

УДК 004.056

DOI <https://doi.org/10.36994/2788-5518-2026-01-11-06>

МАТЕМАТИЧНА МОДЕЛЬ ІНТЕГРАЛЬНОГО ОЦІНЮВАННЯ РІВНЯ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ В ІТС НА ОСНОВІ ІНДИКАТОРІВ SIEM-СИСТЕМ

Писарчук О. О., д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна. <https://orcid.org/0000-0001-5271-0248>, platinumpa2212@gmail.com

Кошара А. В., аспірант, Відкритий міжнародний університет розвитку людини «Україна», Київ, Україна. <https://orcid.org/0009-0000-8468-2704>, artemkosharaa@gmail.com

Анотація. У статті запропоновано математичну модель інтегрального оцінювання рівня загроз інформаційній безпеці в інформаційно-телекомунікаційних системах на основі індикаторів, сформованих на підставі даних SIEM-систем. Актуальність дослідження зумовлена зростанням інтенсивності та комбінованим характером кіберзагроз, за яких окремий аналіз подій безпеки вже не забезпечує достатньої повноти оцінювання стану захищеності. Обґрунтовано доцільність переходу від аналізу розрізнених подій і параметрів стану системи до формалізованої сукупності кількісних індикаторів для подальшого багатofакторного оцінювання. Проведено формалізацію системи індикаторів загроз, поділену на дві взаємопов'язані групи: подієві індикатори та індикатори стану компонентів інформаційно-телекомунікаційної системи. Подієві індикатори визначено як нормовані агреговані оцінки подій безпеки за заданий інтервал спостереження з урахуванням вагових коефіцієнтів, що відображають критичність окремих подій, їхній потенційний вплив на систему та значущість у загальній структурі загроз. Індикатори стану подано як відносні показники, що характеризують частку компонентів системи, для яких виявлено відповідні ознаки ризику, зокрема наявність вразливостей, застарілого або неліцензованого програмного забезпечення, а також некоректний стан засобів захисту. На основі сформованої системи індикаторів побудовано інтегральну модель оцінювання рівня загроз у вигляді зваженої лінійної згортки нормованих показників. Для визначення вагових коефіцієнтів індикаторів застосовано метод аналізу ієрархій, що дозволив формалізувати їхню відносну важливість, отримати узгоджену систему ваг і забезпечити інтерпретованість інтегральної оцінки. Запропонований підхід забезпечує приведення різних за природою та масштабом показників до єдиної шкали, що створює методичну основу для комплексного аналізу стану захищеності системи. Отримані результати підтвердили логічну узгодженість моделі, її чутливість до зміни значень найбільш вагомих індикаторів та можливість практичного використання для багатofакторного оцінювання рівня загроз. Продемонстровано, що модель може бути використана як аналітична основа для підтримки прийняття рішень у процесах моніторингу безпеки, виявлення небезпечних тенденцій і подальшого розвитку засобів інтелектуалізованої оцінки стану захищеності ІТС.

Ключові слова: SIEM, індикатори загроз, формалізація, інформаційна безпека, інтегральне оцінювання, математична модель, метод аналізу ієрархій, інформаційно-телекомунікаційні системи, аналіз подій безпеки.

A MATHEMATICAL MODEL FOR THE INTEGRAL ASSESSMENT OF INFORMATION SECURITY THREAT LEVELS IN INFORMATION AND TELECOMMUNICATION SYSTEMS BASED ON SIEM INDICATORS

Oleksii Pysarchuk, Dr Habil., Prof., National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine. <https://orcid.org/0000-0001-5271-0248>, platinumpa2212@gmail.com

Artem Koshara, PhD Student, Open International University of Human Development "Ukraine", Kyiv, Ukraine. <https://orcid.org/0009-0000-8468-2704>, artemkosharaa@gmail.com

