Вимога	Компонент	Вектор загрози	Механізм контролю	Метрика
Доступність сервісу прогнозування	Сервіс прогнозування	Availability / Energy-latency Attacks (NIST)	Обмеження частоти, тайм-аути обчислень	SLA доступності, p95 latency
Авторизованість запитів	Шар інтеграції	Model Extraction (NIST; OWASP ML05)	Автентифікація API, rate limiting	Частка авторизованих запитів

Висновки. Запропонований метод дозволяє розглядати безпеку СПА як архітектурно інтегровану нефункціональну характеристику, що підвищує верифіковність архітектурних рішень. Подальші дослідження передбачають експериментальну валідацію методу на прототипі СПА для задач прогнозування відтоку клієнтів та динамічного ціноутворення.

1. Vassilev A., Oprea A., Fordyce A., Anderson H., Davies X., Hamin M. Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations. NIST AI 100-2 E2025. Gaithersburg: NIST, 2025. DOI: 10.6028/NIST.AI.100-2e2025.
2. OWASP Machine Learning Security Top 10. 2023 edition. URL: https://mltop10.info/ (дата звернення: 06.05.2026).
3. MITRE ATLAS: Adversarial Threat Landscape for Artificial-Intelligence Systems. URL: https://atlas.mitre.org/ (дата звернення: 06.05.2026).
4. ISO/IEC 23894:2023. Information technology — Artificial intelligence — Guidance on risk management. Geneva: ISO, 2023. 28 p.

Оцінювання рівня інформаційної безпеки державних інформаційних ресурсів

УДК 004.056

Валентина Ящук[1], Діана Рівняк[2]

Львівський державний університет безпеки життєдіяльності,
[1]valentina.lender@gmail.com, [2]dianarivnak@gmail.com

У сучасних умовах цифровізації державного управління та зростання інтенсивності кіберзагроз проблема забезпечення належного рівня інформаційної безпеки державних інформаційних ресурсів набуває стратегічного значення. Державні інформаційні ресурси є основою функціонування електронного урядування, а їх компрометація може призвести до значних соціально-економічних і політичних наслідків. Це обумовлює необхідність розроблення ефективних методів оцінювання рівня їх захищеності. Метою роботи є розроблення математичної моделі оцінювання рівня інформаційної безпеки державних інформаційних ресурсів на основі інтегрального підходу з використанням системи індикаторів та вагових коефіцієнтів.

Аналіз існуючих підходів до оцінювання інформаційної безпеки показує, що більшість із них базується на якісних або експертних оцінках, що знижує об’єктивність результатів. Перспективним є застосування кількісних моделей,

які дозволяють формалізувати процес оцінювання та забезпечити порівнюваність результатів.

Нами запропоновано методологію оцінювання, яка передбачає формування системи індикаторів безпеки, що охоплюють такі складові, як рівень захищеності інформаційних систем, ефективність механізмів контролю доступу, стійкість до кіберзагроз та здатність до реагування на інциденти. Для кожного індикатора визначаються відповідні метрики, що дозволяють здійснювати кількісну оцінку стану безпеки. Такий підхід передбачає представлення рівня інформаційної безпеки у вигляді інтегрального показника:

$$I_{sec} = \sum_{i=1}^{n} w_i * S_i \quad (1),$$

де I_{sec} — інтегральний показник рівня інформаційної безпеки;

S_i — значення і-го індикатора безпеки;

w_i — ваговий коефіцієнт важливості відповідного індикатора;

n — кількість індикаторів.

Система індикаторів формується за основними складовими інформаційної безпеки, зокрема конфіденційність інформації, цілісність даних; доступність ресурсів, автентичність та контроль доступу, стійкість до кіберінцидентів. Кожен індикатор оцінюється за шкалою від 0 до 1, де 0 відповідає критичному рівню вразливості, а 1 — повній відповідності вимогам безпеки. Значення індикаторів визначаються на основі аналізу технічних параметрів систем, результатів аудиту безпеки та даних моніторингу.

