DOI: 10.18372/2310-5461.61.18509
УДК 004.946.5.056(477)(045)

О. Г. Корченко**,** д-р техн. наук, проф.,
Державний університет
інформаційно-комунікаційних технологій
orcid.org/0000-0003-3376-0631
e-mail: agkorchenko@gmail.com;

Є. В. Іванченко**,** канд. техн. наук, проф.,
Національний авіаційний університет
orcid.org/0000-0003-3017-5752
e-mail: evivancenko@gmail.com;

О. О. Бакалинський**,** канд. техн. наук,
Департамент кіберзахисту Адміністрації
Державної служби спеціального зв'язку та
захисту інформації України
orcid.org/0000-0001-9712-2036
e-mail: baov@meta.ua;

Д. В. Мялковський Департамент кіберзахисту Адміністрації
Державної служби спеціального зв'язку та
захисту інформації України
orcid.org/0000-0002-8246-8437
e-mail: daniilvm71@gmail.com;

Д. А. Зубков**,** Департамент кіберзахисту Адміністрації
Державної служби спеціального зв'язку та
захисту інформації України
orcid.org/0000-0002-8246-8536
e-mail: d.zubkov@cip.gov.ua

МЕТОД ОЦІНЮВАННЯ РІВНЯ ПІДВИЩЕННЯ СТАНУ КІБЕРЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ДЕРЖАВИ

Вступ

У сучасному цифровому світі процес реалізації кіберзагроз стає все більш вишуканим та складним. Можливості розвитку кіберзлочинності, шпигунства та кібертероризму стають набагато більш доступними завдяки розвитку технологій та збільшенню кількості кібернападів. Критична інфраструктура держави (енергетика, транспорт, медичні установи тощо) все більше стає залежною від інформаційних технологій. Порушення безпеки цих технологій може призвести до серйозних наслідків для життя та здоров'я громадян, а також економічних втрат. Багато країн встановлюють різні регулятивні вимоги стосовно кіберзахисту, наприклад, GDPR в Європейському Союзі або NIST у Сполучених Штатах. Це змушує організації, що управляють критичною інфраструктурою, активно шукати та впроваджувати ефективні методи оцінювання рівня кіберзахисту. Швидкий технологічний прогрес призводить до появи нових методів атак, для захисту від яких необхідно залучати різні ресурси (фінансові, людські, часові тощо) для створення нових більш ефективних засобів для підвищення стану кіберзахисту. Оцінка рівня такого стану в подальшому дасть можливість оцінити ефект від вкладених в безпеку ресурсів. Оновлені методи оцінювання дозволяють враховувати кібервторгневі інновації та застосовувати сучасні техніки та підходи до кіберзахисту. Отже, методи оцінювання рівня підвищення стану кіберзахисту об'єктів критичної інфраструктури є актуальним питанням стратегії кібербезпеки держави та її важливою складовою для забезпечення стійкості суспільства у цифрову епоху.

Аналіз досліджень і публікацій

Проблеми забезпечення кіберзахисту критичної інфраструктури в умовах зростаючих кібер-

загроз [1] свідчать про необхідність розробки відповідних ефективних методів. Відомі методи оцінювання рівня кіберзахисту [2, 3, 4] не орієнтовані на врахування специфіки критичної інфраструктури та не використовують відповідні сучасні техніки та інструменти.

Розуміючи, що збільшення кількості кіберзагроз критичній інфраструктурі потребує нових інноваційних підходів до їхнього виявлення та управління. Використання теорії нечітких множин стає ключовим інструментом для досягнення цієї мети та може суттєво підвищити ефективність кібербезпекових заходів організацій, що підтверджується низкою досліджень, проведених у [5, 6, 7]. Однак в сучасних публікаціях не виявлено методів, які б здійснювали оцінювання рівня підвищення стану кіберзахисту об'єктів критичної інфраструктури на основі експертного оцінювання, що ґрунтується на теорії нечітких множин.

Тому ***метою*** даного дослідження є розробка методу оцінювання рівня підвищення стану кіберзахисту об'єкту критичної інфраструктури держави з метою підвищення її стійкості до кіберзагроз та забезпечення національної без-пеки України. Запропонований метод включає процедури, що реалізуються шістьма етапами: формування лінгвістичних змінних (ЛЗ), фази-фікацію інтервалів та побудову еталонів, фор-мування множини характеристик об'єктів огляду, визначення поточних значень характеристик об'єктів огляду, процес первинного вимірювання, формування базових пар та евристичних правил і візуалізація результатів. Розглянемо кожен з них докладніше.

Основний матеріал

Етап 1. Формування лінгвістичних змінних

Відоповідно до [8] заходи кіберзахисту – «Ідентифікація ризиків кібербезпеки (ID)», «Кіберзахист» (PR), «Виявлення кіберінцидентів» (DE), «Реагування на кіберінциденти» (RS), «Відновлення стану кібербезпек» (RC), кожна з яких містить клас ЗКЗ «Ідентифікація ризиків кібербезпеки (ID)» – ID.AM, ID.BE, ID.GV, ID.RA, ID.RM, ID.SC, «Кіберзахист» (PR) – PR.AC, PR.AT, PR.DS, PR.IP, PR.MA, PR.PT, «Виявлення кіберінцидентів» (DE) – DE.AE, DE.CM, DE.DP, «Реагування на кіберінциденти» (RS) – RS.RP, RS.CO, RS.AN, RS.MI, RS.IM, «Відновлення стану кібербезпеку» (RC) – RC.RP, RC.IM, RC.CO. Кожному класу притаманні відповідні ЗКЗ [4,8], так, наприклад, для ID – це ID.AM1÷6, ID.BE1÷5, ID.GV1÷4, ID.RA1÷6, ID.RM1÷3, ID.SC1÷5.

Для формалізації процесу вимірювання системи ЗКЗ здійснюється формування ЛЗ на підставі кортежу [5] <***TL***, $\underset{\sim}{T}_{TL}$, X_{TL}> з певною областю визначення базової терм-множини ***TL*** за допомогою f термів. Для кожного з термів виконується вираз

$$\underset{\sim}{T}_{TL} = \bigcup_{i=1}^{f} \underset{\sim}{T}_{TL_i}, \qquad (1)$$

де для значень $i = \overline{1,f}$ визначається свій інтервал, що лежить в межах $X_{TL} = [tl_1; tl_{f+1}]$ та складається з $[tl_1; tl_2[, \ldots, [tl_i; tl_{i+1}[, \ldots, [tl_n; tl_{f+1}]$.

Так, наприклад, для відображення результату оцінювання стану виконання класу ЗКЗ q-тим об'єктом огляду критичної інфраструктури ($q = \overline{1,m}$) введемо ЛЗ ***ACM*** – "*СТАН ЗАХОДІВ КІБЕРЗАХИСТУ*", яку на підставі (1) визначимо кортежем [4] <***ACM***, $\underset{\sim}{T}_{ACM}$, X_{ACM}>. Базова терм-множина ***ACM*** засновується на f термах і має вигляд:

$$\underset{\sim}{T}_{ACM_i} = \cup_{i=1}^{f} \underset{\sim}{T}_{ACM_i}. \qquad (2)$$

Наприклад, для ***ACM*** при $f = 4$ ($i = \overline{1,4}$)

$$\underset{\sim}{T}_{\text{ACM}} = \bigcup_{i=1}^{4} \underset{\sim}{T}_{\text{ACM}_i}, = \{\underset{\sim}{T}_{\text{ACM}_1}, \underset{\sim}{T}_{\text{ACM}_2}, \underset{\sim}{T}_{\text{ACM}_3}, \underset{\sim}{T}_{\text{ACM}_4}\} = \{\text{"НЕ ПОТРЕБУЄТЬСЯ"},$$

"РОЗГЛЯДАЄТЬСЯ ДЛЯ РЕАЛІЗАЦІЇ", "У ПРОЦЕСІ", "РЕАЛІЗОВАНО"},

де $\underset{\sim}{T}_{ACM_i}$ $(i = \overline{1,f})$ – терми НЧ (значення ЛЗ), а $X_{ACM} = [x_{ACM}^{min}, x_{ACM}^{max}] = [x_{ACM}^{min} = X_{ACM1}; X_{ACM2}[, [X_{ACM2}; X_{ACM3}[, \ldots, [X_{ACMi}; X_{ACMi+1}[, \ldots, [X_{ACM_f}; x_{ACM}^{max} = X_{ACM_{f+1}}]$ – область визначення НЧ.

Етап 2. Фазифікація інтервалів та побудова еталону стан заходів кіберзахисту

Для формування еталонних величин за допомогою метода [4] реалізуємо фазифікацію інтервалів $[X_{ACM1}; X_{ACM2}[, \ldots, [X_{ACMi}; X_{ACMi+1}[, \ldots, [X_{ACMf}; X_{ACMf+1}]$, де з урахуванням досліджень в [5] визначимо коефіцієнт зближеності CF=0,25.

Далі, обрахуємо M_i для кожного i-го терму:

$$M_i = \frac{X_{ACM_i} + X_{ACM_{i+1}}}{2}, \; i = \overline{1,f} \qquad (4)$$

та значення

$$SP = M_1 - CF\left(X_{ACM_2} - X_{ACM_1}\right). \qquad (5)$$

Коефіцієнт розтягнення SC, що корегує величини термів в межах $[ACM_1; ACM_{f+1}]$ визначимо як:

$$SC = \frac{X_{AMC_{f+1}}}{M_f + CF\left(X_{AMC_{f+1}} - X_{AMC_f}\right) - SP}, \quad (6)$$

де f – кількість інтервалів (термів).

Далі на підставі (7)–(10) здійснюється перетворення інтервалів в НЧ:

$$b_{1i} = SC\left(M_i - CF\left(X_{ACM_{i+1}} - X_{ACM_i}\right) - SP\right), \quad (i = \overline{1, f}); \quad (7)$$

$$b_{2i} = SC\left(M_i + CF\left(X_{ACM_{i+1}} - X_{ACM_i}\right) - SP\right), \quad (i = \overline{1, f}); \quad (8)$$

$$a_1 = AMC_1;\ a_i = b_{2i-1},\ (i = \overline{2, f}); \quad (9)$$

$$c_f = AMC_{f+1};\ c_i = b_{1i+1},\ (i = \overline{1, f-1}). \quad (10)$$

Таблиця 1

Значення інтервалів для *ACM* при *f*=4

Тип розподілу	$[X_{ACM_1};$ $X_{ACM_2}[$	$[X_{ACM_2};$ $X_{ACM_3}[$	$[X_{ACM_3};$ $X_{ACM_4}[$	$[X_{ACM_4};$ $X_{ACM_5}[$
Рівномірний	[0; 0]	]0; 50[	[50; 100[	[100; 100]

Наприклад, для ЛЗ ***AMC*** при *f*=4 здійснимо перетворення інтервалів представлених в табл. 1 за (7)–(10). Оскільки *CF* = 0,25, то впевненість експерта щодо належності інтервалу до значення ЛЗ відповідає 50 %, тобто, для $[AMC_1;\ AMC_{f+1}]$ = = [0; 100] половина всіх значень μ(*AMC*) = 1.

Далі за формулою (4)–(6) визначимо: (7)

$$M_1 = (X_{ACM_1} + X_{ACM_2})/2 = (0+0)/2 = 0;$$

$$M_2 = 25;\ M_3 = 75;\ M_4 = 100, \quad (8)$$

а

$$SP = M_1 - CF\left(X_{ACM_2} - X_{ACM_1}\right) = \quad (9)$$

$$= 0 - 0{,}25(0 - 0) = 0,$$

а за допомогою (6) визначається коефіцієнт розтягнення: $SC = \frac{AMC_6}{M_5 + CF\left(X_{ACM_6} - X_5\right) - SP} =$ (10)

$$SC = ACM_5/M_4 + CF\left(X_{ACM_4} - X_{ACM_3}\right) - SP =$$

$$= 100/(100 + 0{,}25(100–100)–0) = 1.$$

Результати фазифікації інтервалів для ***ACM*** при *f* = 4 занесемо табл. 2.

Таблиця 2

Результати фазифікації інтервалів для *ACM* при *f*=4

Тип розподілу НЧ	‘НЧ $\underset{\sim}{T}_{ACM_i} = (a_i;\ b_{1i};\ b_{2i};\ c_i)_{LR}$, $(i = \overline{1,4})$			
	$\underset{\sim}{T}_{ACM_1}$	$\underset{\sim}{T}_{ACM_2}$	$\underset{\sim}{T}_{AM_{M3}}$	$\underset{\sim}{T}_{ACM_4}$
Різнорідний	$(0;\ 0;\ 0;\ 12{,}5)_{LR}$	$(0;\ 12{,}5;\ 37{,}5;\ 62{,}5)_{LR}$	$(37{,}5;\ 62{,}5;\ 87{,}5;\ 100)_{LR}$	$(87{,}5;\ 100;\ 100;\ 100)_{LR}$

Зазначимо, що інтервали при *f* = 4 (див. табл. 2), а відповідно і НЧ $\underset{\sim}{T}_{ACM_i}$ для ***ACM*** віднесемо до нерівномірного (різнорідного) типу розподілу відповідно [5, 6]:

$$\Omega_{\text{р}} = (X_{ACM_2} - X_{ACM_1} \neq X_{ACM_3} - X_{ACM_2}) \vee (X_{ACM_3} - X_{ACM_2} = X_{ACM_4} - X_{ACM_3}) \vee (X_{ACM_4} - X_{ACM_3}) =$$

$$= (0 - 0 \neq 50 - 0) \vee (50 - 0 = 100 - 50) \vee (100 - 100 = 100 - 100) = 1 \vee 1 \vee 1 = 1.$$

Далі, здійснимо перетворення інтервалів ЛЗ ***ACM*** у еталонні НЧ.

За допомогою ЛЗ ***ACM*** можемо здійснювати оцінку системи заходів кіберзахисту, для чого визначимо відповідно до категорії і заходи. Значення цих показників знаходиться в інтервалі від 0 % до 100 % (див. табл. 1) і відповідно визначаються як: не потребується; розглядається для реалізації; у процесі; реалізовано (див. табл. 2).

Оцінювання показника (див. табл. 3) здійснюється за наступною шкалою:

$[X_{ACM1};\ X_{ACM2}] \in [0; 0]$ – «НЕ ПОТРЕБУЄТЬСЯ»; $]X_{ACM2};\ X_{ACM3}[\in]0; 50[$;
«У ПРОЦЕСІ» $[X_{ACM3};\ X_{ACM4}[\in [50; 100[$ – «РОЗГЛЯДАЄТЬСЯ ДЛЯ РЕАЛІЗАЦІЇ»;
$[X_{ACM4;}\ X_{ACM5}] \in [100; 100]$ – «РЕАЛІЗОВАНО».