Abstract. This article proposes a mathematical model for the comprehensive assessment of information security threats in information and telecommunications systems based on indicators derived from SIEM systems. The relevance of the study is driven by the increasing intensity and combined nature of cyber threats, which means that a separate analysis of security events no longer provides a sufficiently comprehensive assessment of the security status. The feasibility of transitioning from analysing isolated events and system state parameters to a formalized set of quantitative indicators for subsequent multifactorial assessment is substantiated. A formalization of the system of threat indicators has been carried out, which is divided into two interrelated groups: event indicators and indicators of

the state of components of the thinformation and telecommunications system. Event indicators are defined as normalized, aggregated assessments of security events over a given observation interval, incorporating weighting coefficients that reflect the criticality of individual events, their potential impact on the system, and their significance within the overall threat structure. Status indicators are presented as relative metrics that characterize the proportion of system components for which relevant risk signs have been detected, specifically the presence of vulnerabilities, outdated or unlicensed software, and incorrect security measures. Based on the developed indicator system, an integrated model for assessing the threat level has been constructed as a weighted linear combination of the normalized indicators. To determine the weighting coefficients of the indicators, a hierarchical analysis method was applied, which formalized their relative importance, yielded a consistent system of weights, and ensured the interpretability of the integrated assessment. The proposed approach ensures the conversion of indicators that are heterogeneous in nature and scale to a single scale, creating a methodological basis for a comprehensive analysis of the system's security status. The results confirmed the model's logical consistency, its sensitivity to changes in the values of the most significant indicators, and its practical applicability to multifactorial threat-level assessment. It has been demonstrated that the model can serve as an analytical basis for decision-making in security monitoring processes, for identifying dangerous trends, and for further developing means for the intelligent assessment of the security status of ITS.

Key words: SIEM, threat indicators, formalization, information security, integral assessment, mathematical model, analytic hierarchy process, information and telecommunication systems, security event analysis.

Вступ

Актуальність оцінювання рівня інформаційної безпеки інформаційно-телекомунікаційних систем у державному секторі є беззаперечною. Порушення конфіденційності, цілісності або доступності інформації тут не обмежується локальним інцидентом, оскільки здатне спричинити збої критичних сервісів, ускладнювати управлінські процеси та порушувати міжвідомчу взаємодію. Масштаб таких наслідків визначається не лише технічними характеристиками, а й місцем конкретної ІТС у загальній інфраструктурі.

Посилення інтенсивності атак підтверджують галузеві аналітичні звіти. У 2025 році у Data Breach Investigations Report компанії Verizon зафіксовано зростання частки системного проникнення серед основних типів порушень. Для державного сектору, зокрема, характерною є значна частка атак соціальної інженерії, експлуатації вебзастосунків і зловживання привілеями [1]. Аналогічні тенденції відзначено й у Microsoft Digital Defense Report 2025, де увагу зосереджено на використанні відомих вразливостей веб-ресурсів і віддалених сервісів [2]. Окремо автори звіту підкреслюють, що розвиток штучного інтелекту посилює як засоби захисту, так і інструменти для атакуючої сторони. У Global Threat Report 2026 компанія CrowdStrike також фіксує різке зростання вішинг-операцій упродовж 2024 року [3]. Сучасні інциденти дедалі рідше мають ізольований характер. На практиці йдеться про послідовний ланцюг дій, що охоплює первинний доступ, подальше переміщення в мережі, компрометацію облікових даних і вплив на кінцеві точки. Саме така зв'язаність етапів формує цілісний сценарій реалізації загрози. ENISA у Threat Landscape 2024 відзначає ескалацію кібератак на тлі геополітичних чинників [4]. IBM у X-Force Threat Intelligence Index 2026 також вказує на зростання кількості атак, початковим етапом яких була експлуатація відкритих сервісів [5]. За таких обставин ізольований аналіз окремих інцидентів уже не має достатньої практичної цінності.

Базовими інструментами моніторингу в такій ситуації залишаються SIEM-системи. Вони агрегують події, виконують кореляцію та забезпечують аналітичне опрацювання даних у реальному часі. Проте навіть значний обсяг подій сам по собі не гарантує коректної оцінки стану захищеності, оскільки вирішальне значення має спосіб інтерпретації отриманих даних. Попередні дослідження показали доцільність розгляду індикаторів за трьома напрямками: соціальна інженерія, мережевий рівень і кінцеві точки [6]. Такий поділ упорядковує інформацію, але ще не розв'язує завдання оцінювання. Проблема полягає в тому, що індикатори відрізняються за масштабом, частотою появи та діагностичною значущістю. Їх поєднання змінюється залежно від конкретної системи та моменту часу, а наперед визначити таку комбінацію практично неможливо. Саме тому наступним кроком стає формалізація, тобто перехід від описових характеристик до системи показників і критеріїв, придатних для багатофакторного оцінювання.

