# Оцінювання стану кіберзахисту об'єктів критичної інфраструктури держави

УДК 004.946.5.056(477)(045)

Володимир Шульга [1], Олександр Корченко[2], Євгенія Іванченко[3]

*Державний університет інформаційно-комунікаційних технологій*
*[1]volodymyr.shulha@nau.edu.ua,[2] agkorchenko@gmail.com,*
*[3]Національний авіаційний університет, evivancenko@gmail.com*

На сьогодні процес реалізації кіберзагроз стає все більш вдосконаленим та складним. Розвиток технологій сприяє зростанню можливостей для кіберзлочинності, шпигунства та кібертероризму, що робить їх доступнішими та поширенішими. Критична інфраструктура, така як енергетика, транспорт та медичні заклади, стає все більш залежною від інформаційних технологій. Оцінка рівня кіберзахисту дозволяє оцінити ефективність витрачених ресурсів на безпеку. Оновлені методи оцінювання враховують кібервторгневі інновації та застосовують 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.

Проблеми забезпечення кіберзахисту критичної інфраструктури в умовах зростаючих кіберзагроз [1] свідчать про потребу у розробці відповідних ефективних методів. Відомі методи оцінювання рівня кіберзахисту [2,3,4] не враховують специфіки критичної інфраструктури та не використовують 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. Це може суттєво підвищити ефективність кібербезпекових заходів організацій, як підтверджується низкою досліджень [5,6,7]. Однак сучасні публікації не містять методів оцінювання рівня підвищення стану кіберзахисту об'єктів критичної інфраструктури на основі експертного оцінювання, що ґрунтується на теорії нечітких множин. Проблема забезпечення кіберзахисту критичної інфраструктури в умовах зростаючих кіберзагроз [1] свідчить 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.

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 безпеки України. Запропонований метод включає процедури, що реалізуються шістьма етапами: формування лінгвістичних змінних (ЛЗ), фазифікацію інтервалів та побудову еталонів, формування 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.

На етапі 1 сформуємо лінгвістичні змінні**,** де відповідно 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 заходів кіберзахисту (ЗКЗ) здійснюється формування лінгвістичної змінної (ЛЗ) на підставі кортежу [5] <***TL***, $\underset{\sim}{T}_{TL}$, $X_{TL}$> з певною областю визначення базової терм-множини ***TL*** за допомогою *f* термів.

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:

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

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 $X_{ACM} = [x_{ACM}^{min}, x_{ACM}^{max}] = [x_{ACM}^{min} = X_{ACM1}; X_{ACM2}[, [X_{ACM2}; X_{ACM3}[,\ldots, [X_{ACMi}; X_{ACMi+1}[,\ldots, [X_{ACMf}; x_{ACM}^{max} = X_{ACMf+1}]$ – область визначення НЧ.

На другому етапі проведемо фазифікацію інтервалів та побудову еталону стан заходів кіберзахисту, де за допомогою метода [4] та табл. 1 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*.

*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] |

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 | $(0; 0; 0; 12{,}5)_{LR}$ | $(0; 12{,}5; 37{,}5; 62{,}5)_{LR}$ | $(37{,}5; 62{,}5; 87{,}5; 100)_{LR}$ | $(87{,}5; 100; 100; 100)_{LR}$ |

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

За допомогою ЛЗ ***ACM*** можемо здійснювати оцінку системи заходів кіберзахисту, для чого визначимо відповідно 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 [4,8] 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». Виконаємо формування еталонів НЧ для ЛЗ ***ACM*** за допомогою [4] та табл.2. 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)».

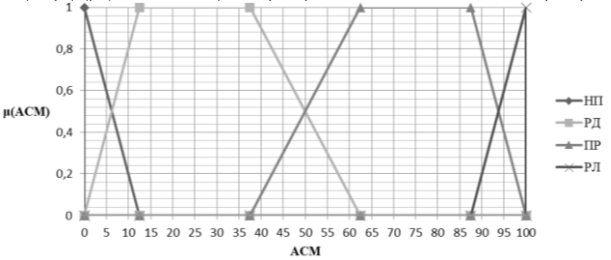


Рис. 1. Терми значень сформованих різнорідно розподілених НЧ для ЛЗ ***ACM*** $\underset{\sim}{T}^{(4)}_{\text{ACM}}$, де відповідно «НП» – «НЕ ПОТРЕБУЄТЬСЯ»; «РД» – «РОЗГЛЯДАЄТЬСЯ ДЛЯ РЕАЛІЗАЦІЇ», «ПР» – «У ПРОЦЕСІ», «РЛ» – «РЕАЛІЗОВАНО».

На третьому етапі сформуємо множину характеристик об’єктів огляду. Для цього введемо множину характеристик, що відображають стан заходів кіберзахисту (СЗКЗ) об’єктів огляду [4]

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

де $\tilde{E}^{q}_{\square} \subseteq \tilde{\boldsymbol{E}}\left(q = \overline{1,m}\right)$ 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.

