, інституційні, технічні, інформаційні, інноваційні та зовнішньополітичні аспекти. Також, запропонована система з 11 критеріїв дозволяє структуровано описати складність кібербезпекових процесів і відобразити специфіку реалізації стратегії кібердипломатії України.

Аналіз методів оцінювання ризиків і стану кібербезпеки, заснованих на класичних кількісних моделях, показує їхню обмежену придатність для державного рівня, особливо в умовах гібридної війни. Натомість використання апарату нечітких множин і мультикритеріального аналізу, обґрунтоване в роботах з методології оцінювання складних систем, створює передумови для побудови адаптивного методу, здатного інтегрувати різнорідні критерії та експертні знання.

Таким чином, постає актуальна науково-прикладна задача розроблення цілісної системи на підставі методу оцінювання рівня кіберзахищеності держави [2], яка базується на інтегрованій системі критеріїв кібердипломатії та реалізується за допомогою мультикритеріального нечіткого підходу з можливістю експериментального моделювання різних рівнів кібербезпекового стану. Розв'язання цієї задачі є необхідною умовою підвищення обґрунтованості державної кіберполітики, ефективності міжнародної взаємодії та стійкості України до сучасних кіберзагроз.

Аналіз останніх досліджень і публікацій

Оцінювання кібербезпеки та кіберзахищеності держави у сучасних наукових і прикладних дослідженнях реалізується переважно в межах трьох основних підходів: індексного (рейтингового), зрілості та спроможностей (capacity/maturity models) і ризик-орієнтованого (risk management). Кожен із цих підходів вирішує окремі аспекти задачі, однак не забезпечує формування універсальної адаптивної системи інтегрального оцінювання, здатної працювати в умовах гібридних загроз, невизначеності та необхідності урахування кібердипломатичного виміру.

Індексні системи оцінювання кібербезпеки держав.

Найбільш відомою міжнародною індексною системою є Global Cybersecurity Index (GCI), розроблений Міжнародним союзом електрозв'язку (ITU), який використовується для порівняльної оцінки рівня кібербезпеки держав за п'ятьма узагальненими напрямами: правовим, технічним, організаційним, розвитком потенціалу та міжнародним співробітництвом [3]. Перевагою GCI є можливість глобального порівняння країн і формування узагальнених рейтингів, однак індексна природа цього інструменту обмежує його придатність для побудови внутрішніх моделей оцінювання, орієнтованих на аналіз сценаріїв і підтримку управлінських рішень.

Подібний підхід реалізовано у National Cyber Security Index (NCSI), розробленому e-Governance Academy (Естонія), який оцінює готовність держав до запобігання кіберзагрозам та управління інцидентами на основі доказової бази та структурованих індикаторів [4]. Разом із тим, NCSI також має переважно описово-рейтинговий характер і не передбачає використання математичного апарату для інтеграції нечітких експертних оцінок.

Моделі спроможностей і зрілості національної кібербезпеки.

Окрему групу досліджень становлять моделі кіберспроможностей і зрілості, серед яких найбільш поширеною є Cybersecurity Capacity Maturity Model for Nations (CMM), розроблена Global Cyber Security Capacity Centre Університету Оксфорда [5]. Модель CMM дозволяє оцінювати рівень розвитку національної кібербезпеки за кількома вимірами та визначати стадії зрілості, що є корисним для стратегічного планування. Водночас CMM застосовується переважно як експертно-аналітичний інструмент і не містить формалізованої процедури розрахунку інтегрального чисельного показника, що ускладнює проведення експериментального моделювання та порівняння альтернативних сценаріїв розвитку.

Нормативні та стандартні підходи до управління кіберризиками.

Значний внесок у формування практик кібербезпеки на державному та організаційному рівнях зробили нормативні та стандартні документи. Зокрема, Директива ЄС NIS2 (Directive (EU) 2022/2555) встановлює обов'язкові вимоги до управління кіберризиками та реагування на інциденти для критичних і важливих секторів [6]. Деталізацію механізмів імплементації NIS2 надають методичні рекомендації ENISA [7]. На організаційному рівні широке застосування мають NIST Cybersecurity Framework (CSF) версії 2.0 [8] та NIST SP 800-30 Rev.1 [9], які формують підґрунтя для ідентифікації, аналізу та управління кіберризиками. Макрорівневі принципи управління цифровими ризиками викладені також у рекомендаціях OECD [10]. Разом із тим, зазначені документи орієнтовані переважно на регуляторні та практичні аспекти управління ризиками і не забезпечують побудови інтегральної системи оцінювання кібербезпеки держави з урахуванням лінгвістичних і експертних оцінок.