Причина полягає в тому, що індикатори мають різну природу, різний масштаб значень, різну частоту появи та неоднакову діагностичну вагу в загальній оцінці стану захищеності. Для кожної конкретної ІТС у кожний момент часу перелік індикаторів і загроз може мати складну апріорно непередбачувану комбінаторику взаємодії, а тому суть дослідження полягає у формалізації системи індикаторів загроз до рівня показників та критеріїв із подальшим застосуванням методів багатофакторного оцінювання. Власне, наступним логічним кроком після класифікації індикаторів є їх формалізація у вигляді системи кількісних показників, придатних для подальшого інтегрального оцінювання [7].

Методологічною основою такого підходу є праці О.О. Писарчука, у яких багатокритеріальне оцінювання розглядається як засіб отримання інтегрованої оцінки за сукупністю часткових критеріїв,

а також як основа ситуаційного управління структурою та параметрами системи забезпечення інформаційної безпеки.

Метою статті є розроблення математичної моделі інтегрального оцінювання рівня загроз інформаційній безпеці в ІТС на основі індикаторів, сформованих на підставі даних SIEM-систем. Для досягнення поставленої мети у роботі здійснено формалізацію системи індикаторів загроз, яку поділено на подієві індикатори та індикатори стану компонентів ІТС, побудовано інтегральну модель оцінювання у вигляді зваженої лінійної згортки нормованих показників, а також визначено вагові коефіцієнти індикаторів методом аналізу ієрархій із перевіркою узгодженості експертних оцінок. Запропонований підхід охоплює етапи відбору та класифікації подій безпеки, формування системи індикаторів, їх нормування та подальше використання для багатофакторного оцінювання рівня загроз інформаційній безпеці в ІТС.

Виконання досліджень

У попередніх дослідженнях індикатори загроз інформаційній безпеці класифіковано за трьома рівнями: соціальної інженерії, мережевого та рівня кінцевої точки. Однак для їх застосування у задачах багатофакторного оцінювання потрібна подальша формалізація. Вона полягає в подачі індикаторів як системи показників, що визначаються на основі подій SIEM-систем і використовуються для кількісного аналізу загроз ІБ.

1. Формалізація системи індикаторів загроз інформаційній безпеці

Індикатори, сформовані за даними SIEM-систем, відображають різні аспекти функціонування ІТС і відрізняються за походженням. Частина характеризує поведінку користувачів, інша – параметри мережевої взаємодії, ще одна група – стан програмного забезпечення та події на кінцевих пристроях. Для подальшого застосування у багатофакторному оцінюванні стану захищеності ІТС їх подають у формалізованому вигляді. Введемо множину індикаторів загроз інформаційній безпеці, узгоджену з підходами багатокритеріального оцінювання [9].

$$I = \{F_{soc}, F_{ip}, F_{url}, F_{ex}, F_b, F_s, F_{lic}, F_{mal}, F_{adm}, F_{mf}\},$$

де F_{soc} – індикатори атак соціальної інженерії; F_{ip} – індикатори комунікації з IP-адресами з негативною репутацією; F_{url} – індикатори комунікації з підозрілими або шкідливими URL-адресами; F_{ex} – індикатори наявності вразливостей мережевих служб, баз даних або застосунків, що можуть бути потенційно експлуатовані; F_b – індикатори брутфорс-атак; F_s – індикатори актуальності версій програмного забезпечення; F_{lic} – індикатори використання неліцензійного програмного забезпечення; F_{mal} – індикатори стану модулів антивірусного захисту; F_{adm} – індикатори використання адміністративних привілеїв; F_{mf} – індикатори виявлення шкідливих файлів.

У такому поданні сукупність індикаторів задається у вигляді вектора-стовпця:

$$D = [F_{soc}, F_{ip}, F_{url}, F_{ex}, F_b, F_s, F_{lic}, F_{mal}, F_{adm}, F_{mf}]^T,$$

де T – операція транспонування вектора.

Загалом індикатори загроз інформаційній безпеці можуть формуватися на основі двох типів даних: подій безпеки та параметрів стану ІТС. У зв'язку з цим множину індикаторів доцільно поділити на дві групи: подієві індикатори та індикатори стану системи.