Таблиця 3

Фрагмент системи заходів кіберзахисту

Категорія ЗКЗ	Опис	ЗКЗ	Опис
Клас ЗКЗ «Ідентифікація ризиків кібербезпеки» (ID)			
ID.AM «Управління активами»	Описуються дані, персонал, пристрої та носії інформації, інформаційні системи, що дозволяють забезпечити надання життєво важливих послуг та функцій до рівня важливості для організації відносно життєво-важливих послуг та	ID.AM-1	Для чого використовується ідентифікація всіх пристроїв, носіїв інформації, інформаційних систем, що проводиться на ОКІ?
		ID.AM-2	Що потрібно зробити з програмними забезпеченнями, що використовуються для забезпечення роботи ОКІІ

Продовження табл. 3

Фрагмент системи заходів кіберзахисту			
Категорія ЗКЗ	Опис	ЗКЗ	Опис
Клас ЗКЗ «Відновлення стану кібербезпеки» (RC)			
	функцій, а також описується політика управління ризиками		ОКІ, які забезпечують надання життєво важливих послуг та виконання життєво важливих функцій?
		ID.AM-3	Які роботи здійснюються для забезпечення надання основної послуги/ виконання основної функції ОКІ? Що відображає структурна схема ін-формаційних потоків? Для чого є важливою ця інформація?
		ID.AM-4	Куди слід віднести інформаційні та інформаційно-комунікаційні системи, які взаємодіють з ОКІІ ОК?
		ID.AM-5	Що класифікує організація? Що визначає та затверджує організація під час процесу інвентаризації?
		ID.AM-6	Які обов'язки та відповідальність визначаються та описуються? Яка політика затверджується та доводиться до персоналу на ОКІ? Які програми впроваджуються?
ID.BE «Середовище надання життєво важливих послуг та функцій»	Формування обов'язків персоналу щодо забезпечення кібербезпеки, а також рішень з управління ризиками у сфері кібербезпеки.	ID.BE-1	З чим можуть бути пов'язані вимоги, визначені в угодах з постачальником?
		ID.BE-2	В чому має визначити свою роль ОКІ?
		ID.BE-3	Щодо чого визначаються пріоритети цілей і завдань на ОКІ? Як здійснюються такі пріоритети?
		ID.BE-4	Чи забезпечує організація ідентифікацію та реєстрацію критично важливих архівів? Яку інформацію містить реєстрація?
		ID.BE-5	Вимоги для чого ідентифікує та визначає організація?
ID.GV «Управління безпекою»	Формування правил, процедур і процесів для управління й моніторингу впроваджених нормативних, екологічних та експлуатаційних вимог, а також вимог щодо забезпечення кібербезпеки.	ID.GV-1	Чи визначає організація політику інформаційної/кібербезпеки? Чи повідомляє організація про існування та зміст інформаціної/ кібербезпеки для партнерів організації?
		ID.GV-2	Які обов'язки, пов'язані із забезпеченням безпеки ОКІ визначаються? З ким може взаємодіяти ОКІ? Хто може залучатись до виконання робіт із забезпечення кіберзахисту? Ким можуть бути викладені вимоги у випадку укладення договору?
		ID.GV-3	Чи дотримуються національні європейські норми при узагальненні та виконанні нормативно-правових та нормативних вимог щодо кібербезпеки?

Продовження табл. 3

Фрагмент системи заходів кіберзахисту			
Категорія ЗКЗ	Опис	ЗКЗ	Опис
Клас ЗКЗ «Відновлення стану кібербезпеки» (RC)			
		ID.GV-4	Для чого складаються переліки суттєвих загроз, вразливостей, через які загрози можуть бути реалізовано? Що рекомендується оцінювати під час проведення аудиту інформаційної безпеки ОКІ або державної експертизи КСЗІ ОКІІ ОКІ?
ID.RA «Оцінка ризиків»	Визначення ризиків у сфері кібербезпеки для процесів надання життєво важливих послуг та функцій, а також активів організації.	ID.RA-1	Для чого відбувається процес управління вразливістю та як оцінюються і виправляються виявлені вразливості?
		ID.RA-2	З ким встановлює контакти організація?
		ID.RA-3	Відповідно чого організація визначає та документує можливі загрози?
		ID.RA-4	Чи виконується оцінка збитків, що можуть бути нанесені ОКІ внаслідок реалізації загроз?
		ID.RA-5	Що визначають критерії, які визначає організація у методології управління ризиками?
		ID.RA-6	Що впроваджує організація на підставі визначеної методології?
ID.RM «Стратегія управління ризиками організації»	Визначення пріоритетів, обмежень, допустимого рівня ризику для підтримки рішень щодо зниження ризиків кібербезпеки.	ID.RM-1	Чим керується організація при забезпеченні визначення процесу управління ризиками? Що забезпечує організація відповідно до стратегії управління ризиками?
		ID.RM-2	Що формулює в методології організація?
		ID.RM-3	Що враховує організація при визначенні порядку обробки ризиків?
ID.SC «Управління ризиками системи постачання»	Визначення пріоритетів, обмежень, допустимого рівня ризику щодо системи постачання для підтримки рішень щодо ризиків, пов’язаних із системою постачання послуг третіми особами.	ID.SC-1	Що використовує організація при проведенні аудиту постачальників товарів і послуг?
		ID.SC-2	Як класифікує своїх постачальників товарів і послуг для ОКІ організація?
		ID.SC-3	Які вимоги можуть бути вказані у випадку укладення договору з постачальниками товарів і послуг?
		ID.SC-4	З якою метою проводиться відстеження ринку постачальників товарів і послуг, партнерів та проводить аудит? Що є необхідним у наданні послуг постачальникам та партнерам?
		ID.SC-5	З якою метою організація визначає, які постачальники братимуть участь у опрацюванні заходів реагування та планах відновлення?
…	…	…	…

Закінчення табл. 3

Фрагмент системи заходів кіберзахисту			
Категорія ЗКЗ	Опис	ЗКЗ	Опис
Клас ЗКЗ «Відновлення стану кібербезпеки» (RC)			
RC.RP «Планування»	Процеси та процедури відновлення виконуються та підтримуються з метою своєчасного відновлення систем або активів, постраждалих від кіберінцидентів.	RC.RP-1	З якою метою організація розробляє свій план ліквідації наслідків кібер-інцидентів?
RC.IM «Удосконалення»	Планування відновлення та процеси відновлення удосконалюються шляхом урахування отриманого досвіду.	RC.IM-1	Чи забезпечує організація, щоб плани відновлення оновлювались з урахуванням заходів, прийнятих на основі накопиченого досвіду?
		RC.IM-2	Чи оновлюються плани відновлення у разі виникнення інцидентів з урахуванням внутрішніх змін?
RC.CO «Комунікації»	Заходи з відновлення координуються з внутрішніми та зовнішніми партнерами організації, такими як координаційні центри, постачальники електронних комунікаційних мереж та/або послуг, власники атакуючих систем, інші групи реагування на інциденти, пов'язані з інформаційною та/або кібербезпекою (CSIRT).	RC.CO-1	Яким чином надається інформація організацією?
		RC.CO-2	З якою метою організація оглядає і коригує політику, принципи, стандарти, методологію і процедури?
		RC.CO-3	Чи забезпечує організація інформування внутрішніх і зовнішніх партнерів про серйозні кіберінциденти?

Виконаємо формування еталонів НЧ для ЛЗ ***ACM*** за допомогою (7) – (10):

$b_{11} = SC(M_1 - CF(\text{ACM}_2 - \text{ACM}_1) - SP) = 0$; $b_{21} = SC(M_1 + CF(\text{ACM}_2 - \text{ACM}) - SP) = 0$

і т.д. $a_1 = 0$; $a_2 = b_{21} = 0$; $a_3 = 37{,}5$; $a_4 = 87{,}5$; $c_1 = b_{12} = 12{,}5$; $c_2 = 62{,}5$; $c_3 = 100$; $c_4 = 100$.

Графічна інтерпретація сформованих різнорідно розподілених НЧ $\underset{\sim}{T}^{(4)}_{\text{ACM}}$ наведена на рис. 1, де $\underset{\sim}{T}_{\text{ACM}_1}$, $\underset{\sim}{T}_{\text{ACM}_2}$, $\underset{\sim}{T}_{\text{ACM}_3}$ *та* $\underset{\sim}{T}_{\text{ACM}_4}$ відповідно відображають – «НЕ ПОТРЕБУЄТЬСЯ (НП)»; «РОЗГЛЯДАЄТЬСЯ ДЛЯ РЕАЛІЗАЦІЇ (РД)», «У ПРОЦЕСІ (ПР)» та «РЕАЛІЗОВАНО (РЛ)».

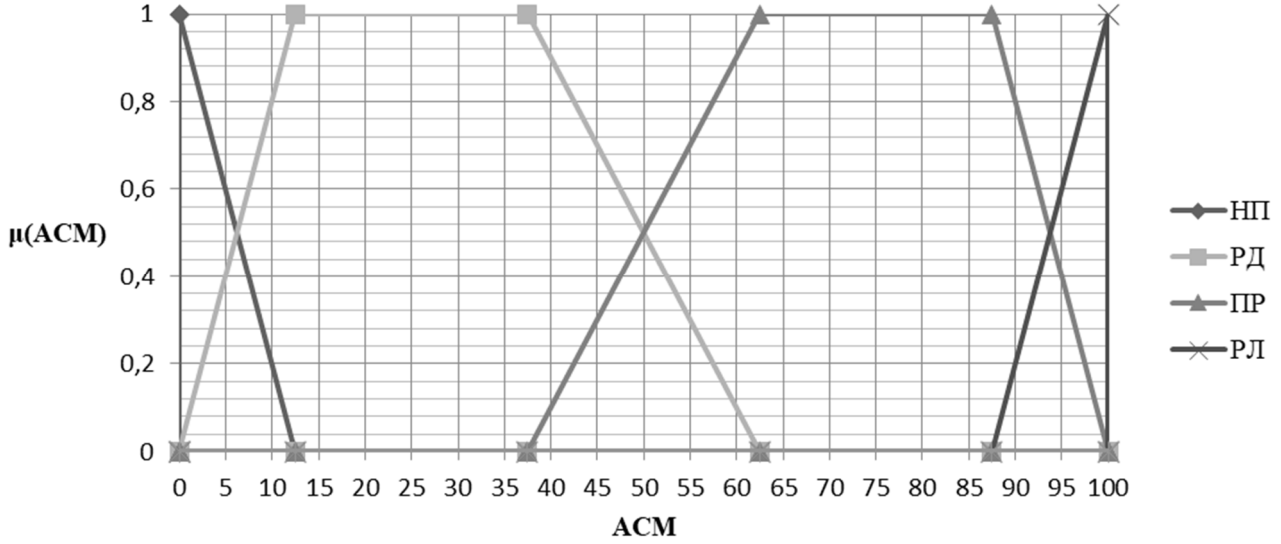

Рис. 1. Терми значень сформованих різнорідно розподілених НЧ для ЛЗ ***ACM*** $\underset{\sim}{T}^{(4)}_{\text{ACM}}$, де відповідно «НП» – «НЕ ПОТРЕБУЄТЬСЯ»; «РД» – «РОЗГЛЯДАЄТЬСЯ ДЛЯ РЕАЛІЗАЦІЇ»; «ПР» – «У ПРОЦЕСІ»; «РЛ» – «РЕАЛІЗОВАНО»

Етап 3. Формування множини характеристик об'єктів огляду

Введемо множину характеристик, що відображають стан заходів кіберзахисту (СЗКЗ) об'єктів огляду [4]

$$\widetilde{\boldsymbol{E}} = \left\{ \bigcup_{q=1}^{m} \tilde{E}^q \right\} = \{\tilde{E}^1, \tilde{E}^2, \dots \tilde{E}^m\}, \qquad (11)$$

де $\tilde{E}^q \subseteq \widetilde{\boldsymbol{E}}\left(q = \overline{1,m}\right)$ НЧ, що характеризує q-ий об'єкт огляду, а m – їх кількість.

Наприклад, при $m = 3$, а $\tilde{E}^1 = \tilde{E}^{\text{АС}}$ = «СК АТОМНОЇ СТАНЦІЇ», $\tilde{E}^2 = \tilde{E}^{\text{АП}}$ = «СК АЕРОПОРТУ» та $\tilde{E}^3 = \tilde{E}^{\text{НПЗ}}$ = «СК НАФТОПЕРЕРОБНОГО ЗАВОДУ», де $\tilde{E}^{\text{АС}}$, $\tilde{E}^{\text{АП}}$ та $\tilde{E}^{\text{НПЗ}}$ – НЧ, що характеризують відповідні об'єкти огляду критичної інфраструктури.

Тоді формулу (11) запишемо як:

$$\widetilde{\boldsymbol{E}}^{\boldsymbol{q}} = \left\{ \bigcup_{q=1}^{3} \tilde{E}^q \right\} = \left\{\tilde{E}^1, \tilde{E}^2, \tilde{E}^3\right\} = \\ = \{\tilde{E}^{\text{АС}}, \tilde{E}^{\text{АП}}, \tilde{E}^{\text{НПЗ}}\}. \qquad (12)$$

Множини системи характеристик q-го об'єкта огляду, яка охоплює класи ЗКЗ відобразимо як:

$$ACM^q = \left\{ \bigcup_{i=1}^{\eta} ACM_i^q \right\} = \\ = \left\{ACM, ACM_2^q, \dots, ACM_\eta^q\right\}, \qquad (13)$$

де $ACM_i^q \subseteq ACM^q\left(i = \overline{1,\eta}\right)$ – ідентифікатор i-го класу ЗКЗ, η – їх кількість, а $q = \overline{1,m}$ (m – кількість об'єктів огляду (див. [4])).

Наприклад, при η =5 з урахуванням класів ЗКЗ (див. табл. 1) формулу (13) запишемо як:

$$ACM^q = \left\{ \bigcup_{i=1}^{\eta} ACM_i^q \right\} = \\ = \left\{ACM_1^q, ACM_2^q, ACM_3^q, ACM_4^q, ACM_5^q\right\} = \\ = \{ID, PR, DE, RS, RC\} =$$

$= \{$*"ІДЕНТИФІКАЦІЯ РИЗИКІВ КІБЕРБЕЗПЕКИ", "КІБЕРЗАХИСТ", "ВИЯВЛЕННЯ КІБЕРІНЦИДЕНТІВ", "РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ", "ВІДНОВЛЕННЯ СТАНУ КІБЕРБЕЗПЕКИ"*$\}$,

де ACM_1^q=*ID="ІДЕНТИФІКАЦІЯ РИЗИКІВ КІБЕРБЕЗПЕКИ"*, ", ACM_2^q=*PR="КІБЕРЗАХИСТ"*, ACM_3^q=*DE="ВИЯВЛЕННЯ КІБЕРІНЦИДЕНТІВ"*, ACM_4^q=*RS= "РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ"*, ACM_5^q=*RC="ВІДНОВЛЕННЯ СТАНУ КІБЕРБЕЗПЕКИ"*.

