УДК 004.056:004.738.5
DOI https://doi.org/10.32782/2663-5941/2026.3.1/21

Марченко О.І.
https://orcid.org/0000-0001-5754-4920
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ В УМОВАХ ЗРОСТАННЯ КІБЕРЗАГРОЗ ЦИФРОВОГО СЕРЕДОВИЩА

Метою дослідження є розробка прикладного підходу до підвищення кіберстійкості інформаційних систем. Поєднано аналітичні моделі з багаторівневими архітектурами захисту та інтелектуальними механізмами виявлення атак. Робота фокусується на взаємозв'язках між параметрами функціонування систем і результативністю захисних заходів. Формалізація процесів оцінювання ризиків забезпечує вибір оптимальних рішень для стабільності інфраструктури. Методологія дослідження об'єднує математичне моделювання, аналіз потокових даних та машинне навчання. Застосовано підходи, що враховують часові характеристики інцидентів і рівень вразливості активів. Аналізуючи навантаження на систему, інтегровано моделі поведінкового аналізу з алгоритмами класифікації. Для перевірки ефективності розробленого підходу використано аналітичні розрахунки та порівняння показників моніторингу. Оцінювання базується на верифікації параметрів стійкості обчислювальних ресурсів. Застосування інтегрованих моделей підвищує точність ідентифікації інцидентів, скорочуючи загальний час реагування. Поєднання розподіленої обробки даних із централізованим аналізом гарантує ефективний контроль стану мережі. Рівень кіберстійкості безпосередньо залежить від узгодженості архітектурних компонентів та аналітичних модулів. Використання інтелектуальних алгоритмів мінімізує кількість помилкових спрацювань під час класифікації загроз. Це дозволяє адміністраторам швидше локалізувати вектори проникнення зловмисників. Практичне значення результатів полягає у впровадженні розроблених механізмів у корпоративні інформаційні системи. Запропоновані рішення адаптуються до змінних умов функціонування та вільно масштабуються у розподілених середовищах. Такі інструменти оптимізують витрати на безпеку, зменшуючи потенційні втрати від кіберінцидентів. Наукова новизна роботи полягає у створенні комплексної аналітичної системи оцінювання стійкості. Розроблена модель інтегрує технічні, поведінкові та економічні параметри захисту. Отримані дані розширюють можливості моделювання процесів захисту для розвитку адаптивних систем безпеки.

Ключові слова: *кібербезпека інформаційних систем, кіберризик, кіберстійкість, інтелектуальні системи захисту, SOC-SIEM системи, адаптивні моделі безпеки.*

Постановка проблеми. Стабільність функціонування інформаційних систем залежить від ефективності протидії складним кіберзагрозам. Підприємства масштабують цифрову інфраструктуру через хмарні сервіси та API. Такі технологічні зміни розширюють поверхню атак на корпоративні мережі. Мінімізація збитків безпосередньо корелює зі швидкістю реагування на інциденти. Сучасна архітектура безпеки обов'язково містить аналітичні модулі реального часу. Математичне моделювання дозволяє формалізувати оцінювання стійкості обчислювальних ресурсів [1, с. 126]. Інтеграція технічних і поведінкових засобів захисту залишається неузгодженою. Автономне функціонування засобів безпеки заважає швидкій кореляції подій. Відсутність синхронізації між рівнями оборони збільшує тривалість ідентифікації загроз. Проєктування систем захисту вимагає одночасного обчислення багатьох параметрів. Розробники враховують операційне навантаження, показники доступності та фінансові ризики. Створення адаптивних механізмів забезпечить керованість процесів кібербезпеки.

Аналіз останніх досліджень і публікацій. У публікації Костюк Ю. В., Складанний П. М., Рзаєва С. Л., Самойленко Ю. О., Коршун Н. В. [2] наведені результати досліджень інтелектуальних систем керування у кіберфізичних середовищах. Показано залежність ефективності захисту від рівня інтеграції аналітичних модулів. Водночас залишаються відкритими питання масштабування

таких рішень у розподілених інформаційних системах. У дослідженні Фесьоха В. С., Субач І. Ю. [5] подано концептуальні підходи до підвищення кіберстійкості інформаційно-комунікаційних систем. Автори визначили основні параметри адаптації систем до змін загроз. Разом із тим недостатньо опрацьовано механізми кількісного оцінювання стійкості при високих навантаженнях.

У науковому бачені від групи Хлапонін Ю. І. та ін. [6] виділено функціональні складові систем захисту критичної інфраструктури. Показано роль структурного розподілу захисних механізмів. Проте не розкрито методи інтеграції цих компонентів у єдину аналітичну систему. У публікації Альджумая О. та ін. [7] проаналізовано ризики інформаційної інфраструктури на основі NIST-підходу. Наведено класифікацію загроз і вразливостей. Однак відсутня деталізація динамічних моделей оцінювання ризику в умовах змінних параметрів системи.