Наукові підходи та авторські системи оцінювання.

У наукових працях з кібербезпеки дедалі більше уваги приділяється геополітичному та кібердипломатичному виміру. Зокрема, у роботах J. Nye обґрунтовано роль кіберпростору у стримуванні та міжнародній безпеці [11], а в сучасних дослідженнях аналізується участь державних і недержавних акторів у кіберконфліктах [12]. Проте ці підходи мають переважно концептуальний характер і не містять формалізованих інструментів оцінювання.

У вітчизняних дослідженнях запропоновано низку авторських підходів до формування систем критеріїв оцінювання кіберзахищеності України, зокрема в аспекті кібердипломатії [1]. Подальший розвиток цього напряму здійснено у працях, присвячених методу мультикритеріального нечіткого оцінювання та системі оцінювання ризиків інформаційної безпеки, де реалізовано структурні моделі, алгоритми та програмну підтримку процесу оцінювання [2].

Постановка завдання

Проведений аналіз показує, що наявні міжнародні індекси, моделі зрілості та нормативні рамки не забезпечують повноцінної реалізації інтегральної системи оцінювання кібербезпеки держави, адаптованої до умов гібридних загроз і потреб кібердипломатії. Це зумовлює необхідність розроблення авторської системи оцінювання, яка поєднує формалізовану систему критеріїв, мультикритеріальний нечіткий метод інтеграції показників та експериментальне моделювання різних рівнів кібербезпекового стану.

Метою дослідження є розроблення та експериментальне обґрунтування системи оцінювання рівня кібербезпеки держави, яка базується на формалізованій системі критеріїв (у тому числі з урахуванням кібердипломатичного аспекту) та

реалізує мультикритеріальний нечіткий метод інтегрального оцінювання, адаптований до умов невизначеності та гібридних кіберзагроз.

Для досягнення поставленої мети в роботі необхідно розв'язати такі основні задачі:

1) Проаналізувати існуючі міжнародні системи, індекси та нормативні підходи до оцінювання кібербезпеки держави (GCI, NCSI, CMM, NIS2, NIST, OECD) з метою виявлення їхніх переваг і обмежень у контексті побудови інтегральної системи оцінювання;

2) Розробити структурну модель системи оцінювання рівня кібербезпеки держави, що базується на нечіткій логіці;

3) Побудувати алгоритм функціонування системи оцінювання, який забезпечує послідовну обробку експертних даних, інтеграцію часткових оцінок та формування узагальненого показника рівня кібербезпеки;

4) Реалізувати програмний застосунок для автоматизації процесу оцінювання рівня кібербезпеки держави;

5) Здійснити експериментальне моделювання роботи системи для різних сценаріїв (низького, середнього та високого рівнів кібербезпеки) з метою перевірки чутливості методу до зміни вхідних параметрів.

Основна частина

В роботі [2] був запропонований метод мультикритеріального оцінювання кібербезпекового стану держави на стратегічних індикаторах кібердипломатії на основі теорії нечітких множин. На підставі цього методу пропонується структурна модель системи та її програмна реалізація, яка дозволить автоматизувати такий процес оцінювання при формуванні нових даних (результати експертного оцінювання, нові критерії тощо).

Структурна модель запропонованої системи (рис. 1) складається з двох базових компонент, що відображають підсистеми **введення та керування даними** (ПВКД) та **підсистеми оцінювання та обробки даних** (ПООД). Опишемо склад кожної з них. Вони побудовані на підставі зазначеного методу у відповідності з етапами 1–7 [2].