Наприклад, з урахуванням [5] та фрагменту табл. 3 для методики оцінювання організації діяльності щодо кіберзахисту при η=5, k_1= k_2=6, k_3= k_5=3, k_4=5 формулу (13) запишемо як:

$$ACM^q = \left\{ \bigcup_{i=1}^{\eta} \left\{ \bigcup_{j=1}^{k_i} ACM_{ij}^q \right\} \right\} = \begin{Bmatrix} \{ACM_{11}^q, ACM_{12}^q, \dots ACM_{16}^q\}, \\ \{ACM_{21}^q, ACM_{22}^q, \dots, ACM_{26}^q\}, \\ \{ACM_{31}^q, ACM_{32}^q, ACM_{33}^q\} \\ \{ACM_{41}^q, ACM_{42}^q, \dots, ACM_{45}^q\}, \\ \{ACM_{51}^q, \text{СМС}_{52}^q, \text{СМС}_{53}^q\} \end{Bmatrix} =$$

$$= \begin{Bmatrix} \{ID.AM_1^q, ID.BE_2^q, ID.GV_3^q, ID.RA_4^q, ID.RM_5^q, ID.SC_6^q\}, \\ \{PR.AC_1^q, PR.AT_2^q, PR.DS_3^q, PR.IP_4^q, PR.MA_5^q, PR.PT_6^q\}, \\ \{DE.AE_1^q, DE.CM_2^q, DE.DP_3^q\}, \\ \{RS.RP_1^q, RS.CO_2^q, RS.MI_3^q, RS.IM_4^q\}, \\ \{RC.RP_1^q, RC.IM_2^q, RC.CO_3^q\} \end{Bmatrix},$$

де, наприклад, ACM_{11}^q =$ID.AM_1^q$=«УПРАВЛІННЯ АКТИВАМИ», ACM_{12}^q = $ID.AM_2^q$= «СЕРЕДОВИЩЕ НАДАННЯ ЖИТТЄВО ВАЖЛИВИХ ПОСЛУГ ТА ФУНКЦІЙ», ACM_{16}^q = $ID.AM_6^q$= «УПРАВЛІННЯ РИЗИКАМИ СИСТЕМИ ПОСТАЧАННЯ». Аналогічно на підставі табл. 3 визначаються ACM_{21}^q, ACM_{22}^q … ACM_{53}^q.

Далі, надамо величину, що відображає стан виконання заходів кіберзахисту q-го об'єкту огляду критичної інфраструктури держави:

$$\tilde{E}^{\boldsymbol{q}} = \frac{\sum_{i=1}^{\eta} \widetilde{ACM}_{iJ}^q}{\eta} = \\ = (\widetilde{ACM}_1^q \oplus \widetilde{ACM}_2^q \oplus \dots \oplus \widetilde{ACM}_n^q)/\eta, \qquad (14)$$

де $\widetilde{ACM_i^q}\left(i=\overline{1,\eta}\right)$ i-й клас заходів кіберзахисту q-го об'єкту огляду (визначається НЧ), η – кількість категорій [5], а $\widetilde{\oplus}$ – нечітка сума [6].

Етап 4. Визначення поточних значень характеристик об'єктів огляду

Кожний i-й клас ЗКЗ q-го об'єкту огляду визначається за формулою:

$$\widetilde{ACM_i^q}=\frac{\sum_{j=1}^{k_i}ACM_{ij}^q}{k_i}= \\ =(\widetilde{ACM}_{i1}^q\ \widetilde{\oplus}\ \widetilde{ACM}_{i2}^q\ \widetilde{\oplus}\ \dots\widetilde{\oplus}\ \widetilde{ACM}_{ik_i}^q)/k_i,(j=\overline{1,k_i}). \quad (15)$$

З урахуванням (14) вираз (15) запишемо в наступному вигляді:

$$\tilde{E}^{\boldsymbol{q}}=\widetilde{ACM}_i^q=(\sum_{i=1}^{\eta}(\sum_{j=1}^{k_i}\widetilde{ACM}_{ij}^q)/k_i)/\eta= \\ =((\sum_{j=1}^{k1}\widetilde{ACM}_{1j}^q)/k_1\ \widetilde{\oplus}\ (\sum_{j=1}^{k2}\widetilde{ACM}_{2j}^q)/k_2\ \widetilde{\oplus}\ \dots\widetilde{\oplus}\ (\sum_{j=1}^{k\eta}\widetilde{ACM}_{nj}^q)/k_n)/\eta= \\ =((\widetilde{ACM}_{11}^q\ \widetilde{\oplus}\ \widetilde{ACM}_{12}^q\ \widetilde{\oplus}\dots\widetilde{\oplus}\ \widetilde{ACM}_{1k_1}^q)/k_1\ \widetilde{\oplus}= \\ =(\widetilde{ACM}_{21}^q\ \widetilde{\oplus}\ \widetilde{ACM}_{22}^q\ \widetilde{\oplus}\ \dots\widetilde{\oplus}\ \widetilde{ACM}_{2k_2}^q)/k_2\ \widetilde{\oplus}= \\ \dots \\ =(\widetilde{ACM}_{n1}^q\ \widetilde{\oplus}\ \widetilde{ACM}_{n2}^q\ \widetilde{\oplus}\dots\widetilde{\oplus}\ \widetilde{ACM}_{nk_n}^q)/k_n)/n. \quad (16)$$

Наприклад, при $q=1$, $\eta=5$, $k_1=k_2=6$, $k_3=k_5=3$, $k_4=5$, $\widetilde{ACM_i^1}=\widetilde{ACM_i^{\mathrm{AC}}}$ вираз (16) запишемо в наступному вигляді

$$\tilde{E}^{\boldsymbol{1}}=\tilde{E}^{\mathrm{AC}}=\left\{\sum_{i=1}^{5}(\sum_{j=1}^{k_i}\widetilde{ACM}_{ij}^1)/k_i\right\}=\left\{\sum_{i=1}^{5}(\sum_{j=1}^{k_i}\widetilde{ACM}_{ij}^{\mathrm{AC}})/k_i\right\}= \\ =(\sum_{j=1}^{9}\widetilde{ACM}_{1j}^{\mathrm{AC}}/6\ \widetilde{\oplus}\ \sum_{j=1}^{2}\widetilde{ACM}_{2j}^{\mathrm{AC}}/6\ \widetilde{\oplus}\sum_{j=1}^{9}\widetilde{ACM}_{3j}^{\mathrm{AC}}/3\ \widetilde{\oplus}\ \sum_{j=1}^{5}\widetilde{ACM}_{4j}^{\mathrm{AC}}/5\ \widetilde{\oplus}\sum_{j=1}^{3}\widetilde{ACM}_{5j}^{\mathrm{AC}}/3)/5,$$

де

$$\widetilde{ACM}_1^{AC}=(\sum_{j=1}^{6}\widetilde{ACM}_{1j}^{\mathrm{AC}})/6=(\sum_{j=1}^{6}\widetilde{ID}_{1j}^{AC})/6= \\ =\widetilde{ID.AM}_{11}\ \widetilde{\oplus}\ \widetilde{ID.BE}_{12}\ \widetilde{\oplus}\ \widetilde{ID.GV}_{13}\ \widetilde{\oplus}\ \dots\widetilde{\oplus}\ \widetilde{ID.SC}_{16})/6= \\ =((\widetilde{ID.AM}-1\ \widetilde{\oplus}\ \widetilde{ID.AM}-2\ \widetilde{\oplus}\ \widetilde{ID.AM}-3\ \widetilde{\oplus}\ \widetilde{ID.AM}-4\ \widetilde{\oplus}\ \widetilde{ID.AM}-5\ \widetilde{\oplus}= \\ =\widetilde{ID.AM}-6)/6\ \widetilde{\oplus}\ (\widetilde{ID.BE}-1\ \widetilde{\oplus}\ \widetilde{ID.BE}-2\ \widetilde{\oplus}\ \widetilde{ID.BE}-3\ \widetilde{\oplus}\ \widetilde{ID.BE}-4\ \widetilde{\oplus}= \\ =\widetilde{ID.AB}-5)/5\ \widetilde{\oplus}\ (\widetilde{ID.GV}-1\ \widetilde{\oplus}\ \widetilde{ID.GV}-2\ \widetilde{\oplus}\ \widetilde{ID.GV}-3\ \widetilde{\oplus}= \\ =\widetilde{ID.GV}-4)/4\ \widetilde{\oplus}\ (\widetilde{ID.AM}-1\ \widetilde{\oplus}\ \widetilde{ID.RA}-2\ \widetilde{\oplus}\ \widetilde{ID.RA}-3\ \oplus= \\ =\widetilde{ID.RA}-4\ \widetilde{\oplus}\ \widetilde{ID.RA}-5\ \widetilde{\oplus}\ \widetilde{ID.RA}-6)/6\ \widetilde{\oplus}\ (\widetilde{ID.RM}-1\ \widetilde{\oplus}\ \widetilde{ID.RM}-2\ \widetilde{\oplus}= \\ =\widetilde{ID.RM}-3)/3\ \widetilde{\oplus}\ (\widetilde{ID.SC}-1\ \widetilde{\oplus}\ \widetilde{ID.SC}-2\ \widetilde{\oplus}\ \widetilde{ID.SC}-3\ \widetilde{\oplus}= \\ =\widetilde{ID.SC}-4\ \widetilde{\oplus}\ \widetilde{ID.SC}-5)/5)/6;$$

$$\widetilde{ACM}_2^{AC}=(\sum_{j=1}^{6}\widetilde{ACM}_{2j}^{\mathrm{AC}})/2=(\sum_{j=1}^{6}\widetilde{PR}_{2j}^{AC})/6= \\ (\widetilde{PR.AC}_{21}\ \widetilde{\oplus}\ \widetilde{PR.AT}_{22}\ \widetilde{\oplus}\ PR.DS_{23}\ \widetilde{\oplus}\ \dots\widetilde{\oplus}\ \widetilde{PR.PT}_{26})/6= \\ =((\widetilde{PR.PS}-1\ \widetilde{\oplus}\ \widetilde{PR.PS}-2\ \widetilde{\oplus}\ \widetilde{PR.PS}-3\ \widetilde{\oplus}\ \widetilde{PR.PS}-4\ \widetilde{\oplus}\ \widetilde{PR.PS}-5\ \widetilde{\oplus}\ \widetilde{PR.PS}-6\ \widetilde{\oplus}= \\ =\widetilde{PR.PS}-7)/7\ \widetilde{\oplus}\ (\widetilde{PR.AT}-1\ \widetilde{\oplus}\ \widetilde{PR.AT}-2\ \widetilde{\oplus}\ \widetilde{PR.AT}-3\ \widetilde{\oplus}\ \widetilde{PR.AT}-4\ \widetilde{\oplus}= \\ =\widetilde{PR.AT}-5)/5\ \widetilde{\oplus}\ (\widetilde{PR.DS}-1\ \widetilde{\oplus}\ \widetilde{PR.DS}-2\ \widetilde{\oplus}\ \widetilde{PR.DS}-3\ \widetilde{\oplus}\ \widetilde{PR.DS}-4\ \widetilde{\oplus}\ \widetilde{PR.DS}-5\ \widetilde{\oplus}= \\ =\widetilde{PR.DS}-6\ \widetilde{\oplus}\ \widetilde{PR.DS}-7\ \widetilde{\oplus}\ \widetilde{PR.DS}-8)/8\ \widetilde{\oplus}= \\ =(\widetilde{PR.IP}-1\ \widetilde{\oplus}\ \widetilde{PR.IP}-2\ \widetilde{\oplus}\ \widetilde{PR.IP}-3\ \widetilde{\oplus}\ \widetilde{PR.IP}-4\ \widetilde{\oplus}\ \widetilde{PR.IP}-5\ \widetilde{\oplus}= \\ =\widetilde{PR.IP}-6\ \widetilde{\oplus}\ \widetilde{PR.IP}-7\ \widetilde{\oplus}\ \widetilde{PR.IP}-8\ \widetilde{\oplus}\ \widetilde{PR.IP}-9\ \widetilde{\oplus}\ \widetilde{PR.IP}-10\ \widetilde{\oplus}= \\ =\widetilde{PR.IP}-11\ \widetilde{\oplus}\ \widetilde{PR.IP}-12)^{\frac{\widetilde{\oplus}(\widetilde{PR.MA}-1\widetilde{\oplus}\widetilde{PR.MA}-2)}{12}}= \\ =(\widetilde{PR.RT}-1\ \widetilde{\oplus}\ \widetilde{PR.RT}-2\ \widetilde{\oplus}\ \widetilde{PR.RT}-3\ \widetilde{\oplus}\ \widetilde{PR.RT}-4\ \widetilde{\oplus}\ \widetilde{PR.RT}-5)/5)/6;$$

$$\widetilde{ACM}_3^{AC} = (\sum_{j=1}^{3} \widetilde{ACM}_{3j}^{AC})/2 = (\sum_{j=1}^{3} \widetilde{DE}_{3j}^{AC})/3 \quad = (\widetilde{DE.AE}_{31} \widetilde{\oplus} \widetilde{DE.CM}_{32} \widetilde{\oplus} \widetilde{DE.DP}_{33})/3 =$$
$$= ((\widetilde{DE.AE} - 1 \widetilde{\oplus} \widetilde{DE.AE} - 2 \widetilde{\oplus} \widetilde{DE.AE} - 3 \widetilde{\oplus} \widetilde{DE.AE} - 4 \widetilde{\oplus} \widetilde{DE.AE} - 5)/$$
$$5 \widetilde{\oplus} (\widetilde{DE.CM} - 1 \widetilde{\oplus} \widetilde{DE.CM} - 2 \widetilde{\oplus} \widetilde{DE.CM} - 3 \widetilde{\oplus} \widetilde{DE.CM} - 4 \widetilde{\oplus} \widetilde{DE.CM} - 5 \widetilde{\oplus}$$
$$\widetilde{DE.CM} - 6 \widetilde{\oplus} \widetilde{DE.CM} - 7 \widetilde{\oplus} \widetilde{DE.CM} - 8)/$$
$$8 \widetilde{\oplus} (\widetilde{DE.DP} - 1 \widetilde{\oplus} \widetilde{DE.DP} - 2 \widetilde{\oplus} \widetilde{DE.DP} - 3 \widetilde{\oplus} \widetilde{DE.DP} - 4 \widetilde{\oplus} \widetilde{DE.DP} - 5)/5\ )/3;$$

$$\widetilde{ACM}_4^{AC} = (\sum_{j=1}^{5} \widetilde{ACM}_{4j}^{AC})/5 = (\sum_{j=1}^{5} \widetilde{RS}_{4j}^{AC})/5 =$$
$$= (\widetilde{RS.RP}_{41} \widetilde{\oplus} \widetilde{RS.CO}_{42} \widetilde{\oplus} \widetilde{RS.AN}_{43} \widetilde{\oplus} \dots \widetilde{\oplus} \widetilde{RS.IM}_{45})/5 =$$
$$= ((\widetilde{RS.RP} - 1) \widetilde{\oplus} (\widetilde{RS.CO} - 1 \widetilde{\oplus} \widetilde{RS.CO} - 2 \widetilde{\oplus} \widetilde{RS.CO} - 3 \widetilde{\oplus} \widetilde{RS.CO} - 4 \widetilde{\oplus} =$$
$$= \widetilde{RS.CO} - 5)/5 \widetilde{\oplus} (\widetilde{RS.AN} - 1 \widetilde{\oplus} \widetilde{RS.AN} - 2 \widetilde{\oplus} \widetilde{RS.AN} - 3 \widetilde{\oplus} \widetilde{RS.AN} - 4 \widetilde{\oplus} =$$
$$= \widetilde{RS.AN} - 5)/5 \widetilde{\oplus} (\widetilde{RS.MI} - 1 \widetilde{\oplus} \widetilde{RS.MI} - 2 \widetilde{\oplus} \widetilde{RS.MI} - 3)/3 \widetilde{\oplus} =$$
$$= (\widetilde{RS.IM} - 1 \widetilde{\oplus} \widetilde{RS.IM} - 2)/2)/5.$$

