КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (29), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.29.943
УДК 004.056.5

Юдіна Діана Олексіївна
аспірант факультету комп'ютерних наук та технологій
Державний університет «Київський авіаційний інститут», Київ, Україна
ORCID ID: 0000-0002-1277-8771
diana.yudina22@gmail.com

МОДИФІКАЦІЯ МОДЕЛІ РОЗРАХУНКУ РІВНЯ КІБЕРЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Анотація. Зростаюча інтенсивність кіберзагроз та кібератак, особливо з боку російської федерації, створює безпрецедентну небезпеку для об'єктів критичної інфраструктури та об'єктів критичної інформаційної інфраструктури. Наслідки таких інцидентів можуть мати катастрофічний характер, спричиняючи масштабні економічні збитки, соціальну дестабілізацію та пряму загрозу життю. Таке зростання кількості кібератак вимагає безперервного вдосконалення підходів до забезпечення кібербезпеки та об'єктивної оцінки рівня їх захисту. З огляду на цю потребу, було розроблено модель розрахунку рівня кіберзахисту. В ході апробації моделі виявлено певні недоліки, зокрема недостатність систем критеріїв та неоднозначність інтегрального показника, що обмежувало її релевантність і точність особливо в контексті динамічних змін в українському законодавстві. Це призвело до здійснення модифікації моделі шляхом розширення кількості систем критеріїв та їхніх показників відповідно до актуальних національних нормативно-правових актів, а також специфічних особливостей кожного сектору критичної інфраструктури. Ключовою зміною є розширення набору критеріїв для оцінювання кіберзахисту. До шести обов'язкових груп заходів (Управління, Ідентифікація, Захист, Виявлення, Реагування, Відновлення) додано нову, сьому систему критеріїв — «Секторальна складова». Ця система дозволяє інтегрувати галузеві (секторальні) особливості різних секторів критичної інфраструктури. Модифікована модель має ієрархічну структуру та представляє результат у вигляді єдиного інтегрального кількісного показника, інтерпретованого за п'ятирівневою відсотковою шкалою, що узгоджується з міжнародними моделями зрілості, дає можливість об'єктивно оцінити рівень зрілості кіберзахисту об'єктів критичної інформаційної інфраструктури та розробити цілеспрямовані стратегії для його підвищення.

Ключові слова: кіберзахист; критична інфраструктура; об'єкти критичної інфраструктури; об'єкти критичної інформаційної інфраструктури; модель оцінювання; система критеріїв.

ВСТУП

Одним з основних чинників, що створює безпрецедентну небезпеку об'єктам критичної інфраструктури (ОКІ) та об'єктам критичної інформаційної інфраструктури (ОКІІ) України та світу в цілому, є зростаюча інтенсивність кіберзагроз та кібератак [1]–[3]. В умовах сучасних геополітичних реалій, зокрема повномасштабної агресії, російська федерація послідовно залишається одним з основних джерел загроз національній та міжнародній кібербезпеці. Ця держава-агресор активно реалізує концепцію інформаційного протиборства, що ґрунтується на поєднанні деструктивних дій у кіберпросторі та інформаційно-психологічних операцій, механізми якої широко та безперервно застосовуються у війні проти України.

Така деструктивна активність створює реальну загрозу вчинення актів кібертероризму та кібердиверсій, спрямованих на виведення з ладу або порушення стабільного функціонування ОКІ [4]. Наслідки подібних інцидентів можуть мати

катастрофічний характер, призводячи до масштабних економічних збитків, соціальної дестабілізації та безпосередньої загрози життю та здоров'ю населення. У зв'язку з цим, забезпечення надійного кіберзахисту ОКІ та ОКІІ набуває статусу пріоритетного завдання державної політики та є критично важливим для національної безпеки та стійкості держави [4].

Постановка проблеми. Сучасні геополітичні реалії, зокрема повномасштабна військова агресія, призвели до критичного зростання кіберзагроз, що становлять серйозну небезпеку для ОКІ України. Забезпечення їхньої стійкості є пріоритетом для національної безпеки. Проте, ефективне управління кібербезпекою неможливе без постійного моніторингу та точного оцінювання її поточного стану. Хоча існує низка міжнародних та національних стандартів і методик для оцінки рівня кіберзахисту, вони часто не повною мірою враховують специфіку та масштаби сучасних загроз, а також динамічні зміни в законодавстві України.

Відсутність універсального, але водночас достатньо деталізованого та адаптованого під українські реалії інструменту для оцінювання рівня кіберзахисту ОКІ істотно ускладнює розробку цілеспрямованих стратегій захисту та пріоритезацію заходів, що є критично важливим для забезпечення стійкості держави в умовах безперервної гібридної війни.

Зазначені обставини підкреслюють необхідність постійного моніторингу та об'єктивного оцінювання рівня кіберзахисту ОКІІ. Удосконалення існуючих методик та розробка адаптивних інструментів для такого оцінювання мають ключове значення для формування ефективних стратегій захисту. У даній статті здійснено модифікацію моделі розрахунку рівня кіберзахисту ОКІ.

Аналіз останніх досліджень і публікацій. Існує багато підходів до розрахунку рівня кіберзахисту. З цією метою використовують міжнародні стандарти, фреймворки та моделі оцінювання зрілості кібербезпеки (ISO/IEC 27001:2022 [5], NIST Cybersecurity Framework version 2.0 (NIST CSF 2.0) [6], Capability Maturity Model Integration (CMMI) [7], Cybersecurity Capability Maturity Model (C2M2) [8], Smart Grid Maturity Model (SGMM) [9], CISA Cybersecurity Performance Goals (CPGs) [10] тощо).

В українському законодавстві також є визначені підходи до розрахунку стану кіберзахисту (Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури, затверджені постановою Кабінету Міністрів України від 19.06.2019 № 518 (ПКМУ № 518) [11], Методичні рекомендації щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури, затверджені наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 06.10.2021 № 601 (наказ АД № 601) [12], Базові заходи з кіберзахисту, затверджені наказом Адміністрації Держспецзв'язку від 30.01.2025 № 54 (наказ АД № 54) [13], Методика оцінювання стану кібербезпеки електричних мереж та практик кібербезпеки електричних мереж, затверджена наказом Міністерства енергетики України від 05.08.2024 № 285 (наказ МЕ № 285) [14]).

Провівши детальний аналіз кожного з перелічених документів виявлено наступне.

Вимоги ПКМУ № 518 [11] відповідають більшості вимог ДСТУ ISO/IEC 27001:2023 «Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги», що був прийнятий на основі [5] та окреслюють основні вимоги, що мають бути виконані оператором критичної інфраструктури, проте не надають практичних рекомендацій щодо виконання таких вимог [15]. В ПКМУ № 518 також акцентується увага на необхідності створення

комплексної системи захисту інформації або системи управління інформаційною безпекою з підтвердженою відповідністю [16].

Враховуючи, що наказ АД № 54 [13], було розроблено з урахуванням NIST CSF 2.0 [6], то вони, в переважній більшості, відповідають один одному. В обох документах визначено 106 заходів кіберзахисту, що згруповані у шість функцій (управління, ідентифікація, забезпечення захисту, виявлення, реагування та відновлення), які діляться на категорії та підкатегорії.