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

$$ACM^q = \left\{ \bigcup_{i=1}^{\eta} ACM_i^q \right\} = \{ACM, ACM_2^q, \dots, ACM_\eta^q\}, \quad (3)$$

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

Наприклад, при $\eta$ =5 з урахуванням класів ЗКЗ [8] формулу (3) запишемо як:

$$ACM^q = \{\cup_{i=1}^{\eta} ACM_i^q\} = \{ACM_1^q, ACM_2^q, ACM_3^q, ACM_4^q, ACM_5^q\}$$

$$=\{ID, PR, DE, RS, RC\} = \{\text{"}\textit{ІДЕНТИФІКАЦІЯ РИЗИКІВ КІБЕРБЕЗПЕКИ", "КІБЕРЗАХИСТ", "ВИЯВЛЕННЯ КІБЕРІНЦИДЕНТІВ", "РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ", "ВІДНОВЛЕННЯ СТАНУ КІБЕРБЕЗПЕКИ"}\text{ }\},$$

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".*

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

$$\tilde{E}^{\boldsymbol{q}} = (\sum_{i=1}^{\eta} \widetilde{ACM}_{ij}^q)/\eta = \quad (4)$$

$$(\widetilde{ACM}_1^q \oplus \widetilde{ACM}_2^q \oplus \dots \oplus \widetilde{ACM}_n^q)/\eta,$$

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

На четвертому етапі визначимо поточні значення характеристик об'єктів огляду. Кожний *i*-й клас ЗКЗ $q$-го об'єкту огляду визначається за формулою:

$$\widetilde{ACM}_i^q = (\sum_{j=1}^{k_i} ACM_{ij}^q)/k_i = (\widetilde{ACM}_{i1}^q \oplus \widetilde{ACM}_{i2}^q \oplus \dots \oplus \widetilde{ACM}_{ik_i}^q)/k_i, \quad (5)$$

$$(j = \overline{1,k_i}).$$

На п'ятому етапі здійснюється процес первинного вимірювання, тобто 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

$$h_{ij}^q(\widetilde{ACM}_{ij}^q, \tilde{T}_{scs_{ij}}^q) = \sum_{j=1}^{f} \left| \mu(\widetilde{ACM}_{ij}^q) - \mu(\tilde{T}_{scs_{ij}}^q) \right|, \quad (6)$$

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.

На етапі 6 здійснюється формування базових пар та евристичних правил, за якими, відповідно до оцінок експертів визначається рівень стану заходів кіберзахисту об'єкту огляду, для чого 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 $h_{ij}$ $(\widetilde{ACM}_{ij}^{q}, \tilde{T}_{scs_j}^{q})$, $(i = \overline{1,f})$ за формулою (7)

$$h_{i\,min}^{q} = \bigwedge_{i=1}^{f} h_{i\,j}^{q}(\widetilde{ACM}_{ij}^{q}, \tilde{T}_{scs_j}^{q}), \tag{7}$$

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

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

$$h_{i\,min'}^{q} = \begin{cases} h_{imin-1}^{q}(\widetilde{ACM}_{ij}^{q}, \tilde{T}_{scs_j}^{q}), \\ \text{при } h_{imin-1}^{q}(\widetilde{ACM}_{ij}^{q}, \tilde{T}_{scs_j}^{q}) \leq h_{imin+1}^{q}(\widetilde{ACM}_{ij}^{q}, \tilde{T}_{scs_j}^{q}) \\ h_{imin+1}^{q}(\widetilde{ACM}_{ij}^{q}, \tilde{T}_{scs_j}^{q}), \\ \text{при } h_{imin-1}^{q}(\widetilde{ACM}_{ij}^{q}, \tilde{T}_{scs_j}^{q}) > h_{imin+1}^{q}(\widetilde{ACM}_{ij}^{q}, \tilde{T}_{scs_j}^{q}) \end{cases}, \tag{8}$$

що є найближчим до $h_{i\,min}^{q}$.

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

$$k_i^q = \frac{1}{h_{i\,min}^{q} + h_{i\,min'}^{q}}. \tag{9}$$

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

$$ECI_{ij} = 1 - k_i^q * h_{i\,min}^{q} \text{ та } ECI'_{ij} = 1 - k_i^q * h_{i\,min'}^{q}. \tag{10}$$

Наприклад, відповідно до (7) для $\widetilde{ACM}_1^{AC}$ "ІДЕНТИФІКАЦІЯ РИЗИКІВ КІБЕРБЕЗПЕКИ":

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

а відповідно до (8) $h_{1\,min'}^{q}$: $h_{1\,min'}^{q} = \begin{cases} 95{,}89 \text{ при } 95{,}89 \leq 18{,}39 \\ 18{,}39 \text{ при } 118{,}39 > 95{,}89, \end{cases}$

при цьому $h_{1\,min'}^{q}$ = 18,39.