Для $\widetilde{\text{ACM}}_1^{AC}$ $-$ ***ID*** "ІДЕНТИФІКАЦІЯ РИЗИКІВ КІБЕРЗАХИСТУ"**:**

$\widetilde{ID.AM}$ «УПРАВЛІННЯ АКТИВАМИ» –
$\widetilde{ID.AM} - 1$ = «НП» = $(0;0;0;12{,}5)_{\text{LR}}$,
$\widetilde{ID.AM} - 2$= «РД» = $(0;12{,}5;37{,}5;62{,}5)_{\text{LR}}$,
$\widetilde{ID.AM} - 3$= «РД» = $(0;12{,}5;37{,}5;62{,}5)_{\text{LR}}$,
$\widetilde{ID.AM} - 4$= «ПР» = $(37{,}5;62{,}5;87{,}5;100)_{\text{LR}}$,
$\widetilde{ID.AM} - 5$= «ПР» = $(37{,}5;62{,}5;87{,}5;100)_{\text{LR}}$,
$\widetilde{ID.AM} - 6$= «ПР» = $(37{,}5;62{,}5;87{,}5;100)_{\text{LR}}$;
$\widetilde{ID.BE}$ «СЕРЕДОВИЩЕ НАДАННЯ ЖИТТЕВО ВАЖЛИВИХ ПОСЛУГ ТА ФУНКЦІЙ» –
$\widetilde{ID.BE} - 1$ = «РД» = $(0;12{,}5;37{,}5;62{,}5)_{\text{LR}}$,
$\widetilde{ID.BE} - 2$= «РД» = $(0;12{,}5;37{,}5;62{,}5)_{\text{LR}}$,
$\widetilde{ID.BE} - 3$= «РД» = $(0;12{,}5;37{,}5;62{,}5)_{\text{LR}}$,
$\widetilde{ID.BE} - 4$= «ПР» = $(37{,}5;62{,}5;87{,}5;100)_{\text{LR}}$,
$\widetilde{ID.BE} - 5$= «РД» = $(0;12{,}5;37{,}5;62{,}5)_{\text{LR}}$;
$\widetilde{ID.GV}$ «УПРАВЛІННЯ БЕЗПЕКОЮ» –
$\widetilde{ID.GV} - 1$ = «НП» = $(0;0;0;12{,}5)_{\text{LR}}$,
$\widetilde{ID.GV} - 2$= «РД» = $(0;12{,}5;37{,}5;62{,}5)_{\text{LR}}$,
$\widetilde{ID.GV} - 3$= «ПР» = $(37{,}5;62{,}5;87{,}5;100)_{\text{LR}}$,
$\widetilde{ID.GV} - 4$= «ПР» = $(37{,}5;62{,}5;87{,}5;100)_{\text{LR}}$;
$\widetilde{ID.RA}$ «ОЦІНКА РИЗИКІВ» –
$\widetilde{ID.RA} - 1$ = «НП» = $(0;0;0;12{,}5)_{\text{LR}}$,
$\widetilde{ID.RA} - 2$= «РД» = $(0;12{,}5;37{,}5;62{,}5)_{\text{LR}}$,
$\widetilde{ID.RA} - 3$= «РД» = $(0;12{,}5;37{,}5;62{,}5)_{\text{LR}}$,
$\widetilde{ID.RA} - 4$= «ПР» = $(37{,}5;62{,}5;87{,}5;100)_{\text{LR}}$,
$\widetilde{ID.RA} - 5$= «РЛ» = $(87{,}5;100;100;100)_{\text{LR}}$,
$\widetilde{ID.RA} - 6$= «ПР» = $(37{,}5;62{,}5;87{,}5;100)_{\text{LR}}$;
$\widetilde{ID.RM}$ «СТРАТЕГІЯ УПРАВЛІННЯ РИЗИКАМИ ОРГАНІЗАЦІЇ» –
$\widetilde{ID.RM} - 2$= «НП» = $(0;0;0;12{,}5)_{\text{LR}}$,
$\widetilde{ID.RM} - 3$= «РД» = $(0;12{,}5;37{,}5;62{,}5)_{\text{LR}}$,
$\widetilde{ID.RM} - 4$= «РД» = $(0;12{,}5;37{,}5;62{,}5)_{\text{LR}}$;
$\widetilde{ID.SC}$ «УПРАВЛІННЯ РИЗИКАМИ СИСТЕМИ ПОСТАЧАННЯ» –
$\widetilde{ID.SC} - 1$ = «НП» = $(0;0;0;12{,}5)_{\text{LR}}$,
$\widetilde{ID.SC} - 2$= «РД» = $(0;12{,}5;37{,}5;62{,}5)_{\text{LR}}$,
$\widetilde{ID.SC} - 3$= «РД» = $(0;12{,}5;37{,}5;62{,}5)_{\text{LR}}$,
$\widetilde{ID.SC} - 4$= «РЛ» = $(87{,}5;100;100;100)_{\text{LR}}$,
$\widetilde{ID.SC} - 5$= «ПР» = $(37{,}5;62{,}5;87{,}5;100)_{\text{LR}}$.

Для $\widetilde{\text{АСМ}}_2^{AC}$ $-$ ***PR*** "КІБЕРЗАХИСТ"**:**

$\widetilde{PR.AC}$ «УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ, АВТЕНТИФІКАЦІЄЮ ТА КОНТРОЛЬ ДОСТУПУ» –

$PR.\widetilde{AC} - 1$ = «НП» = $(0;0;\ 0;\ 12{,}5)_{\text{LR}}$,

$PR.\widetilde{AC} - 2$= «РД» = $(0;\ 12{,}5;37{,}5;\ 62{,}5)_{\text{LR}}$,

$PR.\widetilde{AC} - 3$= «РД» = $(0;\ 12{,}5;37{,}5;\ 62{,}5)_{\text{LR}}$,

$PR.\widetilde{AC} - 4$= «РЛ» = $(87{,}5;\ 100;\ 100;\ 100)_{\text{LR}}$,

$PR.\widetilde{AC} - 5$= «ПР» = $(37{,}5;\ 62{,}5;\ 87{,}5;\ 100)_{\text{LR}}$,

$PR.\widetilde{AC} - 6$= «НП» = $(0;0;\ 0;\ 12{,}5)_{\text{LR}}$,

$PR.\widetilde{AC} - 7$= «РД» = $(0;\ 12{,}5;37{,}5;\ 62{,}5)_{\text{LR}}$;

$\widetilde{PR.AT}$ «ОБІЗНАНІСТЬ ТА НАВЧАННЯ» –

$PR.\widetilde{AT} - 1$ = «НП» = $(0;0;\ 0;\ 12{,}5)_{\text{LR}}$,

$PR.\widetilde{AT} - 2$= «РД» = $(0;\ 12{,}5;37{,}5;\ 62{,}5)_{\text{LR}}$,

$PR.\widetilde{AT} - 3$= «РЛ» = $(87{,}5;\ 100;\ 100;\ 100)_{\text{LR}}$,

$PR.\widetilde{AT} - 4$= «РЛ» = $(87{,}5;\ 100;\ 100;\ 100)_{\text{LR}}$,

$PR.\widetilde{AT} - 5$= «ПР» = $(37{,}5;\ 62{,}5;\ 87{,}5;\ 100)_{\text{LR}}$;

$\widetilde{PR.DS}$ «БЕЗПЕКА ДАНИХ» –

$PR.\widetilde{DS} - 1$ = «НП» = $(0;0;\ 0;\ 12{,}5)_{\text{LR}}$,

$PR.\widetilde{DS} - 2$= «РД» = $(0;\ 12{,}5;37{,}5;\ 62{,}5)_{\text{LR}}$,

$PR.\widetilde{DS} - 3$= «НП» = $(0;0;\ 0;\ 12{,}5)_{\text{LR}}$,

$PR.\widetilde{DS} - 4$= «РД» = $(0;\ 12{,}5;37{,}5;\ 62{,}5)_{\text{LR}}$,

$PR.\widetilde{DS} - 5$= «ПР» = $(37{,}5;\ 62{,}5;\ 87{,}5;\ 100)_{\text{LR}}$,

$PR.\widetilde{DS} - 6$= «НП» = $(0;0;\ 0;\ 12{,}5)_{\text{LR}}$,

$PR.\widetilde{DS} - 7$= «РД» = $(0;\ 12{,}5;37{,}5;\ 62{,}5)_{\text{LR}}$,

$PR.\widetilde{DS} - 8$= «РЛ» = $(87{,}5;\ 100;\ 100;\ 100)_{\text{LR}}$;

$\widetilde{PR.IP}$ «ПРОЦЕСИ ТА ПРОЦЕДУРИ КІБЕРЗАХИСТУ» –

$PR.\widetilde{IP} - 1$ = «НП» = $(0;0;\ 0;\ 12{,}5)_{\text{LR}}$,

$PR.\widetilde{IP} - 2$= «РД» = $(0;\ 12{,}5;37{,}5;\ 62{,}5)_{\text{LR}}$,

$PR.\widetilde{IP} - 3$= «РД» = $(0;\ 12{,}5;37{,}5;\ 62{,}5)_{\text{LR}}$,

$PR.\widetilde{IP} - 4$= «ПР» = $(37{,}5;\ 62{,}5;\ 87{,}5;\ 100)_{\text{LR}}$,

$PR.\widetilde{IP} - 5$= «РЛ» = $(87{,}5;\ 100;\ 100;\ 100)_{\text{LR}}$,

$PR.\widetilde{IP} - 6$= «РЛ» = $(87{,}5;\ 100;\ 100;\ 100)_{\text{LR}}$,

$PR.\widetilde{IP} - 7$= «РЛ» = $(87{,}5;\ 100;\ 100;\ 100)_{\text{LR}}$,

$PR.\widetilde{IP} - 8$= «ПР» = $(37{,}5;\ 62{,}5;\ 87{,}5;\ 100)_{\text{LR}}$,

$PR.\widetilde{IP} - 9$ = «НП» = $(0;0;\ 0;\ 12{,}5)_{\text{LR}}$,

$PR.\widetilde{IP} - 10$= = «РД» = $(0;\ 12{,}5;37{,}5;\ 62{,}5)_{\text{LR}}$,

$PR.\widetilde{IP} - 11$= «РД» = $(0;\ 12{,}5;37{,}5;\ 62{,}5)_{\text{LR}}$,

$PR.\widetilde{IP} - 12$= «РЛ» = $(87{,}5;\ 100;\ 100;\ 100)_{\text{LR}}$;

$\widetilde{PR.MA}$ «ТЕХНІЧНЕ ОБСЛУГОВУВАННЯ» –

$PR.\widetilde{MA} - 1$= «РЛ» = $(87{,}5;\ 100;\ 100;\ 100)_{\text{LR}}$,

$PR.\widetilde{MA} - 2$= «ПР» = $(37{,}5;\ 62{,}5;\ 87{,}5;\ 100)_{\text{LR}}$;

$\widetilde{PR.PT}$ «ТЕХНОЛОГІЇ КІБЕРЗАХИСТУ» –

$PR.\widetilde{PT} - 1$= «НП» = $(0;0;\ 0;\ 12{,}5)_{\text{LR}}$,

$PR.\widetilde{PT} - 2$= = «РД» = $(0;\ 12{,}5;37{,}5;\ 62{,}5)_{\text{LR}}$,

$PR.\widetilde{PT} - 3$= «НП» = $(0;0;\ 0;\ 12{,}5)_{\text{LR}}$,

$PR.\widetilde{PT} - 4$= «РЛ» = $(87{,}5;\ 100;\ 100;\ 100)_{\text{LR}}$,

$PR.\widetilde{PT} - 5$= «РЛ» = $(87{,}5;\ 100;\ 100;\ 100)_{\text{LR}}$.