CPGs [10] є загальним набором засобів захисту, що організовані відповідно до NIST Cybersecurity Framework version 1.1 [17]. Найбільш зручним в застосуванні [10] є запропоновані чек-лист та матриця з додатковою інформацію та референційними посиланнями. CPGs [10] має 38 цілей, що згруповані у 5 великих цілей, а також рекомендовані дії для виконання тієї чи іншої цілі [16].

Наказ АД № 601 [12], розроблено з урахуванням NIST Cybersecurity Framework version 1.1 [17]. Вони базуються на нормативних документах, національних та міжнародних стандартах, усталеній практиці захисту інформації та забезпечення кібербезпеки, що розвиваються разом з технологіями забезпечення кібербезпеки. В наказі АД № 601 [12] визначено 108 заходів кіберзахисту, що згруповані у п’ять класів заходів кіберзахисту — Ідентифікація ризиків кібербезпеки, Кіберзахист, Виявлення кіберінцидентів, Реагування на кіберінциденти та Відновлення стану кібербезпеки [16].

Наказ МЕ № 285 [14] було розроблено з урахуванням C2M2 [8]. Він визначає модель зрілості спроможностей кібербезпеки електричних мереж для оцінки та вдосконалення програм з кібербезпеки електричних мереж та зміцнення їх експлуатаційної стійкості, проте може бути використаний для інших секторів критичної інфраструктури. Методика наказу МЕ № 285 та модель C2M2, [14], [8] включають 356 практик, які класифіковані в 10 областей.

SGMM [9] має 8 доменів, описаних шістьома рівнями зрілості (від 0 до 5). Для кожної комбінації домену/рівня зрілості описано понад 200 характеристик, проте наявні ключові 180 показників (індикаторів), які представлені у вигляді запитань для самооцінювання [18], [19].

CMMI [7] має 5 рівнів зрілості (від 1 до 5) і складається з таких ключових елементів: процесні області (групи пов’язаних процесів, 22 області), цілі (обов’язкові результати, яких слід досягти в кожній процесній області), практики (дії, які виконуються для досягнення цілей), представлення (модель може бути представлена в поетапному (staged) або неперервному (continuous) форматі).

Водночас, зараз в Україні на законодавчому рівні визначено обов’язковість використання усіма силами кіберзахисту (в тому числі і операторами критичної інфраструктури) базових заходів з кіберзахисту. Відповідно до постанови Кабінету Міністрів України від 29.12.2021 № 1426 [20] базовими заходами з кіберзахисту є заходи з управління, ідентифікації, забезпечення захисту, виявлення, реагування та відновлення.

Таким чином, при оцінюванні стану кіберзахисту ОКІ мають бути використані саме ці шість груп заходів. Проте, немає визначеної вимоги щодо обмеження кількості таких груп.

У табл. 1 систематизовано результати проведеного аналізу розповсюджених існуючих вимог та рекомендацій щодо розрахунку рівня кіберзахисту критичної інфраструктури за такими критеріями:

Дескриптивність (ДС) — описовий характер без встановлення конкретних вимог або норм; гнучкість (ГН) — здатність адаптувати або змінювати правила, вимоги чи рекомендації відповідно до конкретних умов, ситуацій або потреб; можливість інтеграції

з іншими стандартами та настановами (ІН); простота реалізації у співвідношенні затребуваного часу та кількості ресурсів для виконання конкретних вимог (ПР); юрисдикційна релевантність (ЮР) — ступінь відповідності документа чинному законодавству України (зокрема вимогам постанови Кабінету Міністрів України від 29.12.2021 № 1426), національній термінології, структурі органів управління та контексту критичної інформаційної інфраструктури; контекстуальна релевантність (КР) — ступінь відповідності документа контексту діяльності ОКІ, відображає наскільки документ вписується в реальні умови, операційні потреби та специфічні ризики конкретного ОКІІ.

Таблиця 1

Порівняльний аналіз вимог та рекомендацій щодо підвищення рівня кіберзахисту ОКІ

Вимоги / рекомендації з підвищення рівня кіберзахисту	ДС	ГН	ІН	ПР	ЮР	КР
ISO/IEC 27001:2022	-	+	+	-	-	-
NIST CSF 2.0	+	+	+	+	-	-
C2M2	+	+	+	+	-	-
SGMM	+	+	+	+	-	-
CPGs	+	+	+	+	-	-
CMMI	+	-	+	-	-	-
ПКМУ № 518	-	-	-	-	-	-
Наказ АД № 601	+	+	+	-	-	-
Наказ АД № 54	+	+	+	+	+	-
Наказ МЕ № 285	+	+	+	+	-	-

Таким чином, з табл. 1 видно, що найбільш придатним за усіма критеріями є наказ АД № 54 [13], оскільки він повністю відповідає вимогам чинного законодавства України, надає чіткі та зрозумілі механізми для оцінювання стану кіберзахисту, а також передбачає можливість інтеграції з іншими стандартами або настановами. Однак такий наказ має універсальний характер та не враховує специфічні особливості функціонування ОКІ різних секторів критичної інфраструктури.

У роботі [16] запропоновано модель розрахунку рівня кіберзахисту ОКІ, яка за рахунок введення базової множини системи критеріїв та відповідних критеріїв дає можливість розрахувати рівень кіберзахисту ОКІ.

Основні результати реалізації запропонованої моделі формуються у вигляді єдиного інтегрального кількісного показника, який синтезує всі враховані критерії.

Слід зазначити, що при визначенні кількісного показника рівня кіберзахисту були визначені такі недоліки:

– обмеженість критеріїв: кількість систем критеріїв, які охоплюють групи заходів із кіберзахисту *SC*, є недостатньою;
– відсутність комплексного підходу: існуюча кількість критеріїв кожної групи заходів із кіберзахисту *SCi* не охоплює весь спектр заходів кіберзахисту, що перешкоджає якісному обрахунку рівня кіберзахисту.

Отже, є необхідність модифікувати розроблену модель розрахунку рівня кіберзахисту ОКІІ, шляхом розширення кількості систем критеріїв, які охоплюють групи заходів із кіберзахисту, та кількості критеріїв кожної групи заходів із кіберзахисту.

Таким чином, основні результати моделі будуть представлені у вигляді єдиного інтегрального кількісного показника, який синтезує всі враховані критерії. Показник

відображатиме поточний рівень кіберзахисту ОКІІ та інтерпретуватиметься за розробленою автором п'ятирівневою шкалою в діапазоні від 0 до 1 (табл. 2). Назви рівнів стану кіберзахисту відповідають загальноприйнятим градаціям, таким як [6] та [7]. Запропоновані діапазони забезпечують достатню диференціацію для об'єктивного оцінювання.

Таблиця 2

Шкала інтерпретації результатів поточного рівня кіберзахисту ОКІІ

Рівні шкали	Діапазон отриманого показника
Початковий / неприйнятний (критичний) рівень	0 – 0,2
В процесі формування / низький рівень	0,21 – 0,45
Визначений / середній рівень	0,46 – 0,7
Керований / високий рівень	0,71 - 0,89
Оптимізований / відмінний рівень	0,9 - 1

Інтерпретований інтегральний показник поточного рівня кіберзахисту дозволить здійснити об'єктивну оцінку стану ОКІІ та визначити відхилення від «оптимізованого» рівня. Ця інформація є основою для розроблення та імплементації ефективних стратегій і заходів, спрямованих на підвищення рівня кіберзахисту.

