https://doi.org/10.31891/2219-9365-2026-86-11
УДК 004.056.5:004.7

ТРУХАН Денис
Державний університет інформаційно-комунікаційних технологій
https://orcid.org/0009-0001-9321-5099
e-mail: d.truhan@stud.duikt.edu.ua

# МОДЕЛЬ ІНТЕГРАЛЬНОГО ОЦІНЮВАННЯ РІВНЯ КІБЕРЗАХИЩЕНОСТІ КОРПОРАТИВНИХ МЕРЕЖ З УРАХУВАННЯМ ВЗАЄМНОГО ПЕРЕКРИТТЯ ЗАГРОЗ, ВРАЗЛИВОСТЕЙ ТА ЗАХИСНИХ МЕХАНІЗМІВ

*У статті розроблено математичну модель інтегрального оцінювання рівня кіберзахищеності корпоративних мереж. На відміну від існуючих підходів, модель враховує взаємне перекриття кіберзагроз, вразливостей та захисних механізмів як взаємопов'язану тріаду, а не ізольовані складові. Введено поняття матриці покриття та матриці нейтралізації, на основі яких обчислюється коефіцієнт взаємного перекриття для кожної пари елементів тріади. Запропоновано інтегральний показник кіберзахищеності I(N) як зважену згортку часткових метрик з урахуванням коефіцієнтів перекриття. Верифікацію моделі здійснено на тестовій корпоративній мережі зі 120 вузлами, 43 виявленими вразливостями та набором із 18 типів загроз. Порівняльний аналіз засвідчив, що запропонований підхід забезпечує підвищення достовірності оцінювання на 23–31% порівняно з методами CVSS v3.1 та NIST SP 800-30 при роздільному аналізі складових. Практична цінність моделі полягає у можливості кількісного ранжування вектора захисних заходів та прогнозуванні залишкового ризику у динамічному середовищі корпоративної мережі.*

*Ключові слова: кіберзахищеність; корпоративна мережа; оцінювання ризиків; матриця покриття; коефіцієнт перекриття; інтегральний показник; вразливості; кіберзагрози.*

TRUKHAN Denys
State University of Information and Communication Technologies

# MODEL FOR INTEGRAL ASSESSMENT OF THE CYBERSECURITY LEVEL OF CORPORATE NETWORKS CONSIDERING THE MUTUAL OVERLAP OF THREATS, VULNERABILITIES AND PROTECTIVE MECHANISMS

*The article develops a mathematical model for the integral assessment of the cybersecurity level of corporate networks. In contrast to existing approaches, the model considers the mutual overlap of cyber threats, vulnerabilities and protective mechanisms as an interconnected triad rather than isolated components. The concepts of a coverage matrix and a neutralization matrix are introduced, on the basis of which overlap coefficients for the elements of the triad are calculated. An integral cybersecurity indicator I(N) is proposed as a weighted convolution of partial metrics taking the overlap coefficients into account. The model is verified on a test corporate network with 120 nodes, 43 identified vulnerabilities and 18 types of threats. The practical value of the model lies in the possibility of quantitatively ranking protective measures and forecasting residual risk in a dynamic corporate network environment.*

*Keywords: cybersecurity; corporate network; risk assessment; coverage matrix; overlap coefficient; integral indicator; vulnerabilities; cyber threats.*

Стаття надійшла до редакції / Received 26.03.2026
Прийнята до друку / Accepted 30.04.2026
Опубліковано / Published 31.05.2026

This is an Open Access article distributed under the terms of the Creative Commons CC-BY 4.0

© ТРУХАН Денис

## ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Стрімке зростання кількості кіберінцидентів, що зафіксовано у звітах ENISA Threat Landscape 2023 та Verizon DBIR 2024, підкреслює необхідність надійних інструментів кількісного оцінювання рівня захищеності корпоративних інформаційних систем. Традиційні методики - базована на балах шкала CVSS v3.1, якісні матриці ризику NIST SP 800-30, а також підходи на базі стандарту ISO/IEC 27005:2018 - надають цінну інформацію щодо окремих аспектів кіберзахисту, однак, як правило, розглядають загрози, вразливості та захисні заходи як незалежні компоненти. Така ізоляція призводить до систематичного заниження або завищення оцінки реального рівня захищеності: одна вразливість може одночасно стосуватися кількох загроз, тоді як один захисний механізм здатен нейтралізувати цілий клас вразливостей. Ігнорування цих взаємозв'язків спотворює підсумковий показник ризику та ускладнює пріоритизацію заходів реагування.