ДЛЯ $\widetilde{\text{АСМ}}_3^{AC}$ $-$ ***DE*** "ВИЯВЛЕННЯ КІБЕРІНЦИДЕНТІВ"**:**

$\widetilde{DE.AE}$ «АНОМАЛІЇ ТА КІБЕРІНЦИДЕНТИ» –

$DE.\widetilde{AE} - 1$= «РД» = $(0;\ 12{,}5;37{,}5;\ 62{,}5)_{\text{LR}}$,

$DE.\widetilde{AE} - 2$= «НП» = $(0;0;\ 0;\ 12{,}5)_{\text{LR}}$,

$\widetilde{DE.AE}$ – 3= «РД» = (0; 12,5;37,5; 62,5) LR,
$\widetilde{DE.AE}$ – 4= «НП» = (0;0; 0; 12,5) LR,
$\widetilde{DE.AE}$ – 5= «РЛ» = (87,5; 100; 100; 100) LR;
$\widetilde{DE.CM}$ «БЕЗПЕРЕРВНИЙ МОНІТОРИНГ КІБЕРБЕЗПЕКИ» –
$\widetilde{DE.CM}$ – 1= «РД» = (0; 12,5;37,5; 62,5) LR,
$\widetilde{DE.CM}$ – 2= «РЛ» = (87,5; 100; 100; 100) LR,
$\widetilde{DE.CM}$ – 3= «РЛ» = (87,5; 100; 100; 100) LR,
$\widetilde{DE.CM}$ – 4= «РЛ» = (87,5; 100; 100; 100) LR,
$\widetilde{DE.CM}$ – 5= «РД» = (0; 12,5;37,5; 62,5) LR,
$\widetilde{DE.CM}$ – 6 = «НП» = (0;0; 0; 12,5) LR,
$\widetilde{DE.CM}$ – 7 = «РД» = (0; 12,5;37,5; 62,5) LR,
$\widetilde{DE.CM}$ – 8= «НП» = (0;0; 0; 12,5) LR;
$\widetilde{DE.DP}$ «ПРОЦЕСИ ВИЯВЛЕННЯ КІБЕРІНЦИДЕНТІВ» –
$\widetilde{DE.DP}$ – 1= «РЛ» = (87,5; 100; 100; 100) LR,
$\widetilde{DE.DP}$ – 2= «РЛ» = (87,5; 100; 100; 100) LR,
$\widetilde{DE.DP}$ – 3= «ПР» = (37,5; 62,5; 87,5; 100) LR,
$\widetilde{DE.DP}$ – 4= «РД» = (0; 12,5;37,5; 62,5) LR,
$\widetilde{DE.DP}$ – 5= «РД» = (0; 12,5;37,5; 62,5) LR.
Для $\widetilde{\text{AMC}}_4^{AC}$ – ***RS*** "РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ"**:**
$\widetilde{RS.RP}$ «ПЛАНУВАННЯ РЕАГУВАННЯ» –
$\widetilde{RS.RP}$ – 1= «РД» = (0; 12,5;37,5; 62,5) LR;
$\widetilde{RS.CO}$ «КОМУНІКАЦІЇ» –
$\widetilde{RS.CO}$ – 1= «РД» = (0; 12,5;37,5; 62,5) LR,,
$\widetilde{RS.CO}$ – 2= «РД» = (0; 12,5;37,5; 62,5) LR,
$\widetilde{RS.CO}$ – 3= «РЛ» = (87,5; 100; 100; 100) LR,
$\widetilde{RS.CO}$ – 4= «ПР» = (37,5; 62,5; 87,5; 100) LR,
$\widetilde{RS.CO}$ – 5 = «ПР» = (37,5; 62,5; 87,5; 100) LR;
$\widetilde{RS.AN}$ «АНАЛІЗ» –
$\widetilde{RS.AN}$ – 1= «НП» = (0;0; 0; 12,5) LR,
$\widetilde{RS.AN}$ – 2= «ПР» = (37,5; 62,5; 87,5; 100) LR,
$\widetilde{RS.AN}$ – 3= «РД» = (0; 12,5;37,5; 62,5) LR,
$\widetilde{RS.AN}$ – 4= «РЛ» = (87,5; 100; 100; 100) LR,
$\widetilde{RS.AN}$ – 5= «РЛ» = (87,5; 100; 100; 100) LR;
$\widetilde{RS.MI}$ «МІНІМІЗАЦІЯ НАСЛІДКІВ» –
$\widetilde{RS.MI}$ – 1= «ПР» = (37,5; 62,5; 87,5; 100) LR,
$\widetilde{RS.MI}$ – 2= «РД» = (0; 12,5;37,5; 62,5) LR,
$\widetilde{RS.MI}$ – 3= «РЛ» = (87,5; 100; 100; 100) LR;
$\widetilde{RS.IM}$ «УДОСКОНАЛЕННЯ» –
$\widetilde{RS.IM}$ – 1 = «НП» = (0;0; 0; 12,5) LR,
$\widetilde{RS.IM}$ – 2= «РД» = (0; 12,5;37,5; 62,5) LR.
Для $\widetilde{\text{AMC}}_5^{AC}$ – ***RC*** "ВІДНОВЛЕННЯ СТАНУ КІБЕРБЕЗПЕКИ"**:**
$\widetilde{RC.RP}$ «ПЛАНУВАННЯ» –
$\widetilde{RC.RP}$ – 1= «ПР» = (37,5; 62,5; 87,5; 100) LR;
$\widetilde{RC.IM}$ «УДОСКОНАЛЕННЯ» –
$\widetilde{RC.IM}$ – 1= «ПР» = (37,5; 62,5; 87,5; 100) LR,
$\widetilde{RC.IM}$ – 2= «РД» = (0; 12,5;37,5; 62,5) LR;
$\widetilde{RC.CO}$ «КОМУНІКАЦІЇ» –
$\widetilde{RC.CO}$ – 1= РД» = (0; 12,5;37,5; 62,5) LR,,
$\widetilde{RC.CO}$ – 2= «РД» = (0; 12,5;37,5; 62,5) LR,
$\widetilde{RC.CO}$ – 4= «ПР» = (37,5; 62,5; 87,5; 100) LR.

З урахуванням вищезазначеного вираз (16) має вигляд:

$$\widetilde{ACM}_1^{AC} = (\sum_{j=1}^{6} \widetilde{ACM}_{1j}^{AC})/6 = (\sum_{j=1}^{6} \widetilde{ID}_{1j}^{AC})/6 =$$
$$= (\widetilde{ID.AM}_{11} \widetilde{\oplus} \widetilde{ID.BE}_{12} \widetilde{\oplus} \widetilde{ID.GV}_{13} \widetilde{\oplus} \dots \widetilde{\oplus} \widetilde{ID.SC}_{16})/6 =$$
$$= ((\widetilde{ID.AM} - 1 \widetilde{\oplus} \widetilde{ID.AM} - 2 \widetilde{\oplus} \widetilde{ID.AM} - 3 \widetilde{\oplus} \widetilde{ID.AM} - 4 \widetilde{\oplus} =$$
$$= \widetilde{ID.AM} - 5 \widetilde{\oplus} \widetilde{ID.AM} - 6)/6 \widetilde{\oplus} (\widetilde{ID.BE} - 1 \widetilde{\oplus} \widetilde{ID.BE} - 2 \widetilde{\oplus} \widetilde{ID.BE} - 3 \widetilde{\oplus} =$$
$$= \widetilde{ID.BE} - 4 \widetilde{\oplus} \widetilde{ID.BE} - 5)/5 \widetilde{\oplus} (\widetilde{ID.GV} - 1 \widetilde{\oplus} \widetilde{ID.GV} - 2 \widetilde{\oplus} \widetilde{ID.GV} - 3 \widetilde{\oplus} =$$
$$= \widetilde{ID.GV} - 4)/4 \widetilde{\oplus} (\widetilde{ID.AM} - 1 \widetilde{\oplus} \widetilde{ID.RA} - 2 \widetilde{\oplus} \widetilde{ID.RA} - 3 \oplus =$$
$$= \widetilde{ID.RA} - 4 \widetilde{\oplus} \widetilde{ID.RA} - 5 \widetilde{\oplus} \widetilde{ID.RA} - 6)/6 \widetilde{\oplus} =$$
$$= (\widetilde{ID.RM} - 1 \widetilde{\oplus} \widetilde{ID.RM} - 2 \widetilde{\oplus} \widetilde{ID.RM} - 3)/3 \widetilde{\oplus} (\widetilde{ID.SC} - 1 \widetilde{\oplus} =$$
$$\widetilde{ID.SC} - 2 \widetilde{\oplus} \widetilde{ID.SC} - 3 \widetilde{\oplus} \widetilde{ID.SC} - 4 \widetilde{\oplus} \widetilde{ID.SC} - 5)/5)/6 =$$

(((0;12,5; 37,5; 62,5)$_{LR}$ $\widetilde{\oplus}$ (0; 12,5;37,5; 62,5)$_{LR}$ $\widetilde{\oplus}$ (0; 12,5;37,5; 62,5)$_{LR}$ $\widetilde{\oplus}$ (37,5; 62,5;87,5;100)$_{LR}$ $\widetilde{\oplus}$ (37,5; 62,5; 87,5; 100)$_{LR}$ $\widetilde{\oplus}$ (37,5; 62,5; 87,5; 100)$_{LR}$)/6) $\widetilde{\oplus}$ (0; 12,5;37,5; 62,5)$_{LR}$ $\widetilde{\oplus}$ (0; 12,5;37,5; 62,5)$_{LR}$ $\widetilde{\oplus}$ (0;12,5; 37,5; 62,5)$_{LR}$ $\widetilde{\oplus}$ (37,5; 62,5; 87,5; 100)$_{LR}$$\widetilde{\oplus}$ (0;12,5; 37,5; 62,5)$_{LR}$)/5) $\widetilde{\oplus}$ (((0;0; 0; 12,5)$_{LR}$ $\widetilde{\oplus}$ (0;12,5; 37,5; 62,5)$_{LR}$ $\widetilde{\oplus}$ (0; 37,5; 62,5; 87,5; 100) $_{LR}$ $\widetilde{\oplus}$ (37,5; 62,5; 87,5; 100)$_{LR}$)/4) $\widetilde{\oplus}$(((0;0; 0; 12,5)$_{LR}$ $\widetilde{\oplus}$ (0; 12,5;37,5; 62,5)$_{LR}$ $\widetilde{\oplus}$ (0; 12,5;37,5; 62,5)$_{LR}$ $\widetilde{\oplus}$ (37,5; 62,5; 87,5; 100)$_{LR}$ $\widetilde{\oplus}$ (87,5; 100; 100; 100)$_{LR}$ $\widetilde{\oplus}$ (37,5; 62,5; 87,5; 100)$_{LR}$)/6) $\widetilde{\oplus}$ (((0;0; 0; 12,5)$_{LR}$$\widetilde{\oplus}$ (0; 12,5;37,5; 62,5)$_{LR}$$\widetilde{\oplus}$ (0; 12,5;37,5; 62,5)$_{LR}$)/3) $\widetilde{\oplus}$(((0;0; 0; 12,5)$_{LR}$$\widetilde{\oplus}$ (0; 12,5;37,5; 62,5)$_{LR}$ $\widetilde{\oplus}$ (0; 12,5;37,5; 62,5)$_{LR}$$\widetilde{\oplus}$ (87,5; 100; 100; 100)$_{LR}$ $\widetilde{\oplus}$ (37,5; 62,5; 87,5; 100)$_{LR}$)/5)))/6=(16,18; 29,97; 48,78; 66,32)$_{LR}$.

Так для $\widetilde{\text{ACM}}_2^{AC}$ $-$ ***PR*** "КІБЕРЗАХИСТ" вираз (16) запишемо як:

$$\widetilde{\text{ACM}}_2^{AC} = (\sum_{j=1}^{6} \widetilde{\text{ACM}}_{2j}^{AC})/2 = (\sum_{j=1}^{6} \widetilde{\text{ACM}}_{2j}^{AC})/6 =$$
$$= (\widetilde{PR}_{21} \widetilde{\oplus} \widetilde{PR}_{22} \widetilde{\oplus} \widetilde{PR}_{23} \widetilde{\oplus} \widetilde{PR}_{24} \widetilde{\oplus} \widetilde{PR}_{25} \widetilde{\oplus} \widetilde{PR}_{26})/6 =$$
$$= (\widetilde{PR.AC}_{21} \widetilde{\oplus} \widetilde{PR.AT}_{22} \widetilde{\oplus} PR.DS_{23} \widetilde{\oplus} \dots \widetilde{\oplus} \widetilde{PR.PT}_{26})/6 =$$
$$= ((\widetilde{PR.AC} - 1 \widetilde{\oplus} \widetilde{PR.AC} - 2 \widetilde{\oplus} \widetilde{PR.AC} - 3 \widetilde{\oplus} \widetilde{PR.AC} - 4 \widetilde{\oplus} \widetilde{PR.AC} - 5 \widetilde{\oplus} \widetilde{PR.AC} - 6 \widetilde{\oplus} =$$
$$= \widetilde{PR.AC} - 7)/7 \widetilde{\oplus} (\widetilde{PR.AT} - 1 \widetilde{\oplus} \widetilde{PR.AT} - 2 \widetilde{\oplus} \widetilde{PR.AT} - 3 \widetilde{\oplus} \widetilde{PR.AT} - 4 \widetilde{\oplus} =$$
$$= \widetilde{PR.AT} - 5)/5 \widetilde{\oplus} (\widetilde{PR.DS} - 1 \widetilde{\oplus} \widetilde{PR.DS} - 2 \widetilde{\oplus} \widetilde{PR.DS} - 3 \widetilde{\oplus} \widetilde{PR.DS} - 4 \widetilde{\oplus} =$$
$$= \widetilde{PR.DS} - 5 \widetilde{\oplus} \widetilde{PR.DS} - 6 \widetilde{\oplus} \widetilde{PR.DS} - 7 \widetilde{\oplus} \widetilde{PR.DS} - 8)/8 \widetilde{\oplus} (\widetilde{PR.IP} - 1 \widetilde{\oplus} \widetilde{PR.IP} - 2 \widetilde{\oplus} =$$
$$= \widetilde{PR.IP} - 3 \widetilde{\oplus} \widetilde{PR.IP} - 4 \widetilde{\oplus} \widetilde{PR.IP} - 5 \widetilde{\oplus} \widetilde{PR.IP} - 6 \widetilde{\oplus} PR.IP - 7 \widetilde{\oplus} \widetilde{PR.IP} - 8 \widetilde{\oplus} =$$
$$= \widetilde{PR.IP} - 9 \widetilde{\oplus} \widetilde{PR.IP} - 10 \widetilde{\oplus} \widetilde{PR.IP} - 11 \widetilde{\oplus} =$$
$$= \widetilde{PR.IP} - 12)/12 \widetilde{\oplus} (\widetilde{PR.MA} - 1 \widetilde{\oplus} \widetilde{PR.MA} - 2)/2 \widetilde{\oplus} (\widetilde{PR.PT} - 1 \widetilde{\oplus} =$$
$$= \widetilde{PR.PT} - 2 \widetilde{\oplus} \widetilde{PR.PT} - 3 \widetilde{\oplus} \widetilde{PR.PT} - 4 \widetilde{\oplus} \widetilde{PR.PT} - 5)/5)/6 =$$