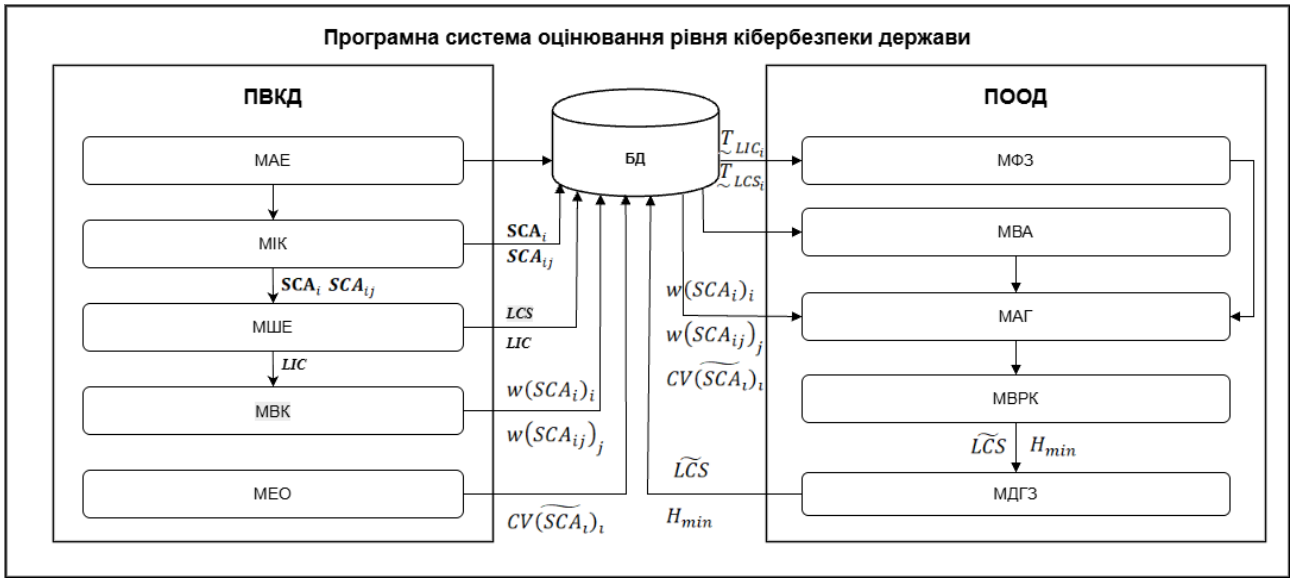

Рис. 1. Структурна модель системи оцінювання рівня кібербезпеки держави

Підсистема ПВКД забезпечує введення та збереження даних експертного оцінювання рівня реалізації підкритерію кожного критерію та налаштування і встановлення вагових коефіцієнтів для них. Вона складається з модуля автентифікації експертів (МАЕ), ініціалізації критеріїв та підкритеріїв (МІК), шкал і еталонів (МШЕ), вагових коефіцієнтів (МВК) та експертного оцінювання (МЕО).

Підсистема ПООД є базовою для оцінювання рівня кібербезпеки. Тут на підставі експертних оцінок, що надходять з ПВКД, після їх перетворення, формуються остаточні значення рівня кібербезпеки. Вона включає в себе модулі фазифікації (МФЗ) та вагового аналізу (МВА), агрегування (МАГ), визначення рівня кібербезпеки (МВРК), дефазифікації результатів і генерації звіту (МДГЗ).

База даних (БД) зберігає: критерії/підкритерії, шкали, еталони, оцінки експертів, ваги, результати отриманих рівнв, звіти/експорти (за потреби).

Розглянемо функціональне призначення кожного з зазначених модулів ПВКД і ПООД. Підсистема ПВКД забезпечує взаємодію експерта із системою та налаштування вхідних параметрів, необхідних для подальшого визначення рівня кібербезпеки. Модуль МАЕ призначений для реалізації процедури ідентифікації та аутентифікації експе-

рта в системі, який після успішної авторизації переходить до процесу визначення вагових коефіцієнтів в МВК відповідно до своєї зони відповідальності для кожного критерію та підкритерію. Також в МАЕ відбувається реєстрація експертів і авторизація адміністратора системи, який після успішної авторизації на перших етапах налаштування системи вносить, якщо вперше, критерії і відповідні підкритерії, а у разі необхідності здійснює їх редагування. Після адміністратор також формує необхідні шкали та еталони за допомогою МШЕ у відповідності із етапом 1 методу [2], а за необхідністю редагує чи створює нові. Після визначення вагових коефіцієнтів, експерт переходить до процесу визначення поточних значень індикаторів (підкритеріїв) у МЕО. Так, відповідно до етапу 4 методу [2] реалізується визначення поточного значення кожного індикатора в МЕО, які були попередньо збережені у базі даних. Тут на основі анкетування щодо значень кожного підкритерію відповідного критерію експерт відповідної предметної області обирає значення ВП – «ВІДСУТНЄ ПОВНІСТЮ», РЧ – «РЕАЛІЗОВАНО ЧАСТКОВО», РО – «РЕАЛІЗОВАНО З ОБМЕЖЕННЯМИ», РП – «РЕАЛІЗОВАНО ПОВНІСТЮ». Користувачі вводять інформацію через інтерфейс, після авторизації, що спрощує процес збору даних. Дані із МЕО надходять до бази даних для збереження отриманих оцінок у вигляді відповідних таблиць. Інтерфейсна частина забезпечує зручний доступ для експертів для введення їх оцінок.