Отже, **метою роботи** є модифікація раніше розробленої моделі розрахунку рівня кіберзахисту ОКІІ.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Оскільки Законом України від 27.03.2025 № 4336-IX [21] було внесено значні зміни в українське законодавство, що стосується кіберзахисту ОКІ та ОКІІ (а саме внесено зміни в статтю 6 Закону України «Про основні засади забезпечення кібербезпеки України», встановивши вимоги до оцінювання стану кіберзахисту ОКІ та ОКІІ) модель розрахунку рівня кіберзахисту ОКІ, розроблена в [16], потребує значних змін і перегляду для забезпечення її актуальності. Необхідно переглянути модель, в частині, що стосується кількості критеріїв для розрахунку рівня кіберзахисту (Етап 1 та Етап 2 моделі, розробленої в [16]).

Етап 1 — Визначення множини систем критеріїв (*SC*)

З метою врахування специфічних галузевих вимог до кіберзахисту ОКІ пропонується додати одну систему критеріїв: $SC_1 = SE =$ *«Секторальна складова»*.

Також, пропонується визначити шість систем критеріїв, відповідно до пункту 6 постанови Кабінету Міністрів України від 29 грудня 2021 року № 1426 [20], а саме: $SC_2 = GV =$ *«Управління»*, $SC_3 = ID =$ *«Ідентифікація ризиків кібербезпеки»*, $SC_4 = PR =$ *«Кіберзахист»*, $SC_5 = DE =$ *«Виявлення кіберінцидентів»*, $SC_6 = RS =$ *«Реагування на кіберінциденти»*, $SC_7 = RC =$ *«Відновлення стану кібербезпеки»*.

Таким чином, при n = 7 (6 обов'язкових систем критеріїв та 1 специфічна галузева система критеріїв) з урахуванням (1) в [16] визначимо повну множину систем критеріїв (*SC*):

$$SC = \{\cup_{i=1}^{n} SC_i\} = \{SC_1, SC_2, SC_3, SC_4, SC_5, SC_6, SC_7\} = \{SE, GV, ID, PR, DE, RS, RC\}, \quad (1)$$

Етап 2 — Визначення підмножини критеріїв кожної системи критеріїв (SC_i).

Кожна з семи систем критеріїв містить певну кількість деталізованих критеріїв. Ці критерії сформовані у відповідності до наказу АД № 54 [13]. Наприклад, система критеріїв Управління (GV) включає 31 критерій, Ідентифікація ризиків кібербезпеки

(ID) — 21, Кіберзахист (PR) — 22, Виявлення кіберінцидентів (DE) — 11, Реагування на кіберінциденти (RS) — 13 та Відновлення стану кібербезпеки (RC) — 8.

Таким чином для множин критеріїв $SC_2, SC_3, SC_4, SC_5, SC_6$ та SC_7, при n = 2, k_2 = 31; n = 3, k_3 = 21; n = 4, k_4 = 22; n = 5, k_5 = 11; n = 6, k_6 = 13 та n = 7, k_7 = 8 відповідно, з використанням (2) в [16], представимо множини систем критеріїв (табл. 3).

Система критеріїв Секторальна складова (SE) є індивідуальною для кожного сектора критичної інфраструктури і складається з різної кількості критеріїв (табл. 4 та рис. 1).

Таблиця 3

Представлення системи критеріїв

Система критеріїв	Назва системи критеріїв	Значення k_i	Показники критеріїв	Критерії
SC_2	GV = «Управління»	k_2 = 31	$SC_{2.1}, SC_{2.2}, \dots, SC_{2.31}$	GV.OC-01, GV.OC-02, GV.OC-03, GV.OC-04, GV.OC-05, GV.RM-01, GV.RM-02, GV.RM-03, GV.RM-04, GV.RM-05, GV.RM-06, GV.RM-07, GV.RR-01, GV.RR-02, GV.RR-03, GV.RR-04, GV.PO-01, GV.PO-02, GV.OV-01, GV.OV-02, GV.OV-03, GV.SC-01, GV.SC-02, GV.SC-03, GV.SC-04, GV.SC-05, GV.SC-06, GV.SC-07, GV.SC-08, GV.SC-09, GV.SC-10
SC_3	ID = «Ідентифікація ризиків кібербезпеки»	k_3 = 21	$SC_{3.1}, SC_{3.2}, \dots, SC_{3.21}$	ID.AM-01, ID.AM-02, ID.AM-03, ID.AM-04, ID.AM-05, ID.AM-07, ID.AM-08, ID.RA-01, ID.RA-02, ID.RA-03, ID.RA-04, ID.RA-05, ID.RA-06, ID.RA-07, ID.RA-08, ID.RA-09, ID.RA-10, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04
SC_4	PR = «Кіберзахист»	k_4 = 22	$SC_{4.1}, SC_{4.2}, \dots, SC_{4.22}$	PR.AA-01, PR.AA-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AA-06, PR.AT-01, PR.AT-02, PR.DS-01, PR.DS-02, PR.DS-10, PR.DS-11, PR.PS-01, PR.PS-02, PR.PS-03, PR.PS-04, PR.PS-05, PR.PS-06, PR.IR-01, PR.IR-02, PR.IR-03, PR.IR-04
SC_5	DE = «Виявлення кіберінцидентів»	k_5 = 11	$SC_{5.1}, SC_{5.2}, \dots, SC_{5.11}$	DE.CM-01, DE.CM-02, DE.CM-03, DE.CM-06, DE.CM-09, DE.AE-02, DE.AE-03, DE.AE-04, DE.AE-06, DE.AE-07, DE.AE-08

SC_6	RS = «Реагування на кіберінциденти»	k_6 = 13	$SC_{6.1}, SC_{6.2}, \dots, SC_{6.13}$	RS.MA-01, RS.MA-02, RS.MA-03, RS.MA-04, RS.MA-05, RS.AN-03, RS.AN-06, RS.AN-07, RS.AN-08, RS.CO-02, RS.CO-03, RS.MI-01, RS.MI-02
SC_7	RC = «Відновлення стану кібербезпеки»	k_7 = 8	$SC_{7.1}, SC_{7.2}, \dots, SC_{7.8}$	RC.RP-01, RC.RP-02, RC.RP-03, RC.RP-04, RC.RP-05, RC.RP-06, RC.CO-03, RC.CO-04

Таблиця 4

Представлення підмножин критеріїв системи «Секторальна складова (SE)»

Назва сектору критичної інфраструктури	Назва підмножини критеріїв	Значення k_i	Критерії
Паливно-енергетичний сектор	SE_{PE} = «Секторальна складова паливно-енергетичного сектору»	k_1 = 5	PE_1 — «Чи проведено всебічну оцінку вашого ОКІ відповідно до наказу Міненерго від 10.09.2024 № 338 «Про затвердження Порядку огляду стану кібербезпеки паливно-енергетичного сектору критичної інфраструктури»?»; PE_2 — «Чи проведено оцінювання стану кібербезпеки електричних мереж, відповідно до наказу Міненерго від 05.08.2024 № 285 «Про затвердження Методики оцінювання стану кібербезпеки електричних мереж та практик кібербезпеки електричних мереж»?»; PE_3 — «Чи існують механізми обміну інформацією про кіберзагрози з іншими суб'єктами енергетичної галузі?»; PE_4 — «Чи може ваш ОКІ ефективно відновити нормальну роботу енергетичних систем після масштабної кібератаки, спрямованої на виведення з ладу критичної інфраструктури?»; PE_5 — «Чи проходить операційний персонал, що працює з OT-системами, спеціалізоване навчання з кібербезпеки, яке враховує особливості та ризики промислових систем?»
Цифрові технології	SE_{DT} = «Секторальна складова сектору Цифрові технології»	k_1 = 4	DT_1 — «Чи існують механізми обміну інформацією про кіберзагрози з іншими суб'єктами галузі Цифрових технологій?»; DT_2 — «Чи забезпечено виконання вимог Закону України «Про хмарні послуги»?»; DT_3 — «Чи забезпечено виконання вимог GDPR?»; DT_4 — «Чи забезпечено виконання вимог SOC 2?»;