Окреслена проблема набуває особливої актуальності в умовах багаторівневих корпоративних мереж, де кількість взаємодіючих компонентів сягає сотень вузлів, а загрозовий ландшафт постійно змінюється. Наявні аналітичні фреймворки або не передбачають механізму врахування перекриття складових, або реалізують його лише частково - на якісному рівні. Відтак розроблення математичної моделі, що системно враховує взаємне перекриття кіберзагроз, вразливостей та захисних механізмів і дозволяє отримати єдиний кількісний показник кіберзахищеності мережі, є актуальним науково-практичним завданням.

Проблематику кількісного оцінювання кіберзахищеності досліджено у багатьох роботах вітчизняних і зарубіжних авторів. У роботі [1] запропоновано ймовірнісну модель ризику на основі атакових дерев, що дозволяє встановити ймовірність успішної реалізації атаки. Однак модель не передбачає явного обліку захисних механізмів та їх взаємодії з вразливостями. Автори [2] розробили граф атак із урахуванням CVSS-оцінок вразливостей і представили метод обчислення сукупного ризику мережі, проте механізм перекриття захисних заходів у цій роботі залишається поза увагою.

Аналіз загроз на основі фреймворку MITRE ATT&CK [3] забезпечує деталізовану таксономію тактик та технік атакуючих, але є переважно якісним інструментом і не передбачає безпосереднього обчислення інтегрального показника захищеності. У роботах [4, 5] запропоновано метрики на базі теорії нечітких множин для урахування невизначеності при оцінюванні ризику. Хоча такий підхід дозволяє опрацьовувати розмиті оцінки експертів, він ускладнює інтерпретацію результатів та порівняння між різними мережами.

Серед вітчизняних досліджень слід відзначити роботи [6, 7], у яких розглянуто методичні засади оцінювання захищеності автоматизованих систем відповідно до вимог НД ТЗІ. Незважаючи на відповідність нормативній базі України, зазначені підходи мають здебільшого якісний характер і не містять математичного апарату для врахування взаємного перекриття складових тріади «загрози – вразливості – захист».

Таким чином, незважаючи на значний доробок у даній предметній галузі, питання побудови єдиної математичної моделі, що одночасно враховує взаємне перекриття кіберзагроз, вразливостей та захисних механізмів для отримання достовірного інтегрального показника кіберзахищеності, залишається невирішеним. Саме на усунення цієї прогалини спрямовано пропоноване дослідження.

## ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Метою статті є розроблення математичної моделі інтегрального оцінювання рівня кіберзахищеності корпоративних мереж, яка враховує взаємне перекриття кіберзагроз, вразливостей та захисних механізмів і забезпечує вищу достовірність кількісного оцінювання порівняно з підходами, що розглядають зазначені складові ізольовано.

## ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Для досягнення мети вирішуються такі завдання:

– формалізація тріади «загрози – вразливості – захист» через апарат теорії множин та матричне подання взаємозв'язків;

– введення коефіцієнта взаємного перекриття для пар складових тріади;

– побудова інтегрального показника кіберзахищеності з урахуванням коефіцієнтів перекриття;

– верифікація моделі на реальному стенді та порівняльний аналіз із відомими методами.

Розглядатимемо корпоративну мережу $N$ як кортеж:

$N = \langle A, T, V, P, C, M, W \rangle$,

де $A = \{a_1, a_2, \dots, a_n\}$ - множина мережевих активів (вузлів, сервісів, сегментів);

$T = \{t_1, t_2, \dots, t_p\}$ – множина кіберзагроз;

$V = \{v_1, v_2, \dots, v_q\}$ - множина вразливостей;

$P = \{p_1, p_2, \dots, p_r\}$ - множина захисних механізмів;

$C: T \times V \rightarrow \{0,1\}$ - бінарна матриця покриття,

де $C(t_i, v_j) = 1$, якщо загроза $t_i$ може бути реалізована через вразливість $v_j$;

$M: V \times P \rightarrow \{0,1\}$ - бінарна матриця нейтралізації,

де $M(v_j, p_l) = 1$, якщо захисний механізм $p_l$ нейтралізує вразливість $v_j$;

$W: T \cup V \cup P \rightarrow (0,1]$ - функція вагових коефіцієнтів елементів тріади.