У дослідженні Бератас К. [8] розглянуто процеси виявлення та відновлення після кібератак. Показано важливість багаторівневого підходу до захисту. Разом із цим не вирішено питання оптимізації часу реагування з урахуванням ресурсних обмежень. У науковій публікації Гнатюк С., Побережна З., Заліський М. [9] досліджено взаємозв'язок кібербезпеки та економічної стійкості підприємства. Автори обґрунтували вплив інцидентів на фінансові результати. Водночас потребують уточнення моделі оцінювання непрямих втрат і репутаційних ризиків.

У монографії Гарасимчук О. [10] узагальнено сучасні методи захисту інформації з використанням штучного інтелекту та Blockchain. Визначено напрями інтеграції нових технологій у системи безпеки. Проте залишаються невирішеними питання узгодження цих технологій з існуючими корпоративними архітектурами. У дослідженні Ібаді Н. А. та ін. [12] було запропоновано комплексні стратегії підвищення рівня кіберзахисту інформаційних систем. Показано ефективність поєднання технічних і управлінських підходів. Разом із тим не деталізовано алгоритми адаптації систем до змін інтенсивності атак. Робота Марадова К. та ін. [16] виокремлює використання байєсівських мереж для підтримки рішень у сфері кібербезпеки. Автори продемонстрували можливість прогнозування інцидентів. Водночас потребують розвитку методи інтеграції таких моделей у реальні системи моніторингу.

Постановка завдання. Мета дослідження – запропонувати інтегрований підхід до забезпечення кіберстійкості для сучасних інформаційних систем.

Задачі дослідження:

– сформувати модель кількісного оцінювання кіберризиків;

– обґрунтувати архітектуру інтегрованої системи кіберзахисту;

– розробити заходи підвищення кіберстійкості інформаційних систем.

Виклад основного матеріалу. Цифрова інфраструктура підприємств змінює структуру ризиків і операційні процеси. Зростає частка розподілених сервісів, мобільних пристроїв і віддалених доступів. Внаслідок цього зростає кількість точок входу для атак. Паралельно збільшується обсяг даних, що циркулюють між системами. Кожен елемент інфраструктури формує окремий вектор загрози. Складність мереж ускладнює контроль доступу і моніторинг подій. Інженери фіксують зміну структури атак за останні роки. Поширюються комбіновані сценарії, що поєднують технічні та поведінкові впливи. Хакери використовують автоматизовані інструменти для сканування вразливостей. Далі вони переходять до етапу експлуатації через слабкі конфігурації. Значна частина інцидентів виникає через помилки доступу або невчасне оновлення систем. Водночас збільшується кількість атак на хмарні сервіси та API [15, с. 38].

Керівники IT-підрозділів фокусуються на підтримці безперервності процесів. Збої в інформаційних системах призводять до втрат доходів і контрактів. Витрати на відновлення після атак часто перевищують інвестиції в захист. У цьому контексті безпека інтегрується в операційні моделі підприємства. Контроль ризиків переходить від періодичних перевірок до постійного моніторингу. З технічної точки зору, структура кібербезпеки складається з кількох рівнів. Кожен рівень виконує окрему функцію контролю і захисту. На рівні мережі реалізуються механізми фільтрації й сегментації. На рівні додатків застосовуються методи контролю доступу і шифрування. На рівні користувачів діють політики автентифікації та поведінкового аналізу. Для оцінки змін у структурі загроз доцільно використовувати кількісні показники [17]. Дані моніторингу дозволяють відстежувати динаміку інцидентів (табл. 1).

Аналіз показує зміщення акценту від традиційних атак до комбінованих сценаріїв. Найшвидше зростають атаки через API та соціальну інженерію. Час виявлення інцидентів залишається значним. Проблематика вразливостей тісно

пов'язана з архітектурою інформаційних систем. Розподілені середовища містять різнорідні компоненти. Кожен компонент має власні конфігурації і політики доступу. Відсутність централізованого контролю створює додаткові ризики. Часто вразливості виникають через несумісність версій програмного забезпечення. Значна частина інцидентів пов'язана з людським фактором. Працівники використовують слабкі паролі або повторюють їх у різних системах. Операційні служби впроваджують системи постійного контролю подій. Використовуються SIEM-платформи та системи поведінкової аналітики. Вони збирають журнали подій і виявляють відхилення від нормальної активності [19, с. 128-129]. У таблиці 2 наведено оцінку ефективності методів виявлення загроз.

Результати демонструють перевагу інтелектуальних методів. Вони забезпечують швидшу реакцію і вищу точність. Проте їх впровадження потребує ресурсів і підготовки персоналу. Традиційні методи залишаються базовим рівнем захисту.