Формально множина індикаторів визначається як об'єднання двох підмножин:

$$I = I^{event} \cup I^{state},$$

де I^{event} – індикатори, що формуються на основі подій SIEM-системи; I^{state} – індикатори, що відображають стан компонентів ІТС.

До підмножини I^{event} належать: $F_{soc}, F_{ip}, F_{url}, F_b, F_{adm}, F_{mf}$. До підмножини I^{state} належать: $F_s, F_{lic}, F_{mal}, F_{ex}$. Значення подієвих індикаторів визначається як агрегована оцінка подій відповідного типу в межах інтервалу спостереження з урахуванням їхніх вагових коефіцієнтів.

Загалом, індикатори загроз інформаційній безпеці формуються на основі двох типів даних: подій безпеки та параметрів стану ІТС. Відповідно, множину індикаторів поділяють на дві групи: подієві індикатори та індикатори стану системи. Формально множину індикаторів задають як об'єднання двох підмножин:

$$F_i^{event} = \frac{\sum_{j=1}^{N_i(t)} w_{ij}}{N_i^{max}(t) \cdot w_i^{max}},$$

де $N_i(t)$ – кількість подій типу i зафіксованих SIEM-системою протягом інтервалу часу Δt ; w_{ij} – ваговий коефіцієнт j -події, що відображає її критичність, визначається з урахуванням рівня severity [8, 9], репутаційних характеристик джерела, результату виконання дії та потенційного впливу на ІТС. $N_i^{max}(t)$ – максимально допустима або нормативно визначена кількість подій типу i в межах інтервалу спостереження Δt ; w_i^{max} – максимальне можливе значення вагового коефіцієнта для подій типу i . За такого визначення виконується умова $0 \leq F_i^{event} \leq 1$, що забезпечує уніфікованість шкали подієвих

індикаторів і усуває потребу в їх додатковому нормуванні. У результаті значення подієвих індикаторів стають порівнюваними та можуть безпосередньо використовуватися в процедурах багатофакторного оцінювання стану захищеності ІТС. Вагові коефіцієнти визначають із застосуванням методів багато-критеріального аналізу, зокрема, аналітичного ієрархічного процесу [10].

Для індикаторів стану системи значення задають як частку компонентів, що мають відповідну ознаку ризику:

$$F_i^{state} = \frac{N_{risk}}{N_{total}},$$

де N_{risk} – кількість компонентів системи, що мають відповідні ознаки ризику (вразливості, порушення політик безпеки тощо); N_{total} – загальна кількість компонентів системи.

Оскільки значення індикаторів стану також належать інтервалу $[0;1]$, вони, як і подієві індикатори, безпосередньо використовуються як вхідні параметри інтегральної моделі оцінювання без додаткового нормування. У базовій моделі всі компоненти системи розглядаються як рівнозначні. У подальших дослідженнях оцінку уточнюють шляхом введення вагових коефіцієнтів для різних класів активів ІТС. Отримані значення індикаторів можуть відрізнятися за масштабом. У запропонованій моделі подієві індикатори визначаються одразу у нормованій формі, тоді як індикатори стану за своєю природою є відносними величинами.

Отже, усі компоненти вектора загроз належать до єдиного інтервалу $[0;1]$, що забезпечує їх коректне використання в інтегральній моделі оцінювання.

II. Формування показників індикаторів за даними SIEM

Після формалізації системи індикаторів загроз інформаційній безпеці постає завдання визначення механізмів їх практичного формування на основі подій, що реєструються засобами моніторингу безпеки. У сучасних ІТС основним інструментом централізованого збору, кореляції та аналізу подій безпеки є SIEM-системи, які забезпечують інтеграцію журналів подій із різномірних джерел інфраструктури. У результаті кореляції та аналітичної обробки формується інформаційна база, що слугує основою для обчислення значень індикаторів загроз інформаційній безпеці.

У рамках запропонованого підходу значення індикаторів формують шляхом агрегування подій відповідного типу у визначеному часовому інтервалі спостереження Δt . Кожна подія характеризується набором атрибутів, зокрема рівнем критичності, джерелом виникнення, результатом виконання дії та потенційним впливом на ІТС. Ці характеристики використовують для визначення вагових коефіцієнтів подій і подальшого обчислення значень подієвих індикаторів.