Підсистема ПООД виконує основні операції з визначення значення рівня кібербезпеки та формування звітів. Дані, які були збережені у БД з МШЕ у МФЗ фазифікуються. З урахуванням вагових коефіцієнтів, які були збережені в БД з МВК, оцінки отримані з МЕО нормалізуються в МВА і далі формуються первинні дані для оцінювання рівні кібербезпеки згідно етапу 5 методу [2] в МАГ. Далі, в МВРК з МАГ надходять необхідні данні для остаточного формування значення рівня кібербезпеки. Далі, для порівняння отриманих НЧ скористаємось відповідно множиною узагальнених відстаней Хеммінга:

$$\bigcup_{s=1}^{m}\{H(s)\} = \left\{\bigcup_{s=1}^{m} h\left(\widetilde{LCS}, \underset{\sim}{T}_{LCS_s}\right)\right\} = \left\{\bigcup_{s=1}^{m}\sum_{p=1}^{4}\left|\widetilde{LCS}_p - \underset{\sim}{T}_{LCS_{sp}}\right|\right\},$$

де для $\widetilde{LCS}$ мінімальне значення H_{min} із всіх $\bigcup_{s=1}^{m}\{H(s)\}$ буде свідчити про найбільшу наближеність НЧ до еталонного [2] ($s = \overline{1,m}$, де m – кількість терм-множин), а отримані результати зберігаються у відповідних таблицях в базі даних. Для інтерпретації результатів в МДГЗ (етап 7 в [2]) за сформованими асоціативними правилами визначається поточне значення рівня і формується звіт у .xlsx форматі для зручності подальшого опрацювання отриманих даних. Звіт містить графічну і текстову інтерпретацію оціненого рівня кібербезпеки.

Запропонована структурна модель системи оцінки рівня кібербезпеки, наприклад, може бути реалізована програмно і функціонувати на основі запропонованого базового алгоритму (рис. 2).

Відповідно до цього алгоритму, робота системи починається з авторизації (при першому запуску ініціалізується процедура «Реєстрація»).

Після успішної авторизації (див. рис. 2 вершина 3) проводиться налаштування системи адміністратором, яка пов’язана із внесенням необхідних даних для подальшого оцінювання рівнів кібербезпеки. На цьому етапі відбувається реєстрація експертів, введення даних щодо критеріїв та підкритеріїв (реалізація вершини 2 на рис. 2). Усі введені дані зберігаються у базі даних у відповідних таблицях. Процес визначення вагових коефіцієнтів та визначення поточних значень індикаторів пов'язаний з роботою кожного експерта відповідної предметної області реалізується на своєму робочому місці, де здійснюється авторизація в системі. При успішній авторизації (вершина 3, рис. 2) відбувається ініціалізація списку підкритеріїв (див. рис. 2, вершина 4). Далі, експерт проводить оцінювання (див. рис. 2 вершини 5-7). Далі, здійснюється фазифікація еталонів і (з урахуванням отриманих вагових коефіцієнтів), нормування отриманих результатів та визначення рівня кібербезпеки (див. рис. 2 вершини 8-10). Всі результати зберігаються у БД, для зручності результати можна вивести у вигляді звіту. Інтерфейс програмної системи зображений на рис. 3.