Інженерні підходи до захисту інформаційних систем базуються на розподіленій обробці подій. Потоки телеметрії надходять із мережевих пристроїв, серверів і прикладних сервісів. На edge-рівні виконується попередня фільтрація і локальна кореляція інцидентів. Далі агреговані дані передаються у хмарні аналітичні вузли. Така схема знижує затримки обробки та підвищує точність детекції.

Архітектура захисту включає кілька незалежних контурів контролю. Перший контур відповідає за перевірку мережевих з'єднань і сегментацію трафіку. Другий рівень аналізує запити до сервісів і контролює права доступу. Третій контур обробляє поведінкові патерни користувачів. Кожен рівень генерує власні метрики стану безпеки. Взаємодія між контурами здійснюється через централізовану шину подій. Оцінювання ризику виконується через багатофакторну функцію, що враховує динаміку загроз, інтенсивність атак і стан ресурсів [18, с. 217]:

$$R^* = \sum_{i=1}^{n}\left[\omega_i\left(\sum_{j=1}^{m}\frac{P_{ij}V_{ij}^2C_{ij}\ln(1+E_{ij})}{1+\exp\left(-\alpha_{ij}\text{”}\,t_{ij}\right)}\right)\cdot\left(1+\frac{L_i^{\gamma}}{(L_i^{\max})^{\gamma}+\varepsilon}\right)\right]. \quad (1)$$

де:
R^* – інтегральний ризик системи;
P_{ij} – ймовірність атаки;
V_{ij} – коефіцієнт вразливості;
C_{ij} – критичність активу;
E_{ij} – очікувані втрати;
α_{ij} – параметр чутливості до часу;
Δt_{ij} – тривалість інциденту;
L_i – навантаження вузла;
γ – показник нелінійності;
ω_i – вага вузла.

Збільшення навантаження підсилює вплив ризику через степеневу функцію. Логарифмічний множник відображає насичення втрат при великих значеннях збитків. У межах SOC-контурів застосовуються алгоритми кореляції подій. Система враховує помилки класифікації та часові затримки реагування. Для оцінки ефективності використовується наступна функція:

Таблиця 1

Динаміка та структура кіберзагроз у цифровому середовищі [3, 10]

Тип загрози	Частка інцидентів, %	Темп зростання, %	Джерело атаки	Середній час виявлення, год.	Рівень критичності
Malware	28	12	Зовнішній	36	Високий
DDoS	19	15	Зовнішній	12	Високий
Phishing	17	22	Людський фактор	48	Середній
Insider threat	11	9	Внутрішній	72	Високий
API attacks	14	18	Зовнішній	24	Високий
Misconfiguration	11	13	Організаційний	60	Середній

Таблиця 2

Порівняльна ефективність методів виявлення кіберінцидентів [11, 16]

Метод	Точність виявлення, %	Час реакції, хв.	Рівень автоматизації	Складність впровадження
Сигнатурний аналіз	72	10	Низький	Низька
Поведінковий аналіз	88	6	Середній	Середня
AI-моделі	93	3	Високий	Висока
SIEM	85	8	Середній	Середня
UEBA	90	5	Високий	Висока
IDS/IPS	80	7	Середній	Середня
Threat intelligence	87	9	Середній	Середня

$$E^*_{SOC} = \frac{\sum_{s=1}^{h} \eta_s \left(\frac{N_s^{det}}{N_s^{all}}\right)\left(1 - \frac{FP_s^2 + FN_s^2}{(N_s^{all})^2}\right) \cdot \exp\left(-\rho_s T_s^{resp}\right)}{\sum_{s=1}^{h} \eta_s} \cdot \left(1 - \frac{C_{op}^{\delta}}{(C_{op}^{\max})^{\delta}}\right). \quad (2)$$

де:
E^*_{SOC} – інтегральна ефективність системи моніторингу;
N_s^{det} – виявлені інциденти;
FP_s, FN_s – помилки класифікації;
T_s^{resp} – час реагування;
ρ_s – коефіцієнт штрафу за затримку;
C_{op} – операційні витрати;
δ – коефіцієнт нелінійності витрат.

Експоненційна складова знижує ефективність при збільшенні часу реагування. Квадрати помилок підсилюють їх вплив на загальний показник. Аналіз поведінки користувачів виконується через нормовану багатовимірну функцію відхилення:

$$A_u^* = \sqrt{\sum_{k=1}^{p} \lambda_k \left(\frac{x_{uk} - \mu_{uk}}{\sigma_{uk}}\right)^4} + \gamma \sum_{r=1}^{q} \left| \frac{f_{ur} - \hat{f}_{ur}}{\hat{f}_{ur} + \varepsilon} \right|^2. \quad (3)$$

де:
A^*_u – показник аномальності;
x_{uk} – поточні параметри поведінки;
μ_{uk}, σ_{uk} – статистичні характеристики;
λ_k – вагові коефіцієнти;
f_{ur} – фактична частота дій;
$\hat{f}_{ur}$ – прогноз.