Отже, події, що фіксуються SIEM-системою, становлять первинну інформаційну основу для формування системи показників-індикаторів загроз інформаційній безпеці, які надалі застосовуються у процедурах багатофакторного оцінювання стану захищеності ІТС.

Джерела подій для формування індикаторів загроз

Формування показників індикаторів загроз інформаційній безпеці базується на подіях, що фіксуються та обробляються SIEM-системами під час моніторингу ІТС. У сучасних умовах такі системи забезпечують централізований збір, нормалізацію, кореляцію та аналітичну обробку подій безпеки, що надходять із різномірних джерел інфраструктури. До таких джерел належать мережеві засоби захисту, зокрема міжмережеві екрани, системи виявлення та запобігання вторгненням і веб-застосункові екрани, системи автентифікації та управління доступом, засоби захисту кінцевих пристроїв, включаючи антивірусні та EDR-рішення, а також системи управління вразливостями й журнали подій операційних систем і прикладного програмного забезпечення. Кожне джерело відображає окремі аспекти функціонування ІТС і фіксує події, пов'язані як із мережевою активністю, так і з поведінкою користувачів та станом програмно-апаратних компонентів.

Під час роботи SIEM-системи ці події проходять етапи уніфікації та кореляції, що дають змогу отримати узгоджене представлення подій безпеки незалежно від їхнього первинного джерела. Узагальнена сукупність подій слугує основою для формування показників індикаторів загроз інформаційній безпеці. Індикатори загроз у запропонованій моделі не є абстрактними величинами: їх визначають як функції від подій, що фіксуються SIEM-системою, і вони відображають результати агрегації та аналітичної обробки в межах ІТС.

Формування подієвих індикаторів загроз

Подієві індикатори загроз інформаційній безпеці формуються шляхом агрегування подій, що реєструються SIEM-системою під час моніторингу. Значення таких індикаторів визначають у межах заданого інтервалу спостереження шляхом узагальнення подій відповідного типу з урахуванням їх вагових коефіцієнтів, які відображають критичність подій та їхній потенційний вплив на стан захищеності системи. Запропонований підхід передбачає встановлення відповідності між типами подій безпеки, що фіксуються SIEM-системою, та відповідними індикаторами загроз.

У загальному випадку формування подієвих індикаторів ґрунтується на множині подій безпеки, що реєструються SIEM-системою: $E = \{e_1, e_2, \dots, e_n\}$, де E – множина подій безпеки. Для кожного подієвого індикатора F_i^{event} визначають відповідну підмножину подій $E_i \subseteq E$, що відповідає певному типу загроз інформаційній безпеці.

Кожному подієвому індикатору відповідає підмножина подій безпеки, яка характеризує прояви відповідного типу загроз. Так, для індикатора F_{soc} використовують події, пов'язані з виявленням фішингових повідомлень, підозрілої електронної кореспонденції або спроб введення користувачів в оману. Індикатори F_{ip} та F_{url} формуються на основі подій встановлення з'єднань із ресурсами, що мають негативну репутацію або належать до переліків загроз, сформованих на основі threat intelligence. Для індикатора F_b використовують події, що відображають послідовності невдалих спроб автентифікації, які можуть свідчити про спроби підбору облікових даних. Індикатор F_{adm} формується на основі подій використання адміністративних привілеїв, зокрема підвищення рівня доступу або виконання адміністративних операцій. Для індикатора F_{mf} використовуються події виявлення шкідливого програмного забезпечення, зафіксовані антивірусними засобами або EDR.

Кожен подієвий індикатор формується як агрегована кількісна оцінка подій безпеки, що належать до певного типу загроз, відповідно до формалізованого підходу, наведеного у попередньому розділі. Це дозволяє перейти від окремих подій до узагальнених показників, які відображають інтенсивність прояву загроз інформаційній безпеці у визначеному часовому інтервалі.