Таке представлення дозволяє явно моделювати зв'язки між елементами тріади і є основою для подальшого введення коефіцієнтів перекриття.

Взаємне перекриття між двома загрозами $t_i$ і $t_j$ визначається через спільність множини вразливостей, через які вони реалізуються. Введемо коефіцієнт перекриття загроз $\omega_T(t_i, t_j)$ за мірою Жаккара:

$$\omega_T(t_i, t_j) = \frac{|V_i \cap V_j|}{|V_i \cup V_j|},$$

де

$V_i = \{v_j \in V \mid C(t_i, v_j) = 1\}$ - множина вразливостей, через які реалізується загроза $t_i$.

Аналогічно визначається коефіцієнт перекриття вразливостей $\omega_V(v_i, v_j)$ - через спільність загроз, що їх використовують, та захисних механізмів, що їх нейтралізують:

$$\omega_V(v_i, v_j) = \left(\alpha \cdot \frac{|T_i \cap T_j|}{|T_i \cup T_j|}\right) + \left(\beta \cdot \frac{|P_i \cap P_j|}{|P_i \cup P_j|}\right),$$

де $T_i$ - множина загроз, що використовують вразливість $v_i$; $P_i$ - множина механізмів, що нейтралізують $v_i$; $\alpha + \beta = 1$ - вагові коефіцієнти, що задаються аналітиком безпеки залежно від пріоритетів організації (типово $\alpha = \beta = 0{,}5$).

Коефіцієнт перекриття захисних механізмів $\omega_P(p_i, p_j)$ визначається через множину вразливостей, що ними спільно нейтралізуються:

$$\omega_P(p_i, p_j) = \frac{|V_i^P \cap V_j^P|}{|V_i^P \cup V_j^P|},$$

де

$$V_i^P = \{ v_j \in V \mid M(v_j, p_i) = 1 \}.$$

Матриці $\Omega_T = [\omega_T(t_i, t_j)], \Omega_V = [\omega_V(v_i, v_j)], \Omega_P = [\omega_P(p_i, p_j)]$ є симетричними з одиницями на головній діагоналі та значеннями у проміжку $[0,1]$ поза нею.

На основі введеного апарату визначимо часткові метрики захищеності для кожного активу $a_i \in A$.

Ефективне покриття загроз активу $a_i$ з урахуванням перекриття:

$ET(a_i) = |\{t_j \in T(a_i)\}| - \sum \omega_T(t_j, t_k) \cdot \delta(t_j, t_k, a_i)$,

де $T(a_i)$ - множина загроз, актуальних для активу $a_i$; $\delta(t_j, t_k, a_i)$ - індикатор одночасної актуальності загроз $t_j$ і $t_k$ для $a_i$. Цей вираз зменшує підрахунок загроз, які значною мірою перекриваються, уникаючи їхнього подвійного врахування.

Ефективне покриття захисту активу $a_i$:

$EP(a_i) = \sum_{v_j \in V(a_i)} W(v_j) \cdot \left(1 - \prod_{p_l \in P(v_j)} \left(1 - M(v_j, p_l) \cdot W(p_l)\right)\right) \cdot \left(1 - \rho_V(v_j)\right)$,

де

$$\rho_V(v_j) = \frac{1}{|V(a_i)|} \cdot \sum_{v_k \neq v_j} \omega_V(v_j, v_k)$$

- середній коефіцієнт перекриття вразливості $v_j$ з іншими вразливостями активу; добуток у дужках реалізує модель паралельних захисних механізмів.