Підвищення ступеня у формулі підсилює чутливість до відхилень, що надаватиме швидкості при виявленні нестандартної активності (табл. 3).

Інтеграція компонентів виконується через гібридну модель обробки даних. Edge-вузли виконують локальну фільтрацію і швидке реагування. Хмарні платформи забезпечують довготривале зберігання і навчання моделей. Така структура підтримує масштабованість системи. Кіберстійкість мережі визначається через комплексний показник:

$$S^* = \frac{\sum_{i=1}^{n} \omega_i \left[\beta_1 \left(\frac{1}{MTTD_i}\right)^{\theta} + \beta_2 \left(\frac{1}{MTTR_i}\right)^{\theta} + \beta_3 U_i^{\phi} + \beta_4 A_i^{\psi} + \beta_5 \left(1 - \frac{R_i}{R_i^{\max}}\right)^{\xi}\right]}{\sum_{i=1}^{n} \omega_i}. \quad (4)$$

де:
S^* – інтегральна кіберстійкість;
$MTTD_i$, $MTTR_i$ – часові параметри;
U_i – надійність;
A_i – доступність;
θ, ϕ, ψ, ξ – параметри нелінійності.

Показник зменшується при зростанні часу реагування або ризику. Збільшення надійності та доступності підвищує стійкість системи (табл. 4).

Оптимізація архітектури виконується через мінімізацію сукупних витрат і ризиків:

$$J^* = \min\left\{\sum_{r=1}^{z} C_r x_r + \phi \sum_{i=1}^{n} R_i(x) + \psi \sum_{i=1}^{n} \frac{T_i^{det}(x) + T_i^{resp}(x)}{T_i^{crit}} - \chi \sum_{i=1}^{n} S_i(x)\right\}. \quad (5)$$

де:
x_r – змінні вибору механізмів захисту;
C_r – витрати;
$R_i(x)$ – ризик;
T_i^{det}, T_i^{resp} – часові параметри;
$S_i(x)$ – стійкість.

Модель буде враховувати баланс між витратами і рівнем захисту. Підбір параметрів виконується з урахуванням обмежень ресурсів і вимог безпеки. Організації перебудовують кіберза-

Таблиця 3

Технічні параметри функціонування модулів кіберзахисту

Модуль	Частота обробки, подій/с	Затримка, мс	Точність, %	Навантаження CPU, %	Коефіцієнт помилок
SIEM ядро	15000	120	91	68	0,08
UEBA модуль	9000	95	94	72	0,05
IDS/IPS	12000	110	88	65	0,12
AI детектор	8000	70	96	78	0,04
Log collector	20000	50	85	55	0,15
Correlation engine	11000	130	92	74	0,07
Edge analyzer	6000	40	89	48	0,10
Cloud processor	14000	150	95	82	0,06

Таблиця 4

Аналітична оцінка кіберстійкості корпоративної мережі

Вузол	MTTD, хв	MTTR, хв	Рівень ризику	Доступність	Індекс стійкості
Сервер 1	15	40	0,32	0,96	0,71
Сервер 2	12	35	0,28	0,97	0,76
DB вузол	20	55	0,41	0,94	0,63
API шлюз	10	30	0,25	0,98	0,81
Edge вузол	8	25	0,22	0,99	0,85
Cloud кластер	18	45	0,30	0,97	0,74

хист через поєднання управлінських і технічних рішень. Політики доступу узгоджуються з архітектурою сервісів і структурою даних. Кожен бізнес-процес отримує власний профіль ризику. Для цього використовуються журнали подій, фінансові показники та метрики доступності. Паралельно формується карта критичних активів з прив'язкою до інфраструктури (рис. 1).

Під час формування кіберстратегії застосовується багатокритеріальна оцінка стану системи [14]. Розрахунок інтегрує відповідність стандартам, технічний рівень захисту та управлінські фактори:

$$G^{sec} = \sum_{i=1}^{n} \omega_i \left[\frac{C_i^{std} \cdot K_i^{ctrl} \cdot A_i^{proc}}{1 + \exp(-\alpha_i t_i)} + \frac{L_i^{comp}}{L_i^{max} + \varepsilon} \right]. \quad (6)$$

де:
G^{sec} – інтегральний показник зрілості кіберстратегії;
C_i^{std} – рівень відповідності стандартам;
K_i^{ctrl} – ефективність контрольних механізмів;
A_i^{proc} – узгодженість із бізнес-процесами;
L_i^{comp} – рівень комплаєнсу;
t_i – тривалість функціонування системи;
ω_i – вага компонента.