Захист інформації	SE_{CS} = «Секторальна складова сектору Захист інформації»	k_1 = 4	CS_1 — «Чи забезпечено захист чутливої інформації за допомогою сертифікованих криптографічних засобів?»; CS_2 — «Чи організовано безпечне зберігання, генерація, розподіл та знищення криптографічних ключів?»; CS_3 — «Чи забезпечено безперебійний доступ користувачам до сервісів, що надаються?» CS_4 — «Чи існують механізми обміну інформацією про кіберзагрози з іншими суб'єктами галузі Захист інформації?»;
Харчова промисловість та агропромисловий комплекс	SE_{AK} = «Секторальна складова сектору Харчова промисловість та агропромисловий комплекс»	k_1 = 3	AK_1 — «Чи забезпечено захист автоматизованих систем управління технологічними процесами, що використовуються для контролю якості та безпеки продукції?»; AK_2 — «Чи існують механізми обміну інформацією про кіберзагрози з іншими суб'єктами галузі Харчова промисловість та агропромисловий комплекс?»; AK_3 — «Чи забезпечено, де можливо, відключення автоматизованих систем управління технологічними процесами, що використовуються для контролю якості та безпеки продукції від мережі?»
Державний матеріальний резерв	SE_{DR} = «Секторальна складова сектору Державний матеріальний резерв»	k_1 = 3	DR_1 — «Чи існують механізми обміну інформацією про кіберзагрози з іншими суб'єктами галузі Державний матеріальний резерв?»; DR_2 — «Чи забезпечено захист інформаційних систем, що управляють розподілом, наявністю та станом матеріальних цінностей?»; DR_3 — «Чи розроблено та впроваджено плани реагування на кіберінциденти, що враховують можливість компрометації інформації про критичні запаси або логістичні ланцюжки?»
Охорона здоров'я	SE_{HC} = «Секторальна складова сектору Охорона здоров'я»	k_1 = 5	HC_1 — «Чи існують механізми обміну інформацією про кіберзагрози з іншими суб'єктами галузі охорони здоров'я?»; HC_2 — «Чи забезпечено захист персональних даних пацієнтів?»; HC_3 — «Чи існують чіткі політики та процедури для управління доступом до медичних інформаційних систем?»; HC_4 — «Чи існує механізм моніторингу медичного обладнання на предмет несанкціонованих змін або втручання в його роботу?»; HC_5 — «Чи забезпечено резервне копіювання даних електронних медичних карток пацієнтів з можливістю швидкого відновлення?»

Ринки капіталу та організовані товарні ринки	SE_{RK} = «Секторальна складова сектору Ринки капіталу та організовані товарні ринки»	$k_1 = 3$	RK_1 — «Чи існують механізми обміну інформацією про кіберзагрози з іншими суб'єктами галузі Ринки капіталу та організовані товарні ринки?»; RK_2 — «Чи забезпечено моніторинг та аналіз транзакційних даних для виявлення аномальної активності або шахрайства?»; RK_3 — «Чи забезпечено захист конфіденційної інформації про клієнтів, їхні активи та торговельні стратегії?»
Фінансовий сектор	SE_{FS} = «Секторальна складова фінансового сектору»	$k_1 = 4$	FS_1 — «Чи виконуються вимоги постанови Правління Національного банку України від 12.08.2022 № 178?»; FS_2 — «Чи виконуються вимоги постанови Правління Національного банку України від 19.05.2021 № 43?»; FS_3 — «Чи виконуються вимоги постанови Правління Національного банку України від 16.01.2021 № 4?»; FS_4 — «Чи налагоджено взаємодію з CSIRT-NBU?»
Транспорт і пошта	SE_{TP} = «Секторальна складова сектору Транспорт і пошта»	$k_1 = 3$	TP_1 — «Чи існують механізми обміну інформацією про кіберзагрози з іншими суб'єктами галузі Транспорт і пошта?»; TP_2 — «Чи розроблено та регулярно тестуються плани реагування на кіберінциденти, специфічні для атак на системи управління рухом або логістичні платформи?»; TP_3 — «Чи забезпечено захист конфіденційної інформації про клієнтів, їхні відправлення та персональні дані, які обробляються поштовими сервісами?»
Системи життєзабезпечення	SE_{SL} = «Секторальна складова сектору Системи життєзабезпечення»	$k_1 = 4$	SL_1 — «Чи існують механізми обміну інформацією про кіберзагрози з іншими суб'єктами галузі Системи життєзабезпечення?»; SL_2 — «Чи використовуються рішення для захисту від зловмисного програмного забезпечення, адаптовані для промислових систем?»; SL_3 — «Чи існують механізми моніторингу та виявлення несанкціонованих змін у параметрах технологічних процесів, що можуть призвести до збою в роботі системи?»; SL_4 — «Чи проходить операційний персонал, що працює з OT-системами, спеціалізоване навчання з кібербезпеки, яке враховує особливості та ризики промислових систем?»
Місцеве самоврядування	SE_{LS} = «Секторальна складова сектору Місцеве самоврядування»	$k_1 = 4$	LS_1 — «Чи існують механізми обміну інформацією про кіберзагрози з іншими суб'єктами галузі Місцеве самоврядування?»;

			LS_2 — «Чи проводяться регулярні оцінки безпеки електронних послуг, що надаються громадянам через веб-портали та мобільні додатки?»; LS_3 — «Чи забезпечено резервне копіювання даних, пов'язаних з наданням адміністративних послуг, з можливістю швидкого відновлення?»; LS_4 — «Чи існують механізми захисту систем електронного документообігу та електронних реєстрів від несанкціонованого доступу та зміни даних?»
Промисловість	SE_{IS} = «Секторальна складова сектору Промисловість»	k_1 = 5	IS_1 — «Чи існують механізми обміну інформацією про кіберзагрози з іншими суб'єктами галузі Промисловість?»; IS_2 — «Чи проходить операційний персонал, що працює з OT-системами, спеціалізоване навчання з кібербезпеки, яке враховує особливості та ризики промислових систем?»; IS_3 — «Чи розроблено та впроваджено плани реагування на кіберінциденти, специфічні для атак на системи управління технологічними процесами (ICS/SCADA)?»; IS_4 — «Чи забезпечено регулярне оновлення та моніторинг вбудованого програмного забезпечення (firmware) у промисловому обладнанні та контролерах?»; IS_5 — «Чи забезпечено захист даних, пов'язаних з ланцюгом постачання, включаючи інформацію про сировину, виробничі партії та логістику?»
Сектор громадської безпеки	SE_{GS} = «Секторальна складова сектору громадської безпеки»	k_1 = 3	GS_1 — «Чи існують механізми обміну інформацією про кіберзагрози з іншими суб'єктами галузі громадської безпеки?»; GS_2 — «Чи розроблено та регулярно тестуються плани реагування на кіберінциденти, специфічні для атак на системи екстреного виклику або диспетчерські служби?»; GS_3 — «Чи проводиться регулярна оцінка безпеки додатків та програмного забезпечення, що використовуються в правоохоронних органах та службах порятунку?»
Цивільний захист населення і територій	SE_{GZ} = «Секторальна складова сектору Цивільний захист населення і територій»	k_1 = 5	GZ_1 — «Чи існують механізми обміну інформацією про кіберзагрози з іншими суб'єктами галузі Цивільний захист населення і територій?»; GZ_2 — «Чи забезпечено захист систем екстреного оповіщення населення від несанкціонованого доступу та втручання?»;