Формування індикаторів стану ІТС

На відміну від подієвих індикаторів, індикатори стану відображають поточний стан компонентів інформаційно-телекомунікаційної системи і не базуються безпосередньо на потоці подій SIEM-системи. Їх формують на основі даних про конфігурацію, склад і властивості компонентів ІТС, отриманих із систем управління активами, засобів контролю вразливостей, рішень на рівні кінцевої точки та інших джерел інформації про технічний стан системи. Індикатори стану характеризують наявність ознак ризику у компонентах ІТС, зокрема, використання застарілих версій програмного забезпечення, наявність відомих вразливостей, використання неліцензійного програмного забезпечення або некоректний стан засобів захисту. Для кожного індикатора стану F_i^{state} оцінка визначається як відношення кількості компонентів системи, що мають відповідну ознаку ризику, до загальної кількості розглянутих компонентів:

$$F_i^{state} = \frac{N_{risk}}{N_{total}},$$

де N_{risk} – кількість компонентів ІТС, для яких зафіксовано відповідну ознаку ризику; N_{total} – загальна кількість компонентів, що входять до розглядуваної множини.

Значення індикатора стану інтерпретують як частку компонентів системи, що перебувають у потенційно небезпечному або некоректному стані. У базовому варіанті всі компоненти вважаються рівнозначними, однак у подальшому модель можна уточнити, вводячи вагові коефіцієнти для різних класів активів з урахуванням їхньої критичності для функціонування ІТС.

Для узагальнення запропонованої системи індикаторів наведено їх характеристики за типом, джерелами даних і принципом формування (табл. 1).

Таблиця 1
Характеристика індикаторів загроз інформаційній безпеці

Індикатор	Тип	Джерело даних	Принцип формування
F_{soc}	подієвий	secure email gateway, SIEM	події фішингу та suspicious email, агреговані за Δt з урахуванням вагових коефіцієнтів
F_{ip}	подієвий	SIEM, threat intelligence	події звернень до IP-адрес з негативною репутацією, агреговані за Δt з урахуванням вагових коефіцієнтів
F_{url}	подієвий	SIEM, web gateway	події доступу до підозрілих/шкідливих URL, агреговані за Δt з урахуванням вагових коефіцієнтів
F_b	подієвий	IAM, AD, SIEM	послідовності невдалих спроб автентифікації, агреговані за Δt з урахуванням вагових коефіцієнтів
F_{adm}	подієвий	SIEM, audit logs	події використання або ескалації адміністративних привілеїв, агреговані за Δt з урахуванням вагових коефіцієнтів
F_{mf}	подієвий	EDR, антивірусні системи	події виявлення шкідливого ПЗ, агреговані за Δt з урахуванням вагових коефіцієнтів
F_s	стану	asset management, CMDB	частка компонентів із застарілими версіями ПЗ
F_{lic}	стану	asset management	частка компонентів із неліцензійним ПЗ
F_{mal}	стану	endpoint security tools	частка систем із некоректним станом захисту
F_{ex}	стану	vulnerability scanners	частка компонентів із вразливостями

Для ілюстрації застосування запропонованого підходу розглянемо умовний приклад. У межах інтервалу спостереження Δt SIEM-системою зафіксовано 12 подій невдалих спроб автентифікації, 3 звернення до IP-адрес із негативною репутацією та 2 події виявлення шкідливого програмного забезпечення. Тоді відповідні подієві індикатори F_b^{event} , F_{ip}^{event} та F_{mf}^{event} визначаються як агреговані значення цих подій з урахуванням їхніх вагових коефіцієнтів. Одночасно, за даними про стан системи, встановлено, що з 100 компонентів ІТС 18 мають відомі вразливості, а 7 – використовують застарілі версії програмного забезпечення. Відповідно, значення індикаторів стану становлять $F_{ex}^{state} = 0,18$ та $F_s^{state} = 0,07$. Наприклад, якщо для індикатора брутфорс-атак у межах інтервалу Δt зафіксовано $N_b(\Delta t) = 12$ подій, вагові коефіцієнти яких позначено через w_{bj} , а нормативно визначене максимальне значення для цього інтервалу становить $N_b^{max}(\Delta t) = 20$ при $w_b^{max} = 1$, то значення подієвого індикатора визначається як:

$$F_b^{event} = \frac{\sum_{j=1}^{12} w_{bj}}{20 \cdot 1}.$$

Подієвий індикатор одразу набуває нормованого значення в інтервалі $[0;1]$, що забезпечує його подальше безпосереднє використання в інтегральному оцінюванні.