Функція враховує динаміку розвитку системи та ступінь інтеграції політик безпеки. Операційні підрозділи виконують управління ризиками через циклічну модель. Вона включає виявлення загроз, їх кількісну оцінку та вибір заходів реагування. Для розрахунку оптимального сценарію використовується залежність виду:

$$R^{opt} = \min \left\{ \sum_{j=1}^{m} \left(P_j \cdot D_j \cdot \ln(1 + \tau_j) \right) - \sum_{k=1}^{p} \left(E_k \cdot S_k^{\beta} \right) \right\}. \quad (7)$$

де:
R^{opt} – оптимізований рівень ризику;
P_j – ймовірність інциденту;
D_j – величина втрат;
τ_j – тривалість інциденту;

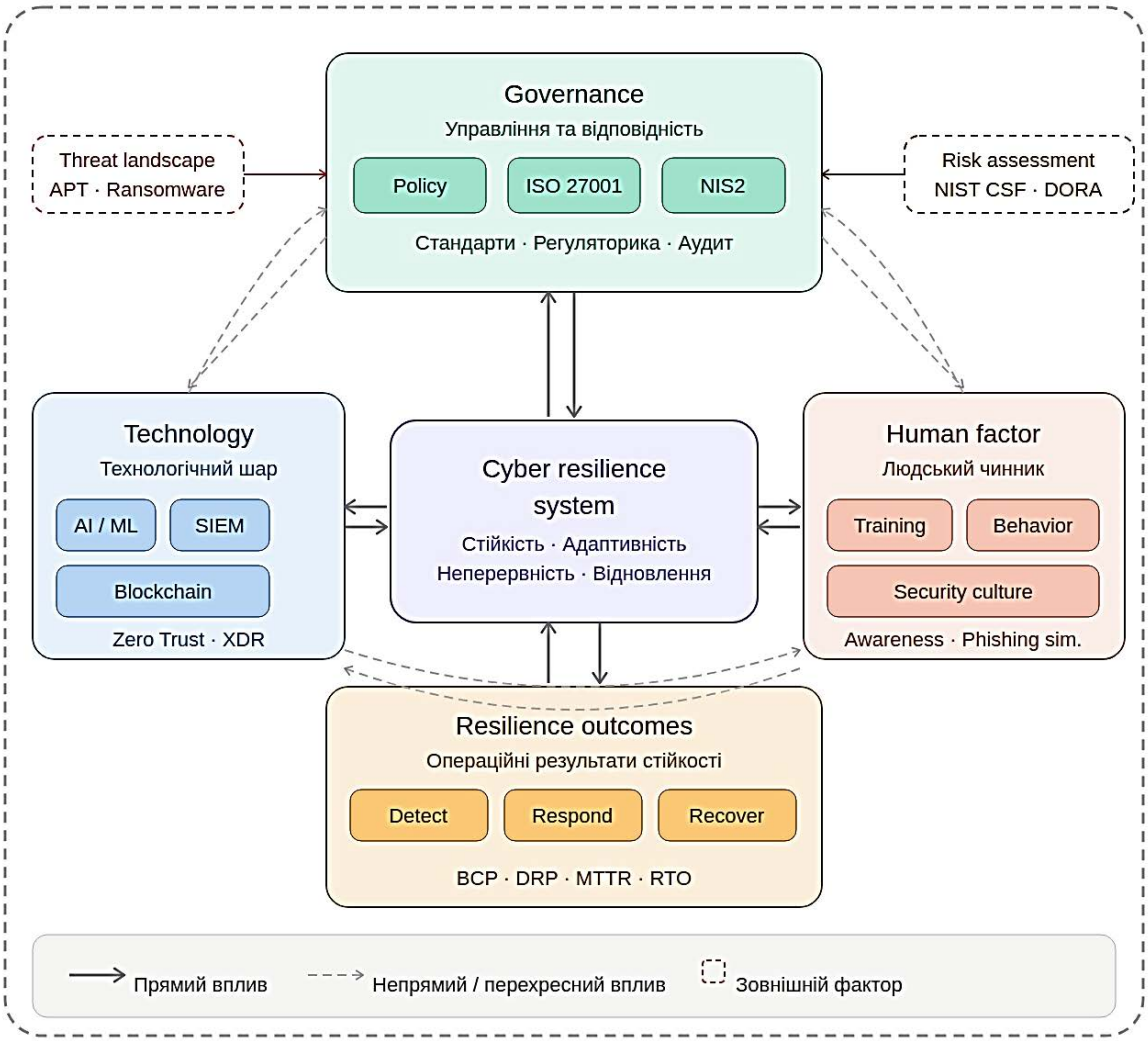

Рис. 1. Інтегрована модель кіберстійкої інформаційної системи (розроблено автором в середовищі SolidWorks)

E_k – ефективність заходів захисту;
S_k – рівень покриття системи захистом;
β – коефіцієнт впливу заходів.