			GZ_3 — «Чи розроблено та регулярно тестуються плани реагування на кіберінциденти, специфічні для атак на системи управління надзвичайними ситуаціями?»; GZ_4 — «Чи забезпечено захист критичної інфраструктури, що використовується для забезпечення цивільного захисту (наприклад, системи зв'язку, системи моніторингу)?»; GZ_5 — «Чи проводиться регулярна оцінка безпеки додатків та програмного забезпечення, що використовуються в службах цивільного захисту?»
Охорона навколишнього природного середовища	SE_{ES} = «Секторальна складова сектору Охорона навколишнього природного середовища»	$k_1 = 4$	ES_1 — «Чи існують механізми обміну інформацією про кіберзагрози з іншими суб'єктами галузі Охорона навколишнього природного середовища?»; ES_2 — «Чи забезпечено захист систем моніторингу стану навколишнього середовища від несанкціонованого втручання?»; ES_3 — «Чи розроблено та регулярно тестуються плани реагування на кіберінциденти, специфічні для атак на системи управління ліквідацією екологічних катастроф?»; ES_4 — «Чи існують чіткі протоколи та системи для захисту геоінформаційних систем, що містять дані про заповідні території, екологічні об'єкти та зони ризику?»
Сектор оборони	SE_{DS} = «Секторальна складова сектору оборони»	$k_1 = 3$	DS_1 — «Чи існують механізми обміну інформацією про кіберзагрози з іншими суб'єктами галузі оборони?»; DS_2 — «Чи розроблено та регулярно тестуються плани реагування на кіберінциденти, специфічні для атак на військові системи?»; DS_3 — «Чи проводиться регулярна оцінка безпеки додатків та програмного забезпечення, що використовуються в оборонному секторі?»
Правосуддя	SE_{JS} = «Секторальна складова сектору Правосуддя»	$k_1 = 3$	JS_1 — «Чи існують механізми обміну інформацією про кіберзагрози з іншими суб'єктами галузі Правосуддя?»; JS_2 — «Чи розроблено та регулярно тестуються плани реагування на кіберінциденти, специфічні для атак на судові реєстри або електронні архіви?»; JS_3 — «Чи проводиться регулярна оцінка безпеки додатків та програмного забезпечення, що використовуються в судових органах?»
Виконання кримінальних	SE_{PK} = «Секторальна складова сектору	$k_1 = 4$	PK_1 — «Чи існують механізми обміну інформацією про кіберзагрози з іншими

покарань, тримання під вартою та утримання військовополонених	Виконання кримінальних покарань, тримання під вартою та утримання військовополонених»		суб'єктами галузі Виконання кримінальних покарань, тримання під вартою та утримання військовополонених?»; $РК_2$ — «Чи існують чіткі протоколи та системи для захисту інформації про місцезнаходження, переміщення та стан здоров'я ув'язнених /військовополонених?»; $РК_3$ — «Чи розроблено та регулярно тестуються плани реагування на кіберінциденти, специфічні для атак на системи контролю доступу до режимних об'єктів?»; $РК_4$ — «Чи проводиться регулярна оцінка безпеки додатків та програмного забезпечення, що використовуються в установах виконання покарань?»
Державна реєстрація	SE_{CP} = «Секторальна складова сектору Державна реєстрація»	$k_1 = 3$	$СР_1$ — «Чи існують механізми обміну інформацією про кіберзагрози з іншими суб'єктами галузі Державна реєстрація?»; $СР_2$ — «Чи реалізовано багаторівневу систему управління доступом до реєстрів, що дозволяє контролювати права доступу персоналу?»; $СР_3$ — «Чи забезпечено захист конфіденційної інформації про громадян та підприємства, що зберігається в реєстрах?»
Наукові дослідження та розробки	SE_{SR} = «Секторальна складова сектору Наукові дослідження та розробки»	$k_1 = 4$	SR_1 — «Чи існують механізми обміну інформацією про кіберзагрози з іншими суб'єктами галузі Наукові дослідження та розробки?»; SR_2 — «Чи забезпечено захист інтелектуальної власності, наукових розробок та патентної інформації від несанкціонованого доступу?» SR_3 — «Чи існують чіткі протоколи та системи для захисту інформації, що передається між науковими установами та міжнародними партнерами?» SR_4 — «Чи розроблено та регулярно тестуються плани реагування на кіберінциденти, специфічні для атак на дослідницькі мережі та бази даних?»
Вибори та референдуми	SE_{ER} = «Секторальна складова сектору Вибори та референдуми»	$k_1 = 4$	ER_1 — «Чи існують механізми обміну інформацією про кіберзагрози з іншими суб'єктами галузі Вибори та референдуми?»; ER_2 — «Чи існують чіткі протоколи та системи для захисту інформації, що передається між виборчими комісіями та центральними органами?»; ER_3 — «Чи розроблено та регулярно тестуються плани реагування на кіберінциденти, специфічні для атак на

			електронні виборчі системи або онлайн-ресурси?»; ER_4 — «Чи проводиться регулярна оцінка безпеки додатків та програмного забезпечення, що використовуються в процесі виборів?»
Соціальний захист	SE_{SS} = «Секторальна складова сектору Соціальний захист»	$k_1 = 4$	SS_1 — «Чи існують механізми обміну інформацією про кіберзагрози з іншими суб'єктами галузі Соціальний захист?»; SS_2 — «Чи існують чіткі протоколи та системи для захисту інформації, що передається між реєстрами соціальних виплат та іншими державними установами?»; SS_3 — «Чи запроваджено механізми моніторингу та виявлення несанкціонованих змін у базах даних, що містять інформацію про отримувачів соціальних послуг?»; SS_4 — «Чи реалізовано багаторівневу систему управління доступом до реєстрів, що дозволяє контролювати права доступу персоналу?»
Інформаційний сектор	SE_{IN} = «Секторальна складова інформаційного сектору»	$k_1 = 4$	IN_1 — «Чи існують механізми обміну інформацією про кіберзагрози з іншими суб'єктами інформаційного сектору?»; IN_2 — «Чи розроблено та регулярно тестуються плани реагування на кіберінциденти, специфічні для атак на інформаційні ресурси, такі як веб-портали або бази даних?»; IN_3 — «Чи проводиться регулярна оцінка безпеки додатків та програмного забезпечення, що використовуються в інформаційному секторі?»; IN_4 — «Чи реалізовано багаторівневу систему управління доступом до інформаційних ресурсів, що дозволяє контролювати права доступу персоналу?»
Державна влада	SE_{SA} = «Секторальна складова сектору Державна влада»	$k_1 = 3$	SA_1 — «Чи існують механізми обміну інформацією про кіберзагрози з іншими суб'єктами галузі Державна влада?»; SA_2 — «Чи розроблено та регулярно тестуються плани реагування на кіберінциденти, специфічні для атак на державні реєстри, системи електронного урядування та веб-портали?»; SA_3 — «Чи проводиться регулярна оцінка безпеки додатків та програмного забезпечення, що використовуються в державних установах?»