Далі вирахуємо коефіцієнт належності поточного значення до еталонних за допомогою (9)

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

та відповідно з (10) сформуємо показник

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

Далі формуємо шаблон асоціативного правила $AR(\widetilde{ACM}^{q}_{\square}; \underset{\sim}{T}_{SCS}/ECI; \underset{\sim}{T}'_{SCS}/ECI')$, де $\widetilde{ACM}^{q}_{i}$ – $i$-та характеристика об'єкту огляду, $j=\overline{1,f}$, $\underset{\sim}{T}_{SCSi}$ – рівні захисту. Для даної характеристики, при $\widetilde{ACM}^{q}_{\square} = \widetilde{ACM}^{AC}_{1}$, $\underset{\sim}{T}_{SCS} = \underset{\sim}{T}_{SCS_2}$ = «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 наступим чином:

$$AR(\widetilde{ACM}^{AC}_{1}; \text{"ЗРЗ"}/ECI'_{12}, \text{"ДРЗ"}/ECI_{13};) =$$

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 (7-10) визначаємо стан кіберзахисту для інших характеристик об'єкту огляду.

На наступному етапі проведемо візуалізацію результатів оцінювання стану кіберзахисту об'єктів огляду для $\widetilde{ACM}^{q}_{j}$ , де $j=\overline{1,n}$, $q=\overline{1,m}$ та $\widetilde{SD}^{q}_{\square}$. 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 $\widetilde{ACM}^{AC}_{\square}$ «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.

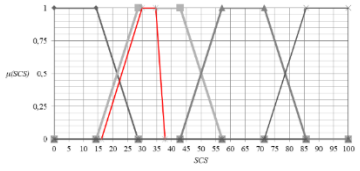

Рис. 2 Графічне подання отриманого результату $\widetilde{ACM}^{AC}_{1}$ "ІДЕНТИФІКАЦІЯ РИЗИКІВ КІБЕРБЕЗПЕКИ"»

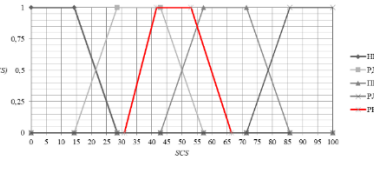

Рис. 3. Графічне подання отриманого результату $\widetilde{ACM}^{AC}_{2}$ "КІБЕРЗАХИСТ"»

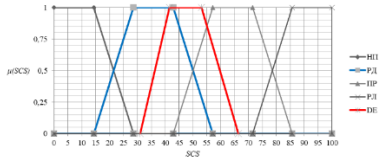


Рис. 4. Графічне подання отриманого результату $\widehat{ACM}_3^{AC}$ "ВИЯВЛЕННЯ КІБЕРІНЦИДЕНТІВ"

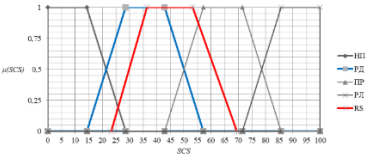


Рис. 5. Графічне подання отриманого результату $\widehat{ACM}_4^{AC}$ "РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ"

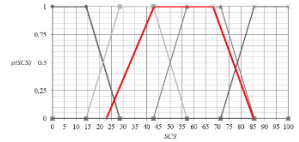


Рис. 6. Графічне подання отриманого результату $\widehat{ACM}_5^{AC}$ "ВІДНОВЛЕННЯ СТАНУ КІБЕРБЕЗПЕКИ"

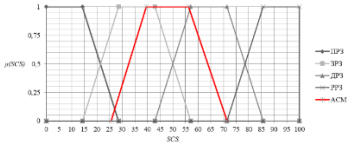


Рис. 7. Графічне подання отриманого результату $\widehat{ACM}_{\square}^{AC}$ «СТАН ЗАХОДІВ КІБЕРЗАХИСТУ»

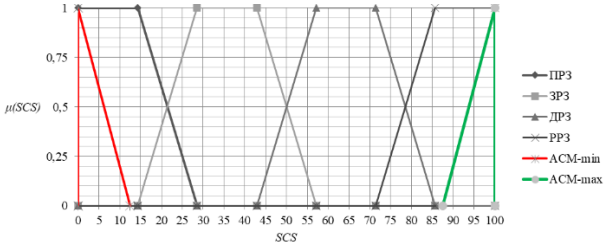


Рис. 8. Графічне подання отриманого результату $\widehat{ACM}_{min}^{AC}$ «СТАН ЗАХОДІВ КІБЕРЗАХИСТУ» та $\widehat{ACM}_{max}^{AC}$ «СТАН ЗАХОДІВ КІБЕРЗАХИСТУ»

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.

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 (ІІ). 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. Монографія. 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).