Модель враховує одночасно втрати і ефективність захисних механізмів. Інтелектуальні системи детекції атак використовують комбіновані алгоритми. Вони інтегрують нейронні мережі та статистичні моделі. Обробка даних виконується у режимі потокового аналізу. Для визначення рівня загрози формується новий показник:

$$T^{AI} = \sum_{i=1}^{n} \lambda_i \left[\left(\frac{x_i - \mu_i}{\sigma_i} \right)^2 + \gamma_i \left(\frac{f_i - \hat{f}_i}{\hat{f}_i + \varepsilon} \right)^2 \right] \cdot \exp(-\delta_i t). \quad (8)$$

де:
T^{AI} – рівень загрози;
x_i – поточні параметри системи;
μ_i, σ_i – статистичні характеристики;
f_i, $\hat{f}_i$ – фактичні і прогнозовані значення;
δ_i – коефіцієнт затухання.

Показник реагує на відхилення та зменшується при стабілізації системи. Інженерна реалізація механізмів захисту потребує узгодження технологій із параметрами навантаження, затримок і точності детекції. Вибір рішень здійснюється з урахуванням частоти оновлення, рівня ризику та вартості впровадження. В таблиці 5 подано систематизовані пропозиції щодо інтеграції компонентів кіберзахисту в корпоративну інфраструктуру з характеристиками їхньої ефективності.

Захист даних доповнюється технологіями розподіленого зберігання. Blockchain використовується для фіксації подій і забезпечення незмінності записів. Кожен блок містить хеш попереднього стану системи. Це унеможливлює приховане редагування журналів. Цифрові двійники систем безпеки застосовуються для моделювання атак. Вони відтворюють структуру мережі та поведінку сервісів. Під час симуляції система тестує різні сценарії загроз [13]. Результати використовуються для оптимізації конфігурацій. Вплив людського фактора враховується через поведінкові індекси. Для оцінки ризику користувачів вводимо таку функцію:

$$H^{risk} = \sum_{u=1}^{k} \theta_u \left[\frac{A_u^{anom}}{A_u^{max}} + \frac{E_u^{err}}{E_u^{tot}} \right] \cdot (1 + \ln(1 + t_u)). \quad (9)$$

де:
H^{risk} – ризик; пов'язаний з користувачами;

Таблиця 5

Пропозиції щодо впровадження механізмів кіберзахисту в корпоративних системах (сформовано автором)

Компонент	Тип технології	Частота оновлення	Рівень ризику	Вартість впровадження	Очікуваний ефект	Пріоритет
SIEM	Аналітика подій	5 хв	Високий	Висока	Зниження інцидентів	1
AI детектор	ML	1 хв	Високий	Висока	Рання детекція	1
Blockchain логування	Розподілені системи	10 хв	Середній	Середня	Цілісність даних	2
Zero Trust	Контроль доступу	Постійно	Високий	Середня	Обмеження доступу	1
SOC центр	Моніторинг	24/7	Високий	Висока	Швидке реагування	1
Edge аналіз	Локальна обробка	30 сек	Середній	Середня	Зменшення затримок	2
Threat intelligence	Дані загроз	1 год	Середній	Низька	Прогнозування атак	3

Таблиця 6

Пропозиції щодо підвищення кіберстійкості інформаційних систем (сформовано автором)

Захід	Тип впливу	Частота реалізації	Зменшення ризику	Витрати	Час впровадження	Результат
Навчання персоналу	Організаційний	1 раз/квартал	18%	Низькі	2 тижні	Зниження помилок
Оновлення ПЗ	Технічний	1 раз/місяць	25%	Середні	1 тиждень	Закриття вразливостей
Впровадження AI	Технічний	Постійно	32%	Високі	2 місяці	Рання детекція
Zero Trust	Архітектурний	Постійно	28%	Середні	1 місяць	Контроль доступу
SOC розширення	Організаційний	Постійно	30%	Високі	3 місяці	Швидке реагування
Blockchain	Технічний	Постійно	20%	Середні	2 місяці	Захист даних
Edge інтеграція	Технічний	Постійно	22%	Середні	1 місяць	Зменшення затримок
Аудит безпеки	Контрольний	2 рази/рік	15%	Низькі	3 тижні	Виявлення проблем

A_u^{anom} – кількість аномалій;
E_u^{err} – кількість помилок;
t_u – тривалість активності.

Зростання активності без контролю підвищує значення ризику. Підвищення кіберстійкості досягається через поєднання організаційних і технічних заходів, що впливають на ризик, час реагування та стабільність сервісів [4, с. 10]. Оцінювання ефекту потребує кількісного порівняння витрат і результатів впровадження. У таблиці 6 наведено структуровані пропозиції щодо оптимізації системи захисту з урахуванням частоти реалізації та очікуваних змін показників.

Завершальний етап передбачає оптимізацію всієї системи кіберзахисту. Для цього використовується багатокритеріальна функція:

$$J^{final} = \min\left\{\sum_{r=1}^{z} C_r x_r + \phi\sum_{i=1}^{n} R_i + \psi\sum_{i=1}^{n}\frac{T_i^{det} + T_i^{resp}}{T_i^{crit}} - \chi\sum_{i=1}^{n} S_i\right\}. \quad (10)$$

де:
J^{final} – інтегральний критерій оптимізації;
C_r – витрати;
R_i – ризик;
T_i^{det}, T_i^{resp} – часові параметри;
S_i – стійкість системи.