= (((0;0; 0; 12,5)$_{LR}$$\widetilde{\oplus}$(0; 12,5;37,5; 62,5)$_{LR}$$\widetilde{\oplus}$(0; 12,5;37,5; 62,5)$_{LR}$$\widetilde{\oplus}$(87,5; 100; 100; 100)$_{LR}$$\widetilde{\oplus}$(37,5; 62,5; 87,5; 100)$_{LR}$$\widetilde{\oplus}$(0;0; 0; 12,5)$_{LR}$$\widetilde{\oplus}$(0; 12,5;37,5; 62,5)$_{LR}$)/7) $\widetilde{\oplus}$(((0;0; 0; 12,5)$_{LR}$$\widetilde{\oplus}$(0; 12,5;37,5; 62,5)$_{LR}$$\widetilde{\oplus}$(87,5; 100; 100; 100)$_{LR}$$\widetilde{\oplus}$(87,5; 100; 100; 100)$_{LR}$$\widetilde{\oplus}$(37,5; 62,5; 87,5; 100)$_{LR}$)/5) $\widetilde{\oplus}$(((0;0; 0; 12,5)$_{LR}$$\widetilde{\oplus}$(0; 12,5;37,5; 62,5)$_{LR}$$\widetilde{\oplus}$(0;0; 0; 12,5)$_{LR}$$\widetilde{\oplus}$(0; 12,5;37,5; 62,5)$_{LR}$$\widetilde{\oplus}$(37,5; 62,5; 87,5; 100)$_{LR}$$\widetilde{\oplus}$(0;0; 0; 12,5)$_{LR}$$\widetilde{\oplus}$(0; 12,5;37,5; 62,5)$_{LR}$$\widetilde{\oplus}$(87,5; 100; 100; 100)$_{LR}$)/8) $\widetilde{\oplus}$(((0;0; 0; 12,5)$_{LR}$$\widetilde{\oplus}$(0; 12,5;37,5; 62,5)$_{LR}$$\widetilde{\oplus}$(0; 12,5;37,5; 62,5)$_{LR}$$\widetilde{\oplus}$(37,5; 62,5; 87,5; 100)$_{LR}$$\widetilde{\oplus}$(87,5; 100; 100; 100)$_{LR}$$\widetilde{\oplus}$(87,5; 100; 100; 100)$_{LR}$$\widetilde{\oplus}$(87,5; 100; 100; 100)$_{LR}$$\widetilde{\oplus}$(37,5; 62,5; 87,5; 100)$_{LR}$$\widetilde{\oplus}$(0;0; 0; 12,5)$_{LR}$$\widetilde{\oplus}$(0; 12,5;37,5; 62,5)$_{LR}$$\widetilde{\oplus}$(0; 12,5;37,5; 62,5)$_{LR}$$\widetilde{\oplus}$(87,5; 100; 100; 100)$_{LR}$)/12) $\widetilde{\oplus}$(((87,5; 100; 100; 100)$_{LR}$$\widetilde{\oplus}$(37,5; 62,5; 87,5; 100)$_{LR}$)/2) $\widetilde{\oplus}$(((0;0; 0; 12,5)$_{LR}$$\widetilde{\oplus}$(0; 12,5;37,5; 62,5)$_{LR}$$\widetilde{\oplus}$(0;0; 0; 12,5)$_{LR}$$\widetilde{\oplus}$(87,5; 100; 100; 100)$_{LR}$ $\widetilde{\oplus}$ (87,5; 100; 100; 100$_{(LR)}$/5)/6=(34,82;46,71;57,84;57,08)$_{LR}$.

Далі, для $\widetilde{\text{ACM}}_3^{AC}$ ***DE*** "ВИЯВЛЕННЯ КІБЕРІНЦИДЕНТІВ" вираз (16) буде виглядати наступним чином:

$$\widetilde{\text{ACM}}_3^{AC} = (\sum_{j=1}^{3} \widetilde{\text{ACM}}_{3j}^{AC})/3 = (\sum_{j=1}^{3} \widetilde{DE}_{3j}^{AC})/3 =$$
$$= (\widetilde{DE}_{31}^{AC} \widetilde{\oplus} \widetilde{DE}_{32}^{AC} \widetilde{\oplus} \widetilde{DE}_{33}^{AC})/3 =$$

$$= ((DE.\widetilde{AE} - 1 \widetilde{\oplus} DE.\widetilde{AE} - 2 \widetilde{\oplus} DE.\widetilde{AE} - 3 \widetilde{\oplus} DE.\widetilde{AE} - 4 \widetilde{\oplus} DE.\widetilde{AE} - 5)/5 \widetilde{\oplus} =$$
$$= (DE.\widetilde{CM} - 1 \widetilde{\oplus} DE.\widetilde{CM} - 2 \widetilde{\oplus} DE.\widetilde{CM} - 3 \widetilde{\oplus} DE.\widetilde{CM} - 4 \widetilde{\oplus} =$$
$$= DE.\widetilde{CM} - 5 \widetilde{\oplus} DE.\widetilde{CM} - 6 \widetilde{\oplus} DE.\widetilde{CM} - 7 \widetilde{\oplus} DE.\widetilde{CM} - 8)/8 \widetilde{\oplus} =$$
$$= (DE.\widetilde{DP} - 1 \widetilde{\oplus} DE.\widetilde{DP} - 2 \widetilde{\oplus} DE.\widetilde{DP} - 3 \widetilde{\oplus} DE.\widetilde{DP} - 4 \widetilde{\oplus} DE.DP - 5)/5\ )/3 =$$

$= (((0;\ 12{,}5;37{,}5;\ 62{,}5)_{LR} \widetilde{\oplus} (0;0;\ 0;\ 12{,}5)_{LR} \widetilde{\oplus} (0;\ 12{,}5;37{,}5;\ 62{,}5)_{LR} \widetilde{\oplus} (0;0;\ 0;\ 12{,}5)_{LR} \widetilde{\oplus} (87{,}5;\ 100;\ 100;\ 100)_{LR})/5) \widetilde{\oplus} ((0;\ 12{,}5;37{,}5;\ 62{,}5)_{LR} \widetilde{\oplus} (87{,}5;\ 100;\ 100;\ 100)_{LR} \widetilde{\oplus} (87{,}5;\ 100;\ 100;\ 100)_{LR} \widetilde{\oplus} (87{,}5;\ 100;\ 100;\ 100)_{LR} \widetilde{\oplus} (0;\ 12{,}5;37{,}5;\ 62{,}5)_{LR} \widetilde{\oplus} (0;0;\ 0;\ 12{,}5)_{LR} \widetilde{\oplus} (0;\ 12{,}5;37{,}5;\ 62{,}5)_{LR} \widetilde{\oplus} (0;0;\ 0;\ 12{,}5)_{LR})/8)\ ((87{,}5;\ 100;\ 100;\ 100)_{LR} \widetilde{\oplus} (87{,}5;\ 100;\ 100;\ 100)_{LR} \widetilde{\oplus} (37{,}5;\ 62{,}5;\ 87{,}5;\ 100)_{LR} \widetilde{\oplus} (0;\ 12{,}5;37{,}5;\ 62{,}5)_{LR} \widetilde{\oplus} (0;\ 12{,}5;37{,}5;\ 62{,}5)_{LR})/5)/3 = (30{,}94;\ 41{,}56;\ 53{,}02;\ 53{,}85)_{LR}.$

Далі, для $\widetilde{ACM}_4^{AC}$ – ***RS*** "РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ" (16) запишемо наступним чином:

$$\widetilde{ACM}_4^{AC} = (\sum_{j=1}^{5} \widetilde{ACM}_{4j}^{\text{AC}})/5 = (\sum_{j=1}^{5} \widetilde{RS}_{4j}^{AC})/5 =$$
$$= (\widetilde{RS}_{41}^{AC} \widetilde{\oplus} \widetilde{RS}_{42}^{AC} \widetilde{\oplus} \widetilde{RS}_{43}^{AC} \widetilde{\oplus} \widetilde{RS}_{44}^{AC} \widetilde{\oplus} \widetilde{RS}_{45}^{AC})/5 =$$
$$= ((RS.\widetilde{RP} - 1) \widetilde{\oplus} (RS.\widetilde{CO} - 1 \widetilde{\oplus} RS.\widetilde{CO} - 2 \widetilde{\oplus} RS.\widetilde{CO} - 3 \widetilde{\oplus} RS.\widetilde{CO} - 4 \widetilde{\oplus} =$$
$$= RS.\widetilde{CO} - 5)/5 \widetilde{\oplus} (RS.\widetilde{AN} - 1 \widetilde{\oplus} RS.\widetilde{AN} - 2 \widetilde{\oplus} RS.\widetilde{AN} - 3 \widetilde{\oplus} =$$
$$= RS.\widetilde{AN} - 4 \widetilde{\oplus} RS.\widetilde{AN} - 5)/5 \widetilde{\oplus} (RS.\widetilde{MI} - 1 \widetilde{\oplus} RS.\widetilde{MI} - 2 \widetilde{\oplus} =$$
$$= RS.\widetilde{MI} - 3)/3 \widetilde{\oplus} (RS.\widetilde{IM} - 1 \widetilde{\oplus} RS.\widetilde{IM} - 2)/2)/5 =$$

$= (((0;\ 12{,}5;37{,}5;\ 62{,}5)_{LR} \widetilde{\oplus} (((0;\ 12{,}5;37{,}5;\ 62{,}5)_{LR} \widetilde{\oplus} (0;\ 12{,}5;37{,}5;\ 62{,}5)_{LR} \widetilde{\oplus} (87{,}5;\ 100;\ 100;\ 100)_{LR} \widetilde{\oplus} (37{,}5;\ 62{,}5;\ 87{,}5;\ 100)_{LR} \widetilde{\oplus} (37{,}5;\ 62{,}5;\ 87{,}5;\ 100)_{LR})/5) \widetilde{\oplus} (((0;0;\ 0;\ 12{,}5)_{LR} \widetilde{\oplus} (37{,}5;\ 62{,}5;\ 87{,}5;\ 100)_{LR} \widetilde{\oplus} (87{,}5;\ 100;\ 100;\ 100)_{LR} \widetilde{\oplus} (87{,}5;\ 100;\ 100;\ 100)_{LR} \widetilde{\oplus} (87{,}5;\ 100;\ 100;\ 100)_{LR})/5 \widetilde{\oplus} (((37{,}5;\ 62{,}5;\ 87{,}5;\ 100)_{LR} \widetilde{\oplus} (87{,}5;\ 100;\ 100;\ 100)_{LR} \widetilde{\oplus} (87{,}5;\ 100;\ 100;\ 100)_{LR}))/3) \widetilde{\oplus} ((0;0;\ 0;\ 12{,}5)_{LR} \widetilde{\oplus} (87{,}5;\ 100;\ 100;\ 100)_{LR})/2)/5 = (23{,}33;\ 36{,}42;\ 53{,}25;\ 69{,}50)_{LR}.$

Аналогічно, для $\widetilde{ACM}_5^{AC}$ – ***RC*** "ВІДНОВЛЕННЯ СТАНУ КІБЕРБЕЗПЕКИ" формула (16) буде виглядати наступним чином:

$$\widetilde{ACM}_5^{AC} = (\sum_{j=1}^{5} \widetilde{ACM}_{5j}^{\text{AC}})/3 = (\sum_{j=1}^{5} \widetilde{RC}_{5j}^{AC})/3 =$$
$$= (\widetilde{RC.RP}_{51} \widetilde{\oplus} \widetilde{RC.IM}_{52} \widetilde{\oplus} \widetilde{RC.CO}_{53})/3 =$$
$$= ((RC.\widetilde{RP} - 1) \widetilde{\oplus} (RC.\widetilde{IM} - 1 \widetilde{\oplus} RC.\widetilde{IM} - 2)/2 \widetilde{\oplus} (RC.\widetilde{CO} - 1 \widetilde{\oplus} =$$
$$= RC.\widetilde{CO} - 2 \widetilde{\oplus} RC.\widetilde{CO} - 3)/3)/3\ =$$

$= ((37{,}5;\ 62{,}5;\ 87{,}5;\ 100)_{LR} \widetilde{\oplus} ((37{,}5;\ 62{,}5;\ 87{,}5;\ 100)_{LR} \widetilde{\oplus} (87{,}5;\ 100;\ 100;\ 100)_{LR})/2) \widetilde{\oplus} ((87{,}5;\ 100;\ 100;\ 100)_{LR} \widetilde{\oplus} (87{,}5;\ 100;\ 100;\ 100)_{LR} \widetilde{\oplus} (37{,}5;\ 62{,}5;\ 87{,}5;\ 100)_{LR})/3)/3 = (22{,}92;\ 43{,}06;\ 68{,}06;\ 85{,}42)_{LR}.$

Далі, з урахуванням (16) вираз (17) запишемо як:

$$\tilde{E}^{\mathbf{1}} = (\sum_{j=1}^{5} \widetilde{ACM}_i^{\text{AC}})/n = (\widetilde{ACM}_1^{\text{AC}} \oplus \widetilde{ACM}_2^{\text{AC}} \oplus \widetilde{ACM}_3^{\text{AC}} \oplus \widetilde{ACM}_4^{\text{AC}} \oplus \widetilde{ACM}_5^{\text{AC}})/5 = \quad (17)$$

$= ((16{,}18;\ 29{,}97;\ 48{,}78;\ 66{,}32)_{\ LR} \widetilde{\oplus} (34{,}82;46{,}71;57{,}84;57{,}08)_{\ LR} \widetilde{\oplus} (30{,}94;\ 41{,}56;\ 53{,}02;\ 53{,}85)_{\ LR} + (23{,}33;\ 36{,}42;\ 53{,}25;\ 69{,}50)_{\ LR} \widetilde{\oplus} (22{,}92;\ 43{,}06;\ 68{,}06;\ 85{,}42)_{\ LR})/5 = (25{,}64;\ 39{,}54;\ 56{,}19;\ 71{,}43)_{\ LR}.$

Етап 5. Процес первинного вимірювання

На цьому етапі вираховується рівень наближеності поточних значень характеристик об'єктів огляду до визначених на етапі 2 еталонних величин [5] із застосуванням відстані Хемінга (ВХ) [6].

Узагальнене значення для всіх $\widetilde{ACM}_{ij}^{q}$розрахуємо по формулі

$$h_{ij}^{q}(\widetilde{ACM}_{ij}^{q}, \tilde{T}_{scs_{ij}}^{q}) = \sum_{j=1}^{f} \left|\mu(\widetilde{ACM}_{ij}^{q}) - \mu(\tilde{T}_{scs_{ij}}^{q})\right|, \quad (18)$$

де, наприклад, для $\widetilde{ACM}_1^{AC}$ "ІДЕНТИФІКАЦІЯ РИЗИКІВ КІБЕРБЕЗПЕКИ" при $\mu(\widetilde{ACM}_{11}^{1}) = \mu(\widetilde{ACM}_{12}^{1}) = 0$, $\mu(\widetilde{ACM}_{13}^{1}) = 14{,}29$, $\mu(\widetilde{ACM}_{14}^{1}) = 28{,}57$, $\mu(\tilde{T}_{ACM_{11}}^{1}) = 16{,}18$, $\mu(\tilde{T}_{ACM_{12}}^{1}) = 29{,}97$, $\mu(\tilde{T}_{ACM_{13}}^{1}) = 48{,}78$, $\mu(\tilde{T}_{ACM_{14}}^{1}) = 66{,}32$ обрахуємо

$h_{11}^1(\widetilde{SD}_{11}^1, \tilde{T}_{scs_{11}}^1)$ = |(0-16,18)|+|(0-29,97)|+|(14,29-48,78)|+|(28,57-66,32)|= 118,39.