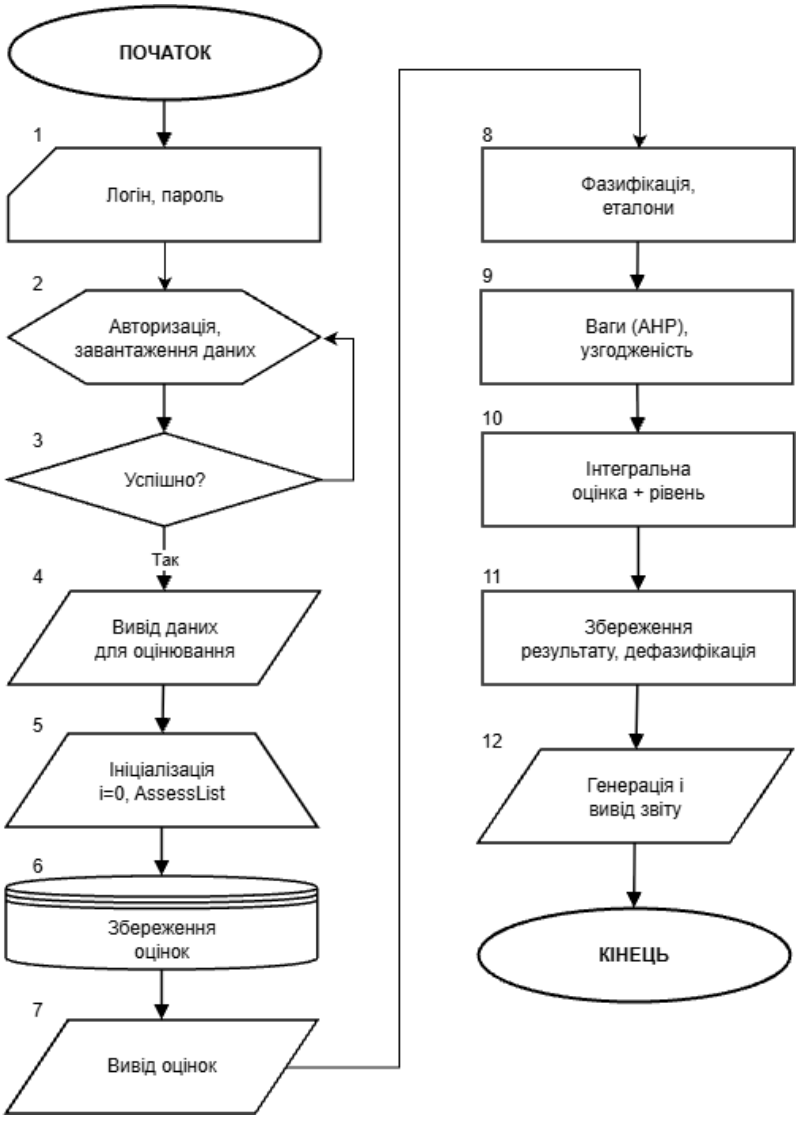

Рис. 2. Базовий алгоритм роботи системи оцінювання рівня кібербезпеки

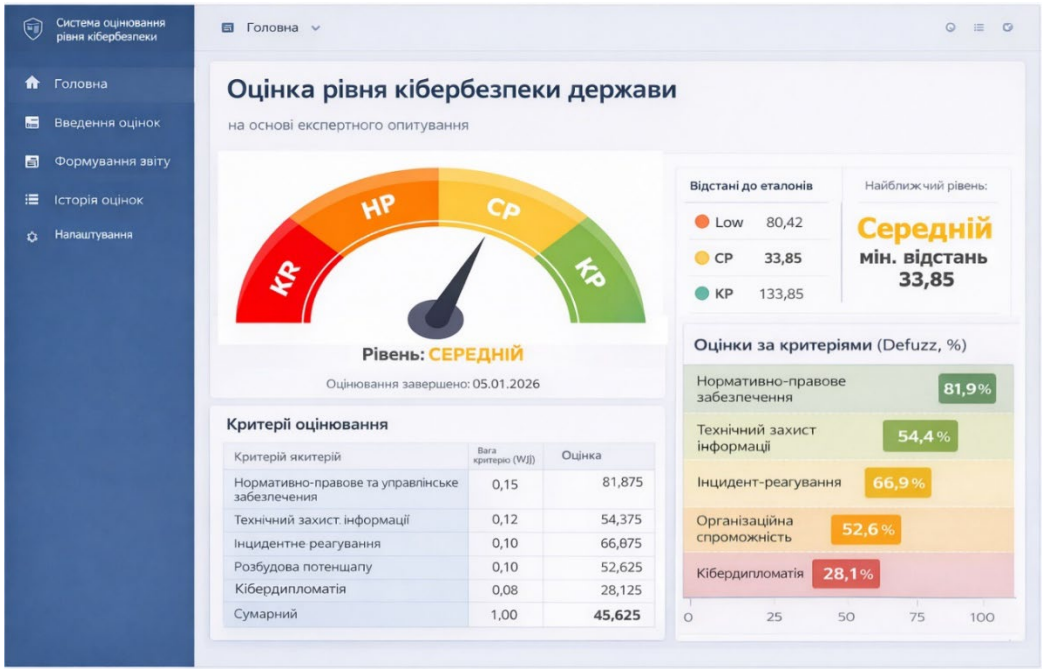

Рис. 3 Приклад інтерфейсу головного вікна прототипу системи оцінювання

Для експерименту було згенеровано низку сценаріїв, наприклад, коли експерти визначили поточні індикатори на рівнях РЧ та ВП тобто з низькі– S1_Низький, на рівнях РЧ та РО – S2_Середній та РП і РО – S3_Високий (див. табл. 1).