Оптимізація виконується з урахуванням ресурсних обмежень. Система змінює конфігурації у відповідь на нові загрози. Такий підхід буде забезпечувати адаптивність і стабільність функціонування певної інформаційної інфраструктури.

Висновки. Дослідження підтвердило залежність кіберстійкості від узгодженості архітектурних і аналітичних компонентів захисту. Поєднання багаторівневого контролю доступу з потоковою обробкою подій скорочує час виявлення інцидентів. Застосовуючи нелінійні моделі оцінювання ризику, розробники точніше враховують динаміку загроз. Розподілена обробка даних підвищує ефективність моніторингу, одночасно знижуючи навантаження на центральні вузли.

Аналіз довів ефективність інтелектуальних алгоритмів у виявленні відхилень поведінки користувачів. Використання адаптивних моделей на основі статистичних методів зменшує кількість хибних спрацювань. Точність класифікації інцидентів зростає завдяки комбінуванню різних джерел даних. Інтеграція поведінкового аналізу в контури безпеки сприяє ранньому виявленню аномалій. Стабільність функціонування інформаційних систем прямо залежить від впровадження таких інструментів.

Отримані результати підтвердили доцільність використання комплексних критеріїв оптимізації кіберзахисту. Врахування витрат і часу реагування забезпечує прийняття збалансованих управлінських рішень. Запропоновані підходи адаптують конфігурації захисту до змін структури атак. Практичне застосування розроблених моделей підвищує надійність функціонування цифрової інфраструктури. Параметри залишкового ризику визначають кінцеву конфігурацію засобів протидії загрозам.

Список літератури:

1. Єсіна М. В., Логачова Є. О., Колованова Є. В. Дослідження та порівняння нормативних регуляторних документів Європейського Союзу у сфері кібербезпеки. *Computer Science and Cybersecurity*. 2025. № 1 (27). С. 123-131. DOI: https://doi.org/10.26565/2519-2310-2025-1-05

2. Костюк Ю. В., Складанний П. М., Рзаєва С. Л., Самойленко Ю. О., Коршун Н. В. Інтелектуальні системи керування та захисту в кіберфізичних і хмарних середовищах Smart Grid. *Кібербезпека: освіта, наука, техніка.* 2025. № 2 (30). С. 125-156. DOI: https://doi.org/10.28925/2663-4023.2025.30.956

3. Ларін С. В. Захист інформації в системі кібербезпеки як стратегічний пріоритет реалізації державних механізмів захисту національних цінностей в Україні. *Публічне управління та регіональний розвиток.* 2025. № 27. С. 278-294. DOI: https://doi.org/10.34132/pard2025.27.12

4. Македон В. В., Волошко Н. О. Вплив транснаціональних корпорацій на реалізацію цілей сталого розвитку. *Інфраструктура ринку.* 2023. Вип. 70. 2023. С. 8-14. DOI: https://doi.org/10.32782/infrastruct70-2.

5. Фесьоха В. С., Субач І. Ю. Концептуальна основа підвищення кіберстійкості інформаційно-комунікаційних систем в умовах еволюції кіберзагроз. *Кібербезпека: освіта, наука, техніка.* 2025. № 4 (28). С. 511-528. DOI: https://doi.org/10.28925/2663-4023.2025.28.856

6. Хлапонін Ю. І., Козубцова Л. М., Козубцов І. М., Штонда Р. В. Функції системи захисту інформації і кібербезпеки критичної інформаційної інфраструктури. *Кібербезпека: освіта, наука, техніка.* 2022. № 3 (15). С. 124-134. DOI: https://doi.org/10.28925/2663-4023.2022.15.1241341

7. Aljumaiah O., Jiang W., Reddy Addula S., Almaiah M. A. Analyzing cybersecurity risks and threats in IT infrastructure based on NIST framework. *Journal of Cyber Security and Risk Auditing.* 2025. Vol. 2025. No 2. pp. 12-26. DOI: https://doi.org/10.63180/jcsra.thestap.2025.2.2.

8. Beretas C. Information systems security, detection and recovery from cyber attacks. *Universal Library of Engineering Technology.* 2024. Vol. 1. No 1. pp. 27-40. DOI: https://doi.org/10.70315/uloap.ulete.2024.0101005

9. Gnatyuk S., Poberezhna Z., Zaliskyi M. Information security and protection from cyber attacks as a component of the economic security system of the enterprise. *CEUR Workshop Proceedings.* 2025. Vol. 4042. pp. 180-192.