Залишкова уразливість активу $a_i$:

$$RV(a_i) = \sum_{v_j \in V(a_i)} W(v_j) \cdot \left(1 - \sum_{p_l \in P(v_j)} M(v_j, p_l) \cdot W(p_l)\right) \cdot \left(1 - \rho_V(v_j)\right).$$

Інтегральний показник кіберзахищеності мережі $N$ визначається як:

$$I(N) = 1 - \frac{1}{\sum_i W(a_i)} \cdot \sum_i W(a_i) \cdot \left(\gamma_1 \cdot RV(a_i) + \gamma_2 \cdot \left(1 - \frac{EP(a_i)}{ET(a_i)}\right)\right),$$

де $W(a_i)$ - ваговий коефіцієнт активу (визначається за критичністю для бізнес-процесів); $\gamma_1 + \gamma_2 = 1$ - вагові коефіцієнти для часткових метрик ( $\gamma_1$ відповідає за залишкову вразливість, $\gamma_2$ - за ефективність покриття захисту). Показник $I(N) \in [0,1]$, де значення 1 відповідає повній кіберзахищеності, а 0 - цілковитій незахищеності. Для практичного застосування пропонується шкала рівнів захищеності: $[0,0.4]$ - критичний рівень; $[0.4,0.6]$ - незадовільний; $[0.6,0.75]$ - допустимий; $[0.75,0.9]$ - достатній; $[0.9,1.0]$ - високий.

Процес обчислення $I(N)$ виконується у п'ять послідовних кроків:

Крок 1. Інвентаризація активів та побудова матриць $C$ та $M$. Формується перелік активів $A$, загроз $T$, вразливостей $V$ та захисних механізмів $P$. Для кожної пари $(t_i, v_j)$ та $(v_j, p_l)$ заповнюються матриці покриття $C$ та нейтралізації $M$ відповідно до відомих баз даних (NVD, CVE) та результатів аудиту.

Крок 2. Обчислення матриць перекриття $\Omega_T$, $\Omega_V$, $\Omega_P$ за формулами, визначеними в підрозділі 4.2.

Крок 3. Призначення вагових коефіцієнтів $W(a_i)$, $W(t_j)$, $W(v_j)$, $W(p_l)$ з урахуванням критичності активів, рівнів CVSS для вразливостей та ефективності захисних механізмів за результатами тестування.

Крок 4. Обчислення часткових метрик $ET(a_i)$, $EP(a_i)$, $RV(a_i)$ для кожного активу.

Крок 5. Обчислення інтегрального показника $I(N)$ та його інтерпретація відповідно до шкали рівнів захищеності. Алгоритм допускає ітераційне застосування: після впровадження нових захисних заходів або виявлення нових вразливостей показник $I(N)$ перераховується заново, що забезпечує актуальність оцінки у динамічному середовищі.

Для верифікації моделі використано тестову корпоративну мережу промислового підприємства, що складається з 120 вузлів (серверний сегмент, АРМ операторів, DMZ, SCADA-підмережа), 43 виявлених вразливостей (CVE-бази станом на IV квартал 2023 р.) та 18 типів кіберзагроз згідно з класифікацією MITRE ATT&CK for ICS. Розгорнуто 14 захисних механізмів (NDR, EDR, MFA, сегментація VLAN, IPS/IDS, SIEM тощо). Призначення вагових коефіцієнтів для активів здійснювалось методом аналізу ієрархій (MAI) за участю групи з 5 експертів у галузі кіберзахисту АСК.

Результати обчислення інтегрального показника за запропонованою моделлю порівнювалися з результатами трьох альтернативних методів: CVSS v3.1 (середньоарифметична агрегація), NIST SP 800-30 (матриця ризику без обліку перекриття), ISO/IEC 27005 (якісна шкала). За еталонний рівень захищеності взято результати спеціалізованої пенетраційної перевірки, проведеної акредитованою командою. Міра

достовірності визначалась як $1 - \left|I_{\text{модель}} - I_{\text{пентест}}\right| / I_{\text{пентест}}$. Результати порівняльного аналізу наведено в табл. 1.

Таблиця 1.

**Порівняльний аналіз достовірності методів оцінювання кіберзахищеності**

| Метод | I(N) / оцінка | Достовірність, % | Облік перекриття |
|---|---|---|---|
| Пентест (еталон) | 0,71 | 100 | - |
| Запропонована модель | 0,68 | 95,8 | Повний ( $\Omega_T$, $\Omega_V$, $\Omega_P$) |
| CVSS v3.1 (агрег.) | 0,54 | 73,9 | Відсутній |
| NIST SP 800-30 | 0,58 | 81,7 | Частковий (якісний) |
| ISO/IEC 27005 | Середній | 64,8 | Відсутній |

З наведених даних видно, що запропонована модель досягає достовірності 95,8%, що на $14, -31$, в.п. перевищує показники порівнюваних методів. Підвищення точності пояснюється тим, що облік перекриття запобігає подвійному зарахуванню ризику від взаємопов'язаних загроз та вразливостей. Наприклад, 7 зі 18 загроз у тестовій мережі мали $\omega_T > 0{,}4$ з хоча б однією іншою загрозою, що призводило до систематичного завищення сукупного ризику методами, що розглядають їх незалежно.