Таблиця 1

Оцінки за індикаторами

Код індикатора (підкритерію)	S1_Низький	S2_Середній	S3_Високий
1.1	РЧ	РО	РП
1.2	РЧ	РО	РП
1.3	РЧ	РЧ	РП
2.1	ВП	РО	РП
2.2	РЧ	РО	РО
2.3	РЧ	РЧ	РП
2.4	РЧ	РО	РП
2.5	ВП	РО	РП
3.1	РЧ	РЧ	РП
3.2	РЧ	РО	РО
3.3	РЧ	РО	РП
3.4	ВП	РЧ	РП
3.5	РЧ	РО	РП
4.1	РЧ	РО	РП
4.2	РЧ	РЧ	РО
4.3	ВП	РО	РП
4.4	РЧ	РО	РП
4.5	РЧ	РЧ	РП
5.1	РЧ	РО	РП
5.2	ВП	РО	РО
5.3	РЧ	РЧ	РП
5.4	РЧ	РО	РП
5.5	РЧ	РО	РП
6.1	ВП	РЧ	РП
6.2	РЧ	РО	РО
6.3	РЧ	РО	РП
6.4	РЧ	РЧ	РП
6.5	ВП	РО	РП
7.1	РЧ	РО	РП
7.2	РЧ	РЧ	РО
7.3	РЧ	РО	РП
7.4	ВП	РО	РП
7.5	РЧ	РЧ	РП
8.1	РЧ	РО	РП
8.2	РЧ	РО	РО
8.3	ВП	РЧ	РП
8.4	РЧ	РО	РП
8.5	РЧ	РО	РП
9.1	РЧ	РЧ	РП
9.2	ВП	РО	РО
9.3	РЧ	РО	РП
9.4	РЧ	РЧ	РП
10.1	РЧ	РО	РП
10.2	ВП	РО	РП
10.3	РЧ	РЧ	РО
10.4	РЧ	РО	РП
11.1	РЧ	РО	РП
11.2	ВП	РЧ	РП
11.3	РЧ	РО	РП
11.4	РЧ	РО	РО
11.5	РЧ	РЧ	РП

де ВП – «ВІДСУТНЄ ПОВНІСТЮ», РЧ – «РЕАЛІЗОВАНО ЧАСТКОВО», РО – «РЕАЛІЗОВАНО З ОБМЕЖЕННЯМИ», РП – «РЕАЛІЗОВАНО ПОВНІСТЮ».

Експериментальне моделювання для сценаріїв S1–S3 підтвердило коректність роботи алгоритму, що також проілюстровано на зазначеному прикладі: інтегральний показник монотонно зростає при переході від низьких до високих значень вхідних оцінок, а класифікація за відстанню Хемінга забезпечує однозначне віднесення до рівнів LOW / MEDIUM / HIGH (див. рис. 4). Отримані результати демонструють чутливість системи до зміни експертних параметрів і придатність запропонованого підходу для підтримки управлінських рішень. Таким чином було підтверджено адекватність її функціонування.

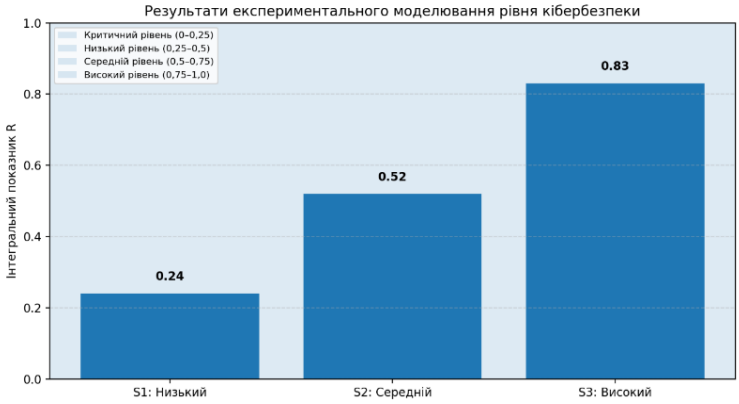

Рис. 4 Приклад експерименту за трьома сценаріями S1–S3

Висновки

Таким чином, розроблено структурну модель системи оцінювання рівня кібербезпеки держави, яка за рахунок компонент підсистем введення та керування даними і оцінювання та обробки даних, а також складових їх модулів авторизації експертів, ініціалізації критеріїв та підкритеріїв, шкал і еталонів, вагових коефіцієнтів, експертного оцінювання, фазифікації, вагового аналізу, агрегування, визначення рівня кібербезпеки і дефазифікації результатів та генерації звіту, в яких реалізовано запропонований метод [2], дозволила розробити алгоритм та відповідний програмний застосунок для автоматизації процесу оцінювання рівня кібербезпеки і на підставі стратегічних індикаторах кібердипломатії.