Для врахування ризиків інформаційної безпеки пропонуємо використовувати коригуючий коефіцієнт ризику.

$$R = \sum_{j=1}^{m} p_j * d_j \quad (2),$$

де R — інтегральний ризик;

p_j — ймовірність реалізації j-ої загрози;

d_j — потенційні збитки від реалізації загрози;

m — кількість загроз.

Відтак з урахуванням ризику інтегральний показник безпеки набуває такого вигляду.

$$I_{sec}^{*} = I_{sec} * (1 - R) \quad (3)$$

Отже, інтегральну оцінку рівня інформаційної безпеки пропонується визначати на основі агрегування часткових показників із використанням вагових коефіцієнтів, що враховують критичність окремих компонентів системи. Такий підхід забезпечує можливість отримання узагальненого показника, який відображає поточний стан захищеності державних інформаційних ресурсів та потенційний вплив загроз на інформаційні ресурси.

Наукова новизна роботи полягає у розробленні інтегрованої моделі оцінювання рівня інформаційної безпеки, яка поєднує індикаторний підхід із ризик-орієнтованим аналізом, що забезпечує підвищення точності та

об'єктивності оцінювання. Практичне значення полягає у можливості застосування запропонованої моделі для проведення аудиту інформаційної безпеки державних інформаційних систем; підтримки прийняття управлінських рішень; визначення пріоритетних напрямів підвищення рівня захищеності; моніторингу змін стану інформаційної безпеки у динаміці.

Результати дослідження свідчать, що використання інтегрального показника дозволяє отримати узагальнену оцінку стану інформаційної безпеки та своєчасно виявляти критичні вразливості. Запропонована модель є гнучкою та може бути адаптована до специфіки конкретних державних інформаційних систем.

У роботі запропоновано модель оцінювання рівня інформаційної безпеки державних інформаційних ресурсів на основі інтегрального показника та ризикоорієнтованого підходу. Використання системи індикаторів та вагових коефіцієнтів дозволяє здійснювати кількісну оцінку стану захищеності інформаційних систем. Запропонований підхід забезпечує підвищення об'єктивності оцінювання та може бути використаний у практиці управління інформаційною безпекою державного сектору.

1. Ящук В., Балацька В. Підвищення кіберстійкості критичної інформаційної інфраструктури держави через вдосконалення процесів реагування на кіберінциденти // Цивільний захист в умовах війни : збірник тез доповідей II Міжнародної науково-практичної конференції, м. Львів, 15 квітня 2026 року. Львів : ЛДУБЖД, 2026. С. 92–95.
2. Венгерський П.С., Вишневська Н.С., Хохлачова Ю.Є., Хорошко В.О., Чобаль О.І. Кількісна оцінка кіберзахищеності інформації. Захист інформації. 2023. Т. 25, №2. С. 53–61.

Проблеми інтервального моніторингу цілісності інформаційного стану корпоративних кіберфізичних систем

УДК 004.056:681.5

Павло Матусяк[1], Ярослав Тарасенко[2]

[1]Державний університет інформаційно-комунікаційних технологій, Pavelmatusyak@gmail.com,
[2]Державний науково-дослідний інститут випробувань і сертифікації озброєння та військової техніки, yaroslav.tarasenko93@gmail.com

В умовах цифровізації виробничих і сервісних процесів корпоративні кіберфізичні системи виступають у ролі середовища з особливими ознаками порушення безпеки. Вторгнення у такому середовищі супроводжується поступовим спотворенням сукупності контрольованих параметрів на відміну від миттєвих відмов, спричинених порушенням цілісності інформаційного стану. Під цілісністю інформаційного стану мається на увазі збереження узгодженості, допустимості та відсутності спотворення поточних оцінок параметрів у часі. Для корпоративних кіберфізичних систем таке формулювання набуває особливого значення через можливість накопичення