Далі, відповідно до (24) обрахуємо:

$h_{12}^1(\widetilde{ACM}_{12}^1, \tilde{T}_{scs_{12}}^1)$ = |(14,29-16,18)|+|(28,57-29,97)|+|(42,86-48,78)|+|(57,14-66,32)| = 18,39,

$h_{13}^1(\widetilde{ACM}_{13}^1, \tilde{T}_{scs_{13}}^1)$ = |(42,86-16,18)|+|(57,14-29,97)|+|(71,34-48,78)|+|(85,71-66,32)| = 95,89,

$h_{14}^1(\widetilde{ACM}_{14}^1, \tilde{T}_{scs_{14}}^1)$= |(71,43-16,18)|+|(85,71-29,97)|+|(100-48,78)|+|(100-66,32)| = 195,89.

Аналогічно:

для $\widetilde{ACM}_2^{AC}$ "КІБЕРЗАХИСТ" –

$h_{21}^1(\widetilde{ACM}_{21}^1, \tilde{T}_{scs_{21}}^1)$ = 166,08,

$h_{22}^1(\widetilde{ACM}_{22}^1, \tilde{T}_{scs_{22}}^1)$ = 66,08,

$h_{23}^1(\widetilde{ACM}_{23}^1, \tilde{T}_{scs_{23}}^1)$ = 48,20,

$h_{24}^1(\widetilde{ACM}_{24}^1, \tilde{T}_{scs_{24}}^1)$ = 148,20;

для $\widetilde{ACM}_3^{AC}$ "ВИЯВЛЕННЯ КІБЕРІНЦИДЕНТІВ" –

$h_{31}^1(\widetilde{ACM}_{31}^1, \tilde{T}_{scs_{31}}^1)$= 149,02,

$h_{32}^1(\widetilde{ACM}_{32}^1, \tilde{T}_{scs_{32}}^1)$ = 49,02,

$h_{33}^1(\widetilde{ACM}_{33}^1, \tilde{T}_{scs_{33}}^1)$ = 65,27,

$h_{34}^1(\widetilde{ACM}_{34}^1, \tilde{T}_{scs_{34}}^1)$ = 165,27;

для $\widetilde{ACM}_4^{AC}$ "РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ" –

$h_{41}^1(\widetilde{ACM}_{41}^1, \tilde{T}_{scs_{41}}^1)$= 139,64;

$h_{42}^1(\widetilde{ACM}_{42}^1, \tilde{T}_{scs_{42}}^1)$ = 39,64;

$h_{43}^1(\widetilde{ACM}_{43}^1, \tilde{T}_{scs_{43}}^4)$ = 74,64;

$h_{44}^1(\widetilde{ACM}_{44}^4, \tilde{T}_{scs_{44}}^1)$ = 174,64;

для $\widetilde{ACM}_5^{AC}$ "ВІДНОВЛЕННЯ СТАНУ КІБЕРБЕЗПЕКИ" –

$h_{51}^1(\widetilde{ACM}_{51}^1, \tilde{T}_{scs_{51}}^1)$ = 176,58,

$h_{52}^1 h(\widetilde{ACM}_{52}^1, \tilde{T}_{scs_{52}}^1)$ = 76,58,

$h_{53}^1(\widetilde{ACM}_{53}^1, \tilde{T}_{scs_{53}}^1)$ = 37,70,

$h_{54}^1(\widetilde{ACM}_{54}^1, \tilde{T}_{scs_{54}}^1)$ = 137,70.

Для $\widetilde{ACM}^{AC}$ «СТАН ЗАХОДІВ КІБЕРЗАХИСТУ» будемо здійснювати обчислення за формулою (19)

$$h_i^q\left(\widetilde{ACM}_i^q, \tilde{T}_{scs_i}^q\right) = \sum_{j=1}^{f} \left|\mu(\widetilde{ACM}_{ij}^q) - \mu(\tilde{T}_{scs_j}^q)\right| \quad (19)$$

і за аналогією з прикладом для (18) отримаємо:

$h_1^1(\widetilde{ACM}_1^{AC}, \tilde{T}_{scs_1}^1)$ = 149,94;

$h_2^1(\widetilde{ACM}_2^{AC}, \tilde{T}_{scs_2}^1)$ = 49,94;

$h_3^1(\widetilde{ACM}_3^{AC}, \tilde{T}_{scs_3}^1)$ = 64,34;

$h_4^1(\widetilde{ACM}_4^{AC}, \tilde{T}_{scs_4}^1)$ = 164,34.

Етап 6. Формування базових пар та евристичних правил

Для формування евристичних правил, за якими, відповідно до оцінок експертів визначимо рівень стану заходів кіберзахисту об'єкту огляду, необхідно визначити базові пари мінімальних ВХ, що будуть виконувати роль аргументів у правилах. Відповідно до властивостей методу, використаному на Етапі 5, і враховуючи, що мінімальне із значень $h_{ij}^q(ACM_{ij}^{AC})$ буде свідчити про найбільшу наближеність НЧ до еталонного, знайдемо мінімальну ВХ із значень h_{ij} $\left(\widetilde{ACM}_{ij}^q, \tilde{T}_{scs_j}^q\right)$, $(i = \overline{1,f})$ за формулою (20):

$$h_{i\,min}^q = \wedge_{i=1}^{f} h_{i\,j}^q \ \ (\widetilde{ACM}_{ij}^q, \tilde{T}_{scs_j}^q),$$

де $h_{imin}^q = h_{ij}^q$, при *min=j*.

Далі для формування базової пари (аргументів) для асоціативних правил визначимо значення:

$$h_{i\,min'}^q = \begin{cases} h_{imin-1}^q(\widetilde{ACM}_{ij}^q, \tilde{T}_{scs_j}^q), \text{при } h_{imin-1}^q(\widetilde{ACM}_{ij}^q, \tilde{T}_{scs_j}^q) \le \ h_{imin+1}^q(\widetilde{ACM}_{ij}^q, \tilde{T}_{scs_j}^q) \\ h_{imin+1}^q(\widetilde{ACM}_{ij}^q, \tilde{T}_{scs_j}^q), \text{при } h_{imin-1}^q(\widetilde{ACM}_{ij}^q, \tilde{T}_{scs_j}^q) > \ h_{imin+1}^q(\widetilde{ACM}_{ij}^q, \tilde{T}_{scs_j}^q), \end{cases} \quad (21)$$

що є найближчим до $h_{i\,min}^q$.

Введемо нормуючий коефіцієнт щодо належності поточного значення до еталонного, який вираховується за виразом

$$k_i^q = \frac{1}{h_{i\,min}^q + h_{i\,min'}^q}. \quad (22)$$

Наступним сформуємо показники рівня впевненості експерта щодо належності поточних значень до оцінювання стану заходів кіберзахисту, що буде вираховуватися за виразом:

$$ECI_{ij} = 1 - k_i^q * h_{i\,min}^q \quad \text{та } ECI'_{ij} = 1 - k_i^q * h_{i\,min'}^q. \quad (23)$$

Наприклад, відповідно до (20) для $\widetilde{ACM}_1^{AC}$ "ІДЕНТИФІКАЦІЯ РИЗИКІВ КІБЕРБЕЗПЕКИ":

$$h_{1\,min}^q = h_{11}^1(\widetilde{ACM}_{11}^1, \tilde{T}_{scs_{11}}^1) \wedge \wedge h_{12}^1(\widetilde{ACM}_{12}^1, \tilde{T}_{scs_{12}}^1) \wedge h_{13}^1(\widetilde{ACM}_{13}^1, \tilde{T}_{scs_{13}}^1) \wedge \wedge h_{14}^1(\widetilde{ACM}_{14}^1, \tilde{T}_{scs_{14}}^1) = 118{,}39 \wedge 18{,}39 \wedge 95{,}89 \wedge \wedge 195{,}89 = 18{,}39,$$

а відповідно до (21)

$$h_{1\,min'}^q : h_{1\,min'}^q = \begin{cases} 95{,}89 \text{ при } 95{,}89 \le 18{,}39 \\ 18{,}39 \text{ при } 118{,}39 > 95{,}89, \end{cases}$$

при цьому $h_{1\,min'}^q = 18{,}39$.

Далі вирахуємо коефіцієнт належності поточного значення до еталонних за допомогою (22)

$$k_1^q = \frac{1}{18{,}39 + 95{,}89} \approx 0{,}009$$

та відповідно з (23) сформуємо показник

$$ECI_{12} = 1 - 0{,}009 * 95{,}89 \approx 0{,}863 \text{ та } ECI'_{13} = = 1 - 0{,}009 * 18{,}39 \approx 0{,}166.$$

Далі формуємо шаблон асоціативного правила $AR(\widetilde{ACM}^q ; \underset{\sim}{T}_{SCS}/ECI; \underset{\sim}{T}'_{SCS}/ECI')$, де $\widetilde{ACM}_i^q$ – *i*-та характеристика об'єкту огляду, $j = \overline{1,f}$, $\underset{\sim}{T}_{SCSi}$ – рівня захисту. Для даної характеристики, при $\widetilde{ACM}^q = \widetilde{ACM}_1^{AC}$, $\underset{\sim}{T}_{SCS} = \underset{\sim}{T}_{SCS_2}$ = «ЗРЗ», $ECI = = ECI_{12} \approx 0{,}863$, $\underset{\sim}{T}'_{SCS} = \underset{\sim}{T}_{SCS_3}$ = «ДРЗ», $ECI' = ECI_{12} \approx 0{,}166$, правило буде виглядати наступним чином:

$$AR(\widetilde{ACM}_1^{AC}; \text{"ЗРЗ"}/ECI'_{12}, \text{"ДРЗ"}/ECI_{13};) =$$
AR ("ІДЕНТИФІКАЦІЯ РИЗИКІВ КІБЕРБЕЗПЕКИ"; "ЗРЗ"/0,863; "ДРЗ"/0,166).

Таким чином, відповідно до прикладу кінцевий варіант правила інтерпретується як: «Стан заходів кіберзахисту для класу заходів кіберзахисту «ІДЕНТИФІКАЦІЯ РИЗИКІВ КІБЕРБЕЗПЕКИ» знаходиться в межах між «ЗАДОВІЛЬНИЙ РІВЕНЬ ЗАХИСТУ» з коефіцієнтом впевненості експерта 0,863 та «ДОСТАТНІЙ РІВЕНЬ ЗАХИСТУ» з коефіцієнтом впевненості експерта 0,166».

Аналогічно, до виразів (20–23) визначаємо стан кіберзахисту для інших характеристик об'єкту огляду.

Для $\widetilde{ACM}_2^{AC}$ "КІБЕРЗАХИСТ":

$$h_{2\,min}^q = 166{,}08 \wedge 66{,}08 \wedge 48{,}20 \wedge 148{,}20 = 48{,}20, \quad h_{2\,min'}^q \approx 66{,}08,$$

k_2^q=0,009, $ECI_{23} \approx 0{,}434$, $ECI'_{22} \approx 0{,}59$.

Таким чином, кінцевий варіант правила інтерпретується як: «Стан заходів кіберзахисту для класу заходів кіберзахисту для $\widetilde{ACM}_2^{AC}$ "КІБЕРЗАХИСТ" знаходиться в межах між «ЗАДОВІЛЬНИЙ РІВЕНЬ ЗАХИСТУ» з коефіцієнтом впевненості експерта 0,434 та «ДОСТАТНІЙ РІВЕНЬ ЗАХИСТУ» з коефіцієнтом впевненості експерта 0,59».

Для $\widetilde{ACM}_3^{AC}$ "ВИЯВЛЕННЯ КІБЕРІНЦИДЕНТІВ":

$$h_{3min}^q = 149{,}02 \wedge 49{,}02 \wedge 65{,}27 \wedge 165{,}27 = 49{,}02, \quad h_{3\,min'}^q \approx 65{,}27,$$

k_3^q=0,009, $ECI_{32} \approx 0{,}5$, $ECI'_{33} \approx 0{,}4$.

Правило інтерпретується як: «Стан заходів кіберзахисту для класу заходів кіберзахисту для $\widetilde{ACM}_3^{AC}$ "ВИЯВЛЕННЯ КІБЕРІНЦИДЕНТІВ" знаходиться в межах між «ЗАДОВІЛЬНИЙ РІВЕНЬ ЗАХИСТУ» з коефіцієнтом впевненості експерта 0,5 та «ДОСТАТНІЙ РІВЕНЬ ЗАХИСТУ» з коефіцієнтом впевненості експерта 0,4».

Для $\widetilde{ACM}_4^{AC}$ "РЕАГУВАННЯ НА КІБЕРІНЦИ ДЕНТИ":

$$h_{4min}^q = 139{,}64 \wedge 39{,}64 \wedge 74{,}64 \wedge 174{,}64 = 39{,}64 \quad h_{4\,min'}^q \approx 74{,}64,$$

k_4^q=0,009; $ECI_{42} \approx 0{,}64$; $ECI'_{43} \approx 0{,}33$.

Кінцевий варіант правила інтерпретується як: «Стан заходів кіберзахисту для класу заходів кіберзахисту для $\widetilde{ACM}_5^{AC}$ "РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ" знаходиться в межах між «ЗАДОВІЛЬНИЙ РІВЕНЬ ЗАХИСТУ» з коефіцієнтом впевненості експерта 0,64 та «ДОСТАТНІЙ РІВЕНЬ ЗАХИСТУ» з коефіцієнтом впевненості експерта 0,33».

Для $\widetilde{ACM}_5^{AC}$ "ВІДНОВЛЕННЯ СТАНУ КІБЕРБЕЗПЕКИ"

$$h_{5\,min}^q = 176{,}58 \wedge 76{,}58 \wedge 37{,}70 \wedge 137{,}70 = 37{,}70, \quad h_{5\,min}^q \approx 76{,}58,$$

k_5^q=0,009; $ECI_{52} \approx 1{,}5$; $ECI'_{51} \approx 0{,}7$,

а правило інтерпретується як: «Стан кіберзахисту характеристики об'єкту огляду для $\widetilde{ACM}_5^{AC}$ "ВІДНОВЛЕННЯ СТАНУ КІБЕРБЕЗПЕКИ" знаходиться в межах між «ЗАДОВІЛЬНИЙ РІВЕНЬ ЗАХИСТУ» з коефіцієнтом впевненості експерта 0,7 та «ДОСТАТНІЙ РІВЕНЬ ЗАХИСТУ» з коефіцієнтом впевненості експерта 1,5».