Також на основі запропонованої моделі розроблено базовий алгоритм і відповідне програмне забезпечення оцінювання у вигляді прикладної програмної системи – «СИСТЕМА ОЦІНЮВАННЯ РІВНЯ КІБЕРБЕЗПЕКИ ДЕРЖАВИ», яка безпосередньо дозволяє реалізовувати процес оцінювання рівня і надавати звіти для використання у загальній системі управління та подальшого прийняття рішення.

ЛІТЕРАТУРА

[1] Shulha, V. P., Korchenko, O. H., Ivanchenko, Ye. V., Kazmyrchuk, S. V., & Kondratiuk, S. V. (2025). Критерії стратегічного оцінювання кібербезпеки держави: кібердипломатичний аспект. *Сучасний захист інформації, 3*(63), С. 205–218.

[2] Шульга В., Корченко О., Казмірчук С., Корченко А., Аскеров М. (2025). Метод мультикритеріального оцінювання кібербезпекового стану держави на стратегічних індикаторах кібердипломатії. Information Technology: Computer Science, Software Engineering and Cyber Security, № 4 (2025). С. 10–39.

[3] Global Cybersecurity Index (GCI) 2024 : Global Report / Int'l Telecommunication Union. – Geneva : ITU, 2024. 112 c. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf. (access data 25.10.2025)

[4] National Cyber Security Index (NCSI), Methodology / e-Governance Academy. e-Governance Academy, 2025. URL: https://ncsi.ega.ee/methodology. (access data 25.10.2025)

[5] Cybersecurity Capacity Maturity Model for Nations (CMM) / Global Cyber Security Capacity Centre, Univ. of Oxford. Oxford : GCSCC, 2022. URL: https://gcscc.ox.ac.uk/the-cmm. (access data 25.10.2025)

[6] Directive (EU) 2022/2555 (NIS2) of the European Parliament and of the Council of 14 October 2022 on measures for a high common level of cybersecurity across the Union. Off. J. Eur. Union, L 277, 2022. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555. (access data 25.10.2025)

[7] Technical Guidelines for the implementation of NIS2 / European Union Agency for Cybersecurity (ENISA). Heraklion : ENISA, 2025. URL: https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance. (access data 25.10.2025)

[8] NIST Cybersecurity Framework (CSF) Version 2.0 / Nat'l Inst. of Standards and Technology. Gaithersburg : NIST, Feb. 2024. Режим доступу: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf. (access data 25.10.2025)

[9] Risk Management Guide for Information Technology Systems (SP 800-30 Rev.1) / Nat'l Inst. of Standards and Technology. Gaithersburg : NIST, Jul. 2012. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf. (access data 25.10.2025)

[10] OECD Recommendation on Digital Security Risk Management for Economic and Social Prosperity / OECD, 2015. URL: https://legalinstruments.oecd.org/public/doc/328/328.en.pdf. (access data 25.10.2025)

[11] Nye J.S. Jr. Deterrence and Dissuasion in Cyberspace. *International Security*. 2017. Vol. 41, № 3. С. 44–71.

[12] Bishop M., Bailey D., Dempsey K. et al. A taxonomy of cyber conflict: The role of states, nonstate actors, and networks. *Journal of Strategic Security*. 2020. Vol. 13, № 2. С. 5–17.

Казмірчук С. В., Шульга В. П.

СИСТЕМА ОЦІНЮВАННЯ КІБЕРБЕЗПЕКОВОГО СТАНУ НА ІНДИКАТОРАХ КІБЕРДИПЛОМАТІЇ

У статті розглянуто проблему формалізованого оцінювання рівня кібербезпеки держави в умовах зростання гібридних загроз, невизначеності вихідних даних та необхідності урахування не лише технічних, а й правових, організаційних та зовнішньополітичних аспектів. Показано, що наявні міжнародні індексні системи, моделі зрілості та нормативні підходи (GCI, NCSI, CMM, NIS2, NIST, OECD) не забезпечують побудови інтегральної адаптивної системи оцінювання, придатної для використання на державному рівні в умовах воєнного протистояння та динамічної трансформації кіберзагроз. Метою дослідження є розроблення та програмна реалізація системи оцінювання рівня кібербезпеки держави, що базується на формалізованій системі критеріїв, включно з кібердипломатичним виміром, та реалізує мультикритеріальний нечіткий метод інтеграції експертних оцінок.