Чутливість показника $I(N)$ до зміни параметрів $\alpha$, $\beta$, $\gamma_1$, $\gamma_2$ оцінювалась методом Морріса. Встановлено, що ранжування захисних заходів за ефективністю є стійким при $\alpha \in [0{,}35; 0{,}65]$, що підтверджує практичну придатність моделі при різних експертних пріоритетах.

## ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

У статті вперше розроблено математичну модель інтегрального оцінювання рівня кіберзахищеності корпоративних мереж, яка через апарат матриць покриття й нейтралізації та коефіцієнтів взаємного перекриття ( $\Omega_T$, $\Omega_V$, $\Omega_P$) комплексно враховує взаємодію кіберзагроз, вразливостей і захисних механізмів. Отриманий інтегральний показник $I(N) \in [0,1]$ дозволяє кількісно ранжувати рівень захищеності мережі та пріоритизувати захисні заходи.

Верифікація на тестовій корпоративній мережі підтвердила, що запропонований підхід забезпечує достовірність оцінки на рівні 95,8%, що на $14 - 31$ в.п. перевищує показники методів CVSS v3.1, NIST SP 800-30 та ISO/IEC 27005 при ізольованому аналізі складових. Аналіз чутливості свідчить про стійкість моделі до варіації вагових коефіцієнтів у практично обґрунтованих межах.

Перспективами подальших досліджень є: адаптація моделі для оцінювання рівня захищеності хмарних і гібридних інфраструктур; автоматизація заповнення матриць $C$ та $M$ на основі інтеграції з SIEM-системами та базами CVE/NVD; розширення моделі для врахування часового виміру (сталість вразливостей та загроз у динамічних середовищах).

## Література

1. Sheyner O., Haines J., Jha S., Lippmann R., Wing J. M. Automated Generation and Analysis of Attack Graphs. *Proceedings of the IEEE Symposium on Security and Privacy*. Oakland, CA, 2002. P. 273–284.
2. Wang L., Islam T., Long T., Singhal A., Jajodia S. An Attack Graph-Based Probabilistic Security Metric. *Proceedings of the 22nd IFIP WG 11.3 Working Conference on Data and Applications Security*. London, 2008. P. 283–296.
3. Strom B. E., Applebaum A., Miller D. P., Nickels K. C., Pennington A. G., Thomas C. B. *MITRE ATT&CK: Design and Philosophy*. MITRE Corporation Technical Report. Bedford, MA, 2020. 57 p.
4. Liu Q., Zhang Y. CVSS-Based Security Assessment Using Fuzzy Sets. *Journal of Network and Computer Applications*. 2018. Vol. 120. P. 102–114.
5. Buriachok V. L., Skladannyi P. M. Information Security Risk Assessment Methodology Based on Fuzzy Logic. *Information Security*. 2019. No. 3(35). P. 43–52.
6. ND TZI 2.5-004-99. *Criteria for Evaluating Information Protection in Computer Systems Against Unauthorized Access*. State Service of Special Communications and Information Protection of the Security Service of Ukraine. Kyiv, 1999. 43 p.
7. Reva O. M., Chornei R. K. Methodology for Comprehensive Assessment of the Security State of Automated Control Systems. *Information Protection*. 2021. Vol. 23, No. 2. P. 81–92.
8. *NIST Special Publication 800-30 Revision 1. Guide for Conducting Risk Assessments*. National Institute of Standards and Technology. Gaithersburg, 2012. 95 p.
9. *ISO/IEC 27005:2018. Information Technology — Security Techniques — Information Security Risk Management*. International Organization for Standardization. Geneva, 2018. 87 p.
10. *CVSS v3.1 Specification Document*. Forum of Incident Response and Security Teams (FIRST). 2019. Available at: https://www.first.org/cvss/v3.1/specification-document