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (29), 2025
ISSN 2663 - 4023

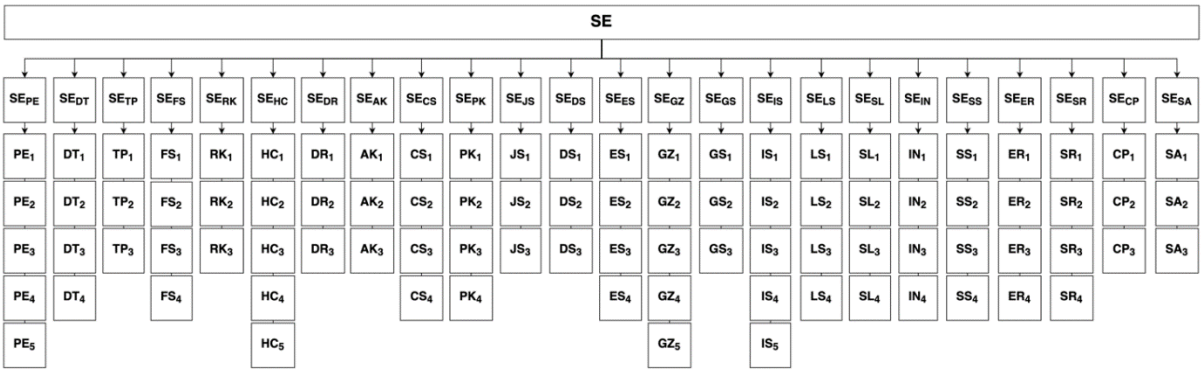

Рис. 1. Візуальне представлення підмножин та критеріїв системи «Секторальна складова»

Наведена на рис. 1 структурна організація системи «Секторальна складова» відображає підмножини критеріїв, що відповідають секторам критичної інфраструктури, визначеними в [22]. Кожна підмножина містить від 3 до 5 критеріїв, що забезпечує достатню деталізацію без надмірного ускладнення системи.

Такий підхід гарантує повне охоплення всіх актуальних нормативних вимог, які стосуються кіберзахисту кожного окремого сектору критичної інфраструктури, і робить систему ефективним інструментом оцінки.

Наприклад, при n = 1, $k_1 = 5$; n = 2, $k_2 = 31$; n = 3, $k_3 = 21$; n = 4, $k_4 = 22$; n = 5, $k_5 = 11$; n = 6, $k_6 = 13$ та n = 7, $k_7 = 8$, з використанням (3) в [16], представимо множину систем критеріїв *SC* таким чином:

$$SC = \left\{ \bigcup_{i=1}^{n} \left\{ \bigcup_{j=1}^{k_i} SC_{ij} \right\} \right\} = \{\{SC_{1.1}, SC_{1.2}, \ldots, SC_{1.5}\}, \{SC_{2.1}, SC_{2.2}, \ldots, SC_{2.31}\}, \{SC_{3.1}, SC_{3.2}, \ldots, SC_{3.21}\}, \{SC_{4.1}, SC_{4.2}, \ldots, SC_{4.22}\}, \{SC_{5.1}, SC_{5.2}, \ldots, SC_{5.11}\} \{SC_{6.1}, SC_{6.2}, \ldots, SC_{6.13}\} \{SC_{7.1}, SC_{7.2}, \ldots, SC_{7.8}\}\}$$

$$= \{\{PE_1, PE_2, PE_3, PE_4, PE_5\}, \{GV.OC-01, GV.OC-02, GV.OC-03, GV.OC-04, GV.OC-05, GV.RM-01, GV.RM-02, GV.RM-03, GV.RM-04, GV.RM-05, GV.RM-06, GV.RM-07, GV.RR-01, GV.RR-02, GV.RR-03, GV.RR-04, GV.PO-01, GV.PO-02, GV.OV-01, GV.OV-02, GV.OV-03, GV.SC-01, GV.SC-02, GV.SC-03, GV.SC-04, GV.SC-05, GV.SC-06, GV.SC-07, GV.SC-08, GV.SC-09, GV.SC-10\}, \{ID.AM-01, ID.AM-02, ID.AM-03, ID.AM-04, ID.AM-05, ID.AM-07, ID.AM-08, ID.RA-01, ID.RA-02, ID.RA-03, ID.RA-04, ID.RA-05, ID.RA-06, ID.RA-07, ID.RA-08, ID.RA-09, ID.RA-10, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04\}, \{PR.AA-01, PR.AA-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AA-06, PR.AT-01, PR.AT-02, PR.DS-01, PR.DS-02, PR.DS-10, PR.DS-11, PR.PS-01, PR.PS-02, PR.PS-03, PR.PS-04, PR.PS-05, PR.PS-06, PR.IR-01, PR.IR-02, PR.IR-03, PR.IR-04\}, \{DE.CM-01, DE.CM-02, DE.CM-03, DE.CM-06, DE.CM-09, DE.AE-02, DE.AE-03, DE.AE-04, DE.AE-06, DE.AE-07, DE.AE-08\}, \{RS.MA-01, RS.MA-02, RS.MA-03, RS.MA-04, RS.MA-05, RS.AN-03, RS.AN-06, RS.AN-07, RS.AN-08, RS.CO-02, RS.CO-03, RS.MI-01, RS.MI-02\}, \{RC.RP-01, RC.RP-02, RC.RP-03, RC.RP-04, RC.RP-05, RC.RP-06, RC.CO-03, RC.CO-04\}\}$$

Загальну структуру модифікованої моделі розрахунку рівня кіберзахисту ОКІІ представлено на рис. 2 (з урахуванням Етапів 3-5 моделі, розробленої в [16]).

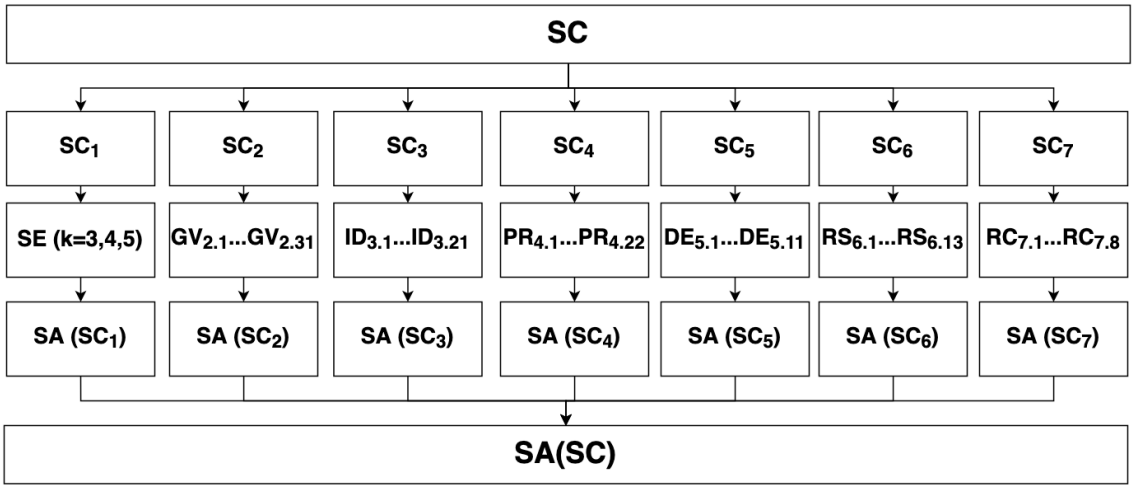

Рис. 2. Модифікована модель розрахунку рівня кіберзахисту ОКІІ

Рис. 2 ілюструє модифіковану модель розрахунку рівня кіберзахисту ОКІІ, яка є ієрархічною за своєю структурою. На найвищому рівні система критеріїв (SC) декомпонується на сім підсистем (SC1 — SC7). Кінцевим результатом функціонування моделі є єдиний інтегральний показник (SA(SC)), який синтезує індивідуальні оцінки (SA(SC1)-SA(SC7)) кожної підсистеми.