10. Harasymchuk O. (Ed.) *Modern methods of ensuring information protection in cybersecurity systems using artificial intelligence and Blockchain technology: collective monograph.* Kharkiv: TECHNOLOGY CENTER PC. 2025. 132 p. DOI: http://doi.org/10.15587/978-617-8360-12-2

11. Hossain A., Islam M. T., Chowdhury B. R., Olajide A. O., Sani A. I., Hossain K., Sinha K. P., Altemimi M. A. H., Al Mamun M. A. Advancements in cybersecurity for managements information systems. *Membrane Technology*. 2024. Vol. 2024. No 6. pp. 16-16. DOI: https://doi.org/10.52710/mt.271

12. Ibadi N. A., Ibrahim S. K., Najem W. M., Hadi T. H. Innovative strategies for enhancing cybersecurity in information systems: a holistic approach in computer engineering. *Journal of Information Systems Engineering and Management.* 2025. Vol. 10. No 35s. pp. 826-839. DOI: https://doi.org/10.52783/jisem.v10i35s.6151

13. Kamariotou M., Kitsios F. Information systems strategy and security policy: a conceptual framework. *Electronics.* 2023. Vol. 12. No 2. pp. 1-12. DOI: https://doi.org/10.3390/electronics12020382

14. KPMG International. *Cybersecurity considerations 2025.* 2025. 44 p. URL: https://assets.kpmg.com/content/dam/kpmgsites/cn/pdf/en/2025/04/cybersecurity-considerations-2025.pdf

15. Makedon V., Koptilyi D. Digital transformation and artificial intelligence as factors in the economic recovery of enterprises following armed conflicts. *Economics, Entrepreneurship, Management.* 2025. Vol. 12. No 1. pp. 33-48. DOI: https://doi.org/10.56318/eem2025.01.033

16. Maradova K., Blecha P., Samelova V., Marada T., Zuth D. Bayesian networks for cybersecurity decision support: enhancing human-machine interaction in technical systems. *Applied Sciences.* 2026. Vol. 16. No 6. pp. 3053-3053. DOI: https://doi.org/10.3390/app16063053

17. Olzak T. Top ten cybersecurity concerns in 2026 and how to manage them. *LinkedIn/ResearchGate. 2026.* 13 p. DOI: https://doi.org/10.13140/RG.2.2.16877.45288

18. Panteli N., Nthubu B. R., Mersinas K. Being responsible in cybersecurity: a multi-layered perspective. *Information Systems Frontiers.* 2026. Vol. 28. pp. 209-227. DOI: https://doi.org/10.1007/s10796-025-10588-0

19. Ramskyi I., Drozd A., Lyhun O., Ponochovna O. System for cybersecurity evaluation of corporate networks. *Computer Systems and Information Technologies.* 2025. No 2. pp. 123-131. DOI: https://doi.org/10.31891/csit-2025-2-14

Marchenko O.I. ENSURING CYBERSECURITY OF INFORMATION SYSTEMS UNDER THE CONDITIONS OF INCREASING CYBER THREATS IN THE DIGITAL ENVIRONMENT

The purpose of the study is to develop an applied approach to enhancing the cyber resilience of information systems. The approach combines analytical models with multi-layered security architectures and intelligent attack detection mechanisms. The work focuses on the relationships between system performance parameters and the effectiveness of protective measures. Formalization of risk assessment processes ensures the selection of optimal solutions for infrastructure stability. The research methodology integrates mathematical modeling, streaming data analysis, and machine learning. The authors applied approaches that account for temporal characteristics of incidents and the vulnerability level of assets. By analyzing system load, behavioral analysis models were integrated with classification algorithms. Analytical calculations and comparison of monitoring indicators were used to validate the effectiveness of the proposed approach. The evaluation is based on verifying the resilience parameters of computational resources.

The application of integrated models increases the accuracy of incident identification while reducing overall response time. The combination of distributed data processing with centralized analytics ensures effective monitoring of network conditions. The level of cyber resilience directly depends on the consistency between architectural components and analytical modules. The use of intelligent algorithms minimizes false positives in threat classification. This enables administrators to localize intrusion vectors more rapidly. The practical significance of the results lies in implementing the proposed mechanisms within corporate information systems. The developed solutions adapt to changing operating conditions and scale efficiently in distributed environments. These tools optimize security costs and reduce potential losses from cyber incidents. The scientific novelty of the study consists in the development of a comprehensive analytical framework for resilience assessment. The proposed model integrates technical, behavioral, and economic parameters of protection. The obtained results extend the capabilities of modeling security processes and support the development of adaptive security systems.

Keywords: *information systems cybersecurity, cyber risk, cyber resilience, intelligent security systems, SOC-SIEM systems, adaptive security models.*

Дата першого надходження статті до видання: 25.03.2026
Дата прийняття статті до друку після рецензування: 21.04.2026
Дата публікації (оприлюднення) статті: 19.05.2026