Для $\widetilde{ACM}^{AC}$ «СТАН ЗАХОДІВ КІБЕРЗАХИСТУ»:

$$h^{q}_{1\,min} = 149{,}94 \wedge 49{,}94 \wedge 64{,}34 \wedge 164{,}34 = 49{,}94,$$

$$h^{q}_{min,} \approx 64{,}34\,,$$

$$k^{q}=0{,}009;\ ECI_2 \approx 0{,}4;\ ECI'_3 \approx 0{,}6.$$

Тут правило інтерпретується як: «Стан заходів кіберзахисту для класу заходів кіберзахисту $\widetilde{ACM}^{AC}$ «СТАН ЗАХОДІВ КІБЕРЗАХИСТУ» знаходиться в межах між «ЗАДОВІЛЬНИЙ РІВЕНЬ ЗАХИСТУ» з коефіцієнтом впевненості експерта 0,4 та «ДОСТАТНІЙ РІВЕНЬ ЗАХИСТУ» з коефіцієнтом впевненості експерта 0,6».

Етап 7. Візуалізація результатів

Далі, на підставі розробленого програмного застосунку здійснимо графічну візуалізацію результатів оцінювання стану кіберзахисту об'єктів огляду для $\widetilde{ACM}^{q}_{j}$, де $j=\overline{1,n}$, $q=\overline{1,m}$ та $\widetilde{SD}^{q}$.

На рис. 2–8 представлена інтерпретація результатів оцінювання. Наприклад, для значення $\widetilde{ACM}^{AC}_{1}$ "ІДЕНТИФІКАЦІЯ РИЗИКІВ КІБЕРБЕЗПЕКИ" (рис. 2) наведено графік отриманого результату, де візуально можна побачити, що зазначена характеристика знаходиться в межах між «ДРЗ» та «ЗРЗ», а на рис. 3, 4, 5, 6 та 7 продемонстровано результат візуалізації для $\widetilde{ACM}^{AC}_{2}$ "КІБЕРЗАХИСТ", $\widetilde{ACM}^{AC}_{3}$ "ВИЯВЛЕННЯ КІБЕРІНЦИДЕНТІВ", $\widetilde{ACM}^{AC}_{4}$ "РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ", $\widetilde{ACM}^{AC}_{5}$ "ВІДНОВЛЕННЯ СТАНУ КІБЕРБЕЗПЕКИ" та $\widetilde{ACM}^{AC}$ «СТАН ЗАХОДІВ КІБЕРЗАХИСТУ» де видно, що вони знаходяться в межах між «ДРЗ» і «ЗРЗ», «ДРЗ» і «ЗРЗ», «ДРЗ» і «ЗРЗ», «ДРЗ» і «ЗРЗ» та «ДРЗ» і «ЗРЗ» відповідно. На рис. 8 представлено значення $\widetilde{ACM}^{AC}_{min}$ коли всі поточні значення відповідають «НП» та $\widetilde{ACM}^{AC}_{max}$, коли всі значення відповідають «РЛ», що є очевидним з логіки причинно-наслідкових зв'язків.

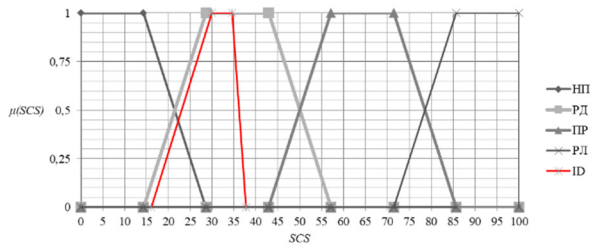

Рис. 2. Графічне подання отриманого результату $\widetilde{ACM}^{AC}_{1}$ "ІДЕНТИФІКАЦІЯ РИЗИКІВ КІБЕРБЕЗПЕКИ"

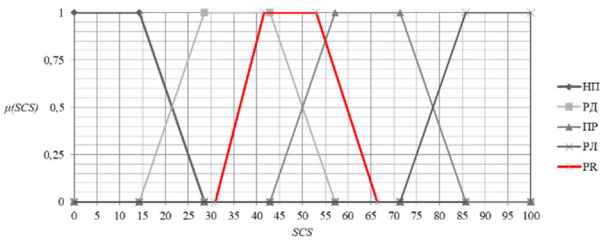

Рис. 3. Графічне подання отриманого результату $\widetilde{ACM}^{AC}_{2}$ "КІБЕРЗАХИСТ"

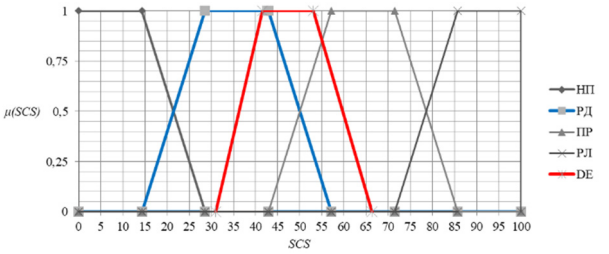

Рис. 4. Графічне подання отриманого результату $\widetilde{ACM}^{AC}_{3}$ "ВИЯВЛЕННЯ КІБЕРІНЦИДЕНТІВ"

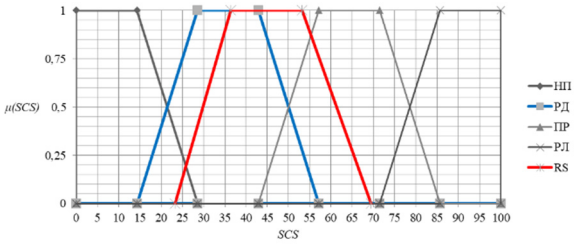

Рис. 5. Графічне подання отриманого результату $\widetilde{ACM}^{AC}_{4}$ "РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ"

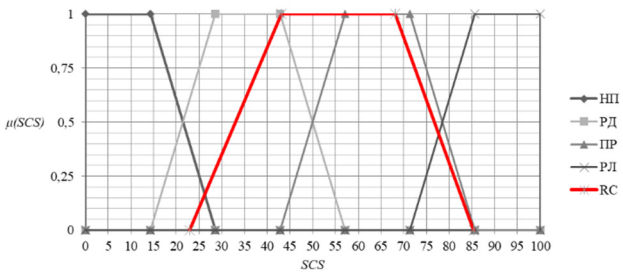

Рис. 6. Графічне подання отриманого результату $\widetilde{ACM}^{AC}_{5}$ "ВІДНОВЛЕННЯ СТАНУ КІБЕРБЕЗПЕКИ"

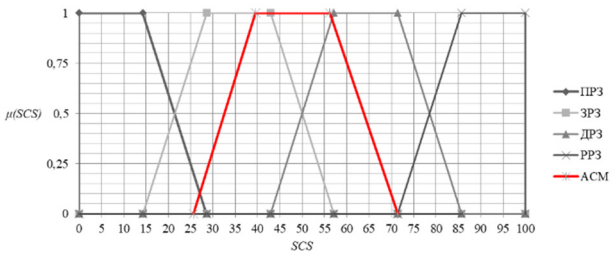

Рис. 7. Графічне подання отриманого результату $\widetilde{ACM}^{AC}$ "СТАН ЗАХОДІВ КІБЕРЗАХИСТУ"

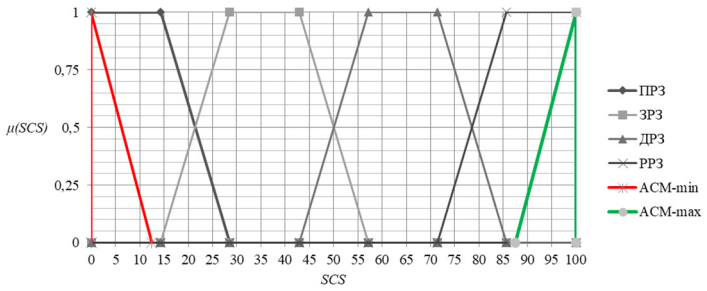

Рис. 8. Графічне подання отриманого результату $\widetilde{ACM}_{min}^{AC}$ «СТАН ЗАХОДІВ КІБЕРЗАХИСТУ» та $\widetilde{ACM}_{max}^{AC}$ «СТАН ЗАХОДІВ КІБЕРЗАХИСТУ»

Висновки

Розроблений метод оцінювання, який за рахунок розробленої моделі системи характеристик, спрямованої на оцінку стану кіберзахисту в Україні, та процедур формування лінгвістичних змінних, фазифікації інтервалів та побудову еталонів, формування множини характеристик об'єктів огляду, процесу первинного вимірювання, формування базових пар і евристичних правил та візуалізації результатів, що формалізуються відповідними етапами, дозволяє реалізовувати процес оцінювання рівня підвищення стану кіберзахисту об'єктів огляду критичної інфраструктури держави. В подальшому необхідно побудувати систему, яка дозволить автоматизувати процес оцінювання підвищення зазначеного стану.

ЛІТЕРАТУРА

[1] Потій О., Семенченко А., Бакалинський О., Мялковський Д. Публічне управління інституціональним розвитком у сфері кіберзахисту. *Науковий вісник: Державне управління.* 2021. № 3(9). С. 136–162.

[2] П'ять методів досягнення кіберстійкості. URL https://www.megatrade.ua/news/reviews/5-metodiv-dosyagnennya-kiberstiykosti/ (дата звернення 25.02.2024)

[3] Належне врядування для забезпечення стійкості критичної інфраструктури, Огляди політики управління ризиками OECD, Публікація OECD, Париж. OECD. 2019.

[4] Шульга В. П., Корченко О. Г. Іванченко Є. В., Бакалинський О. О., Мялковський Д. В., Зубков Д. А., Юдіна Д.О. Метод оцінювання стану кіберзахисту об'єкту огляду критичної інфраструктури держави. *Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем.* 2023. Вип. 25 (II). С. 40–57.

[5] Корченко О. Г. Системи захисту інформації: Монографія. К.: НАУ, 2004. 264 с.

[6] Корченко О. Г., Казмірчук С. В., Ахметов Б. Б. Прикладні системи оцінювання ризиків інформаційної безпеки. Монографія. Київ : ЦП «Компринт», 2017. 435 с.

[7] Корченко А. Методи ідентифікації аномальних станів для систем виявлення вторгнень. Моно графія. Київ.: ЦП «Компринт». 2019. 361 с.

[8] Методичні рекомендації щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури, затверджені наказом Адміністрації Держспецзв'язку від 06.10.2021 № 601. URL https://cip.gov.ua/ua/news/nakaz-ad-2021-10-06-601. (дата звернення 25.02.2024)

Корченко О. Г., Іванченко Є. В., Бакалинський О. О., Мялковський Д. В., Зубков Д. А.
МЕТОД ОЦІНЮВАННЯ РІВНЯ ПІДВИЩЕННЯ СТАНУ КІБЕРЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ДЕРЖАВИ

У зв'язку зі зростанням загроз кібербезпеці, особливо для критичної інфраструктури держави, виникає необхідність у розробці та впровадженні ефективних методів оцінювання рівня кіберзахисту. Критична інфраструктура держави (енергетика, транспорт, медичні установи тощо) все більше стає залежною від інформаційних технологій. Порушення безпеки цих технологій може призвести до серйозних наслідків для життя та здоров'я громадян, а також економічних втрат. Багато країн встановлюють різні регулятивні вимоги стосовно кіберзахисту, наприклад, GDPR в Європейському Союзі або NIST у Сполучених Штатах. Це змушує організації, що управляють критичною інфраструктурою, активно шукати та впроваджувати ефективні методи оцінювання рівня кіберзахисту. Швидкий технологічний прогрес призводить до появи нових методів атак, для захисту від яких необхідно залучати різні ресурси (фінансові, людські, часові тощо) для створення нових більш ефективних засобів для підвищення стану кіберзахисту. Оцінка рівня такого стану в подальшому дасть можливість оцінити ефект від вкладених в безпеку ресурсів. Розроблений метод оцінки підвищення рівня кіберзахисту об'єктів критичної інфраструктури держави ґрунтується на моделі системи характеристик, спрямованої на оцінку стану кіберзахисту в Україні, та процедур формування лінгвістичних

змінних, фазифікації інтервалів та побудови еталонів, формування множини характеристик об'єктів огляду, процесу первинного вимірювання, формуванню базових пар і асоціативних правил та візуалізації результатів, які формалізуються відповідними етапами, дозволяє реалізовувати процес оцінювання стану кіберзахисту об'єкту огляду критичної інфраструктури. Описаний метод може стати ефективним інструментом для аналізу та оцінки рівня кіберзахисту критичної інфраструктури держави з метою забезпечення національної безпеки та захисту від кіберзагроз. В подальшому необхідно побудувати систему, яка дозволить автоматизувати процес оцінювання підвищення стану кіберзахисту на об'єктах огляду.

Ключові слова: інформаційна безпека, кібербезпека, захист інформації, кіберзахист, об'єкти критичної інфраструктури, критична інфраструктура, кіберзагрози, нечіткі множини, методи, моделі.

Korchenko O., Ivanchenko Ye., Bakalinskyi O., Myalkovskyi D., Zubkov D.

METHOD FOR ASSESSING THE LEVEL OF CYBERSECURITY ENHANCEMENT OF CRITICAL INFRASTRUCTURE OBJECTS OF THE STATE

Due to the increasing cybersecurity threats, especially to a state's critical infrastructure, there is a growing need for the development and implementation of effective methods for assessing the level of cybersecurity. The critical infrastructure of a state (such as energy, transportation, medical facilities, etc.) is becoming increasingly dependent on information technologies. Security breaches in these technologies can have serious consequences for citizens' lives and health, as well as economic losses. Many countries are imposing various regulatory requirements regarding cybersecurity, such as GDPR in the European Union or NIST in the United States. This compels organizations managing critical infrastructure to actively seek and implement effective methods for assessing cybersecurity levels. The rapid technological progress leads to the emergence of new attack methods, necessitating the allocation of various resources (financial, human, time, etc.) to develop new, more effective means of enhancing cybersecurity. Assessing the level of cybersecurity enhancement will subsequently allow for evaluating the effectiveness of resources invested in security. The developed method for assessing the enhancement of cybersecurity levels of critical infrastructure objects of the state is based on a model of a characteristic system aimed at assessing the state of cybersecurity in Ukraine. It involves procedures for forming linguistic variables, interval fuzzification, building benchmarks, forming sets of inspection object characteristics, the primary measurement process, forming basic pairs and associative rules, and visualization of results. These are formalized into respective stages, enabling the implementation of the process of assessing the cybersecurity state of critical infrastructure inspection objects. The described method can become an effective tool for analyzing and evaluating the level of cybersecurity of the state's critical infrastructure with the aim of ensuring national security and protection against cyber threats. Further development should focus on building a system that allows for automating the process of assessing the enhancement of cybersecurity levels at inspection objects.

Keywords: information security, cybersecurity, information protection, cyber defense, critical infrastructure objects, critical infrastructure, cyber threats, fuzzy sets, methods, models.

Стаття надійшла до редакції 25.02.2024 р.
Прийнято до друку 10.04.2024 р.