Отриманий інтегральний показник може бути інтерпретований відповідно до п’ятирівневої шкали, що дозволяє визначити рівень зрілості кіберзахисту ОКІІ та розробити цілеспрямовані стратегії для його підвищення.

Таким чином, модель, розроблена в [16] модифікована для підвищення її функціональності, шляхом інтеграції додаткових систем критеріїв та розширення кількості критеріїв у відповідності до законодавства України.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У роботі здійснено аналіз існуючих підходів до розрахунку рівня кіберзахисту, який показав що наказ АД № 54 є найбільш придатним для оцінки кіберзахисту в Україні. Це обумовлено його повною відповідністю чинному законодавству, гнучкістю та чіткими механізмами оцінювання. Розробка моделі була зосереджена на модифікації існуючої моделі розрахунку рівня кіберзахисту ОКІ шляхом розширення кількості систем критеріїв та деталізації показників. До шести обов’язкових систем критеріїв, що базуються на законодавстві України була додана сьома система — «Секторальна складова». Ця нова система дозволяє враховувати специфічні особливості кожного сектору критичної інфраструктури та забезпечує більш точне і повне оцінювання. Модифікована модель має ієрархічну структуру та дозволяє розрахувати єдиний інтегральний показник, який синтезує оцінки за всіма критеріями. Цей показник інтерпретується за п’ятирівневою шкалою, що дає можливість об’єктивно оцінити рівень зрілості кіберзахисту ОКІІ та розробити цілеспрямовані стратегії для його підвищення.

Продовженням дослідження стане розробка методу оцінювання стану кіберзахисту ОКІІ та програмного інструменту, що автоматизує розрахунки та візуалізацію результатів оцінювання. Це дозволить провести експериментальне дослідження розробленого методу для підтвердження його ефективності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Державний центр кіберзахисту Державної служби спеціального зв'язку та захисту інформації України. (2025). *WAR AND CYBER: THREE YEARS OF STRUGGLE AND LESSONS FOR GLOBAL SECURITY. SSSCIP & ICE TASK FORCE.* https://cip.gov.ua/services/cm/api/attachment/download?id=69131
2. Державний центр кіберзахисту Державної служби спеціального зв'язку та захисту інформації України. (2024). *Russian Cyber Operations H2'2024.* https://cip.gov.ua/services/cm/api/attachment/download?id=68768
3. Рада національної безпеки і оборони України. (2024). *Річний аналітичний огляд (жовтень 2023 – вересень 2024).* https://www.rnbo.gov.ua/files/2024/NATIONAL_CYBER_SCC/20250109/Year%20in%20review_UKR_upd.pdf?fbclid=IwY2xjawI-fZRleHRuA2FlbQIxMAABHcaZdkgcVIlSJ0eGnBO78x5xRCDcoBwcJ1GKrT4SAVS5reEAtY5u8ssd4w_aem_0xN1oMO3-toIy6vpuA27mA
4. Президент України. (2021). *Указ від 26.08.2021 р. № 447/2021 «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»»* https://www.president.gov.ua/documents/4472021-40013
5. ISO/IEC. (2022). *27001:2022. Information technology — Security techniques — Information security management systems — Requirements.*
6. National Institute of Standards and Technology. (2024) *NIST Cybersecurity Framework, version 2.0.* https://www.nist.gov/cyberframework
7. CMMI Institute. (2023). *Capability Maturity Model Integration (CMMI) for Development, Version 3.0.* https://cmmiinstitute.com/cmmi
8. U.S. Department of Energy. (2022). *Cybersecurity Capability Maturity Model (C2M2), version 2.1.* https://www.energy.gov/sites/default/files/2022-06/C2M2%20Version%202.1%20June%202022.pdf
9. Carnegie Mellon University's Software Engineering Institute (SEI). (2012). *Smart Grid Maturity Model, version 1.2.* https://www.sei.cmu.edu/library/smart-grid-maturity-model-assets-collection-version-12/
10. Cybersecurity and Infrastructure Security Agency. (2023). *CISA Cybersecurity Performance Goals.* https://www.cisa.gov/sites/default/files/2023-03/CISA_CPG_REPORT_v1.0.1_FINAL.pdf
11. Кабінет Міністрів України. (2019). *Постанова від 19 червня 2019 р. № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури».*
12. Адміністрація Державної служби спеціального зв'язку та захисту інформації України. (2021). *Наказ від 06.10.2021 № 601 «Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури».*
13. Адміністрація Державної служби спеціального зв'язку та захисту інформації України. (2025). *Наказ від 30.01.2025 № 54 «Про затвердження Базових заходів з кіберзахисту та Методичних рекомендацій щодо здійснення базових заходів з кіберзахисту».*
14. Міністерство енергетики України. (2024). *Наказ від 05.08.2024 № 285 «Про затвердження Методики оцінювання стану кібербезпеки електричних мереж та практик кібербезпеки електричних мереж».*
15. Bakalynskyi, Oleksandr & Pakholchenko, Dmytro. (2022). *Деякі питання забезпечення кіберзахисту автоматизованих систем управління технологічними процесами.* https://www.researchgate.net/publication/362112446_Deaki_pitanna_zabezpecenna_kiberzahistu_avtomatizovanih_sistem_upravlinna_tehnologicnimi_procesami
16. Юдіна, Д. (2025). Модель розрахунку рівня кіберзахисту об'єктів критичної інфраструктури. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», *4*(28), 586–598. https://doi.org/10.28925/2663-4023.2025.28.829
17. National Institute of Standards and Technology. (2018) *NIST Cybersecurity Framework, version 1.1.* https://www.nist.gov/cyberframework
18. Khudyntsev, M. M., & Palazhchenko, I. L. (2024). *Cybersecurity maturity models for cybersecurity assessment in critical infrastructure*. Environmental Safety and Natural Resources, 52(4), 122–134. https://doi.org/10.32347/2411-4049.2024.4.122-134
19. Carnegie Mellon University. (2010). *CERT'S PODCASTS: SECURITY FOR BUSINESS LEADERS: SHOW*. https://www.sei.cmu.edu/documents/4622/2010_016_102_67772.pdf
20. Кабінет Міністрів України. (2021). *Постанова від 29.12.2021 № 1426 «Про затвердження Положення про організаційно-технічну модель кіберзахисту».*