Запропонована система дозволяє враховувати лінгвістичні оцінки експертів, різну вагомість критеріїв і підкритеріїв, а також працювати в умовах неповноти та нечіткості інформації. У роботі розроблено структурну модель системи оцінювання, яка складається з підсистем введення та керування даними і підсистеми оцінювання та обробки даних, а також відповідних функціональних модулів автентифікації, ініціалізації критеріїв і підкритеріїв, формування шкал і еталонів, визначення вагових коефіцієнтів, експертного оцінювання, фазифікації, агрегування, дефазифікації результатів і генерації звітів. Запропоновано базовий алгоритм функціонування системи, який забезпечує послідовну обробку експертних даних і формування інтегрального показника рівня кібербезпеки. Для перевірки коректності та чутливості методу проведено експериментальне моделювання роботи системи для трьох сценаріїв, що відповідають низькому, середньому та високому рівням кібербезпекового стану. Результати експерименту підтвердили монотонність зміни інтегрального показника при переході між сценаріями та однозначність класифікації рівнів на основі узагальненої відстані Хеммінга до еталонів. Розроблено прототип програмного застосунку системи оцінювання рівня кібербезпеки держави, який забезпечує автоматизацію процесу збору експертних оцінок, їх обробку та візуалізацію результатів у вигляді інтегрального рівня та оцінок за окремими критеріями. Запропонований підхід може бути використаний як інструмент підтримки прийняття управлінських рішень у сфері державної кіберполітики, стратегічного планування та міжнародної кібердипломатичної взаємодії.

Ключові слова: кібербезпека держави; оцінювання кібербезпекового стану; мультикритеріальний аналіз; нечітка логіка; експертне оцінювання; дефазифікація; кібердипломатія; інтегральний показник; програмна система.

Kazmirchuk S., Shulha V.

SYSTEM FOR ASSESSING THE CYBERSECURITY STATE BASED ON CYBERDIPLOMACY INDICATORS

The article addresses the problem of formalized assessment of a state's cybersecurity level under conditions of growing hybrid threats, uncertainty of initial data, and the need to account not only for technical, but also legal, organizational, and foreign-policy aspects. It is shown that existing international index systems, maturity models, and regulatory approaches (GCI, NCSI, CMM, NIS2, NIST, OECD) do not provide for the construction of an integrated adaptive assessment system suitable for use at the state level in conditions of military confrontation and dynamic transformation of cyber threats. The purpose of the study is to develop and implement in software a system for assessing the level of a state's cybersecurity, based on a formalized system of criteria, including a cyberdiplomacy dimension, and implementing a multicriteria fuzzy method for integrating expert assessments. The proposed system makes it possible to account for linguistic expert evaluations, different weights of criteria and sub-criteria, and to operate under conditions of incomplete and fuzzy information. The paper develops a structural model of the assessment system consisting of a data input and management subsystem and an assessment and data processing subsystem, as well as the corresponding functional modules for authentication, initialization of criteria and sub-criteria, formation of scales and reference benchmarks, determination of weighting coefficients, expert assessment, fuzzification, aggregation, defuzzification of results, and report generation. A basic algorithm for the system's operation is proposed, ensuring consistent processing of expert data and the formation of an integral indicator of the cybersecurity level. To verify the correctness and sensitivity of the method, experimental modeling of the system's operation was conducted for three scenarios corresponding to low, medium, and high levels of the cybersecurity state. The experimental results confirmed the monotonic behavior of the integral indicator when transitioning between scenarios and the unambiguous classification of levels based on the generalized Hamming distance to reference benchmarks. A prototype software application of the state cybersecurity assessment system was developed, providing automation of the collection of expert assessments, their processing, and visualization of results in the form of an integral level and criterion-based evaluations. The proposed approach can be used as a decision-support tool in the field of state cyber policy, strategic planning, and international cyberdiplomatic cooperation.

Keywords: state cybersecurity; cybersecurity state assessment; multicriteria analysis; fuzzy logic; expert assessment; defuzzification; cyberdiplomacy; integral indicator; software system.

Стаття надійшла до редакції 27.11.2025 р.
Прийнято до друку 10.12.2025 р.