21. Верховна Рада України. (2025). *Закон України «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури» № 4336-IX від 27.03.2025 р.*
22. Кабінет Міністрів України. (2020). *Постанова від 09.10.2020 № 1109 «Деякі питання об'єктів критичної інфраструктури».*

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (29), 2025
ISSN 2663 - 4023

Diana Yudina
PhD student of the Faculty of Computer Science and Technology
State University "Kyiv Aviation Institute", Kyiv, Ukraine
ORCID ID: 0000-0002-1277-8771
diana.yudina22@gmail.com

MODIFICATION OF THE MODEL FOR CALCULATING THE LEVEL OF CYBER SECURITY OF CRITICAL INFRASTRUCTURE FACILITIES

Abstract. The growing intensity of cyber threats and cyber attacks, especially from the Russian Federation, poses an unprecedented danger to critical infrastructure and critical information infrastructure. The consequences of such incidents can be catastrophic, causing massive economic damage, social destabilization, and a direct threat to life. This increase in the number of cyberattacks requires continuous improvement of approaches to cybersecurity and an objective assessment of their level of protection. In view of this need, a model for calculating the level of cyber protection was developed. During the testing of the model, certain shortcomings were identified, in particular the inadequacy of the criteria systems and the ambiguity of the integral indicator, which limited its relevance and accuracy, especially in the context of dynamic changes in Ukrainian legislation. This led to the modification of the model by expanding the number of criteria systems and their indicators in accordance with current national regulations and the specific characteristics of each critical infrastructure sector. The key change is the expansion of the set of criteria for assessing cyber protection. A new, seventh system of criteria, "Sectoral Component" has been added to the six mandatory groups of measures (Government, Identification, Protection, Detection, Response, Recovery). This system allows for the integration of industry (sectoral) characteristics of different critical infrastructure sectors. The modified model has a hierarchical structure and presents the result in the form of a single integrated quantitative indicator, interpreted on a five-level percentage scale, consistent with international maturity models, enabling an objective assessment of the maturity level of cyber protection for critical information infrastructure facilities and the development of targeted strategies to improve it.

Keywords: cyber protection; critical infrastructure; critical infrastructure facilities; critical information infrastructure facilities; assessment model; system of criteria.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. State Center for Cyber Protection of the State Service for Special Communications and Information Protection of Ukraine. (2025). WAR AND CYBER: THREE YEARS OF STRUGGLE AND LESSONS FOR GLOBAL SECURITY. SSSCIP & ICE TASK FORCE. https://cip.gov.ua/services/cm/api/attachment/download?id=69131
2. State Center for Cyber Protection of the State Service for Special Communications and Information Protection of Ukraine. (2024). Russian Cyber Operations H2'2024. https://cip.gov.ua/services/cm/api/attachment/download?id=68768
3. National Security and Defense Council of Ukraine. (2024). Annual Analytical Review (October 2023 – September 2024). https://www.rnbo.gov.ua/files/2024/NATIONAL_CYBER_SCC/20250109/Year%20in%20review_UKR_upd.pdf?fbclid=IwY2xjawI-fZRleHRuA2FlbQIxMAABHcaZdkgcVIlSJ0eGnBO78x5xRCDcoBwcJ1GKrT4SAVS5reEAtY5u8ssd4w_aem_0xN1oMO3-toIy6vpuA27mA
4. President of Ukraine. (2021). Decree No. 447/2021 of August 26, 2021, "On the Decision of the National Security and Defense Council of Ukraine of May 14, 2021, "On the Cybersecurity Strategy of Ukraine." https://www.president.gov.ua/documents/4472021-40013
5. ISO/IEC. (2022). 27001:2022. Information technology — Security techniques — Information security management systems — Requirements.
6. National Institute of Standards and Technology. (2024) *NIST Cybersecurity Framework, version 2.0.* https://www.nist.gov/cyberframework

7. CMMI Institute. (2023). *Capability Maturity Model Integration (CMMI) for Development, Version 3.0.* https://cmmiinstitute.com/cmmi
8. U.S. Department of Energy. (2022). *Cybersecurity Capability Maturity Model (C2M2), version 2.1.* https://www.energy.gov/sites/default/files/2022-06/C2M2%20Version%202.1%20June%202022.pdf
9. Carnegie Mellon University's Software Engineering Institute (SEI). (2012). *Smart Grid Maturity Model, version 1.2.* https://www.sei.cmu.edu/library/smart-grid-maturity-model-assets-collection-version-12/
10. Cybersecurity and Infrastructure Security Agency. (2023). *CISA Cybersecurity Performance Goals.* https://www.cisa.gov/sites/default/files/2023-03/CISA_CPG_REPORT_v1.0.1_FINAL.pdf
11. Cabinet of Ministers of Ukraine. (2019). Resolution No. 518 of June 19, 2019, "On Approval of General Requirements for Cyber Protection of Critical Infrastructure Facilities."
12. Administration of the State Service for Special Communications and Information Protection of Ukraine. (2021). Order No. 601 of October 6, 2021, "On Approval of Methodological Recommendations for Improving the Level of Cyber Protection of Critical Information Infrastructure."
13. Administration of the State Service for Special Communications and Information Protection of Ukraine. (2025). Order No. 54 of January 30, 2025, "On Approval of Basic Cyber Security Measures and Methodological Recommendations for the Implementation of Basic Cyber Security Measures."
14. Ministry of Energy of Ukraine. (2024). Order No. 285 of 05.08.2024 "On Approval of the Methodology for Assessing the Cybersecurity Status of Electrical Networks and Cybersecurity Practices for Electrical Networks."
15. Bakalynskyi, Oleksandr & Pakholchenko, Dmytro. (2022). Some issues of ensuring cyber protection of automated process control systems. https://www.researchgate.net/publication/362112446_Deaki_pitanna_zabezpecenna_kiberzahistu_avtomatizovanih_sistem_upravlinna_tehnologicnimi_procesami
16. Yudina, D. (2025). Model for Calculating the Level of Cyber Security of Critical Infrastructure Objects. Electronic professional scientific publication "Cybersecurity: Education, Science, Technology," 4(28), 586–598. https://doi.org/10.28925/2663-4023.2025.28.829
17. National Institute of Standards and Technology. (2018) *NIST Cybersecurity Framework, version 1.1.* https://www.nist.gov/cyberframework
18. Khudyntsev, M. M., & Palazhchenko, I. L. (2024). *Cybersecurity maturity models for cybersecurity assessment in critical infrastructure*. Environmental Safety and Natural Resources, 52(4), 122–134. https://doi.org/10.32347/2411-4049.2024.4.122-134
19. Carnegie Mellon University. (2010). *CERT'S PODCASTS: SECURITY FOR BUSINESS LEADERS: SHOW*. https://www.sei.cmu.edu/documents/4622/2010_016_102_67772.pdf
20. Cabinet of Ministers of Ukraine. (2021). Resolution No. 1426 of December 29, 2021, "On Approval of the Regulations on the Organizational and Technical Model of Cyber Security."
21. Verkhovna Rada of Ukraine. (2025). Law of Ukraine "On Amendments to Certain Laws of Ukraine Regarding Information Protection and Cyber Protection of State Information Resources and Critical Information Infrastructure Facilities" No. 4336-IX of 27.03.2025.
22. Cabinet of Ministers of Ukraine. (2020). Resolution No. 1109 of October 9, 2020, "Certain Issues of Critical Infrastructure Facilities."