У межах запропонованого підходу індикатори загроз інформаційній безпеці формуються на основі двох типів даних: подій безпеки, що агрегуються SIEM-системою, та параметрів стану компонентів ІТС. Подієві індикатори відображають інтенсивність прояву загроз у часі, тоді як індикатори стану характеризують структурний рівень вразливості системи. Значення індикаторів, приведені до уніфікованої шкали, використовують як вхідні параметри для подальшого інтегрального оцінювання рівня захищеності ІТС.

Математична модель інтегрального оцінювання

Формалізація індикаторів загроз інформаційній безпеці у вигляді системи часткових показників є лише проміжним етапом дослідження. Для практичного застосування в задачах моніторингу та підтримки прийняття рішень за даними SIEM-систем необхідно перейти від множини окремих індикаторів до інтегральної оцінки, що узагальнює їхній сукупний вплив на стан захищеності інформаційно-телекомунікаційної системи.

Нехай стан інформаційної безпеки ІТС на інтервалі спостереження Δt° описується вектором нормованих індикаторів загроз:

$$D = [F_{soc}, F_{ip}, F_{url}, F_{ex}, F_b, F_s, F_{lic}, F_{mal}, F_{adm}, F_{mf}]^T,$$

де кожен індикатор $F_i \in [0;1]$ є нормованим або відносним показником відповідного типу загрози чи ознаки ризику. Інтегральна оцінка рівня загроз інформаційній безпеці визначається у вигляді зваженої згортки нормованих індикаторів:

$$S(D) = \sum_{i=1}^{10} w_i F_i, \quad w_i \geq 0, \quad \sum_{i=1}^{10} w_i = 1.$$

де w_i – вагові коефіцієнти, що відображають відносну значущість відповідних індикаторів у загальній структурі оцінювання.

Таким чином, задача оцінювання стану інформаційної безпеки ІТС зводиться до обчислення інтегрального показника на основі багатовимірного вектора індикаторів загроз. Запропонована модель забезпечує монотонність оцінювання: збільшення будь-якого індикатора за незмінності інших не призводить до зменшення інтегрального показника. Оскільки всі нормовані індикатори належать інтервалу $[0;1]$, а сума вагових коефіцієнтів дорівнює одиниці, значення інтегральної оцінки також належить інтервалу $[0;1]$, що забезпечує зручність її інтерпретації.

Для практичного використання інтегральної оцінки доцільно ввести шкалу рівнів загроз інформаційній безпеці, що забезпечує інтерпретацію отриманих результатів і підтримує ухвалення управлінських рішень. Зокрема, інтегральний показник S може бути інтерпретований за такою градацією:

$$S \in [0; 0,33] \quad - \quad \text{низький рівень загроз},$$

$$S \in (0,33; 0,66] \quad - \quad \text{середній рівень загроз},$$

$$S \in (0,66; 1] \quad - \quad \text{високий рівень загроз}.$$

Запропонована шкала дозволяє здійснювати узагальнену оцінку стану захищеності інформаційно-телекомунікаційної системи та ранжувати її за ступенем критичності. Граничні значення інтервалів можуть уточнюватися на основі емпіричних даних, статистичного аналізу або експертних оцінок з урахуванням специфіки предметної області та умов функціонування ІТС.

Визначення вагових коефіцієнтів індикаторів

Визначення вагових коефіцієнтів індикаторів є важливим етапом побудови інтегральної моделі оцінювання, оскільки вони відображають відносну значущість індикаторів у загальній структурі оці-

нювання стану інформаційної безпеки. Значення ваг w_i визначають ступінь впливу відповідних індикаторів на інтегральний показник $S(D)$, а отже, безпосередньо впливають на результати оцінювання.

Для визначення вагових коефіцієнтів застосовують метод аналізу ієрархій (Analytic Hierarchy Process, AHP), який належить до поширених підходів у задачах багатокритеріального прийняття рішень. Метод дає змогу формалізувати експертні оцінки відносної важливості індикаторів шляхом побудови матриці попарних порівнянь.

Нехай задано множину індикаторів $I = \{F_1, F_2, \dots, F_{10}\}$. У межах методу АНР формується матриця попарних порівнянь $A = [a_{ij}]$, де елемент a_{ij} відображає відносну важливість індикатора F_i порівняно з індикатором F_j . Значення елементів матриці визначаються за шкалою Сааті, де $a_{ij} > 1$ означає перевагу індикатора F_i , $a_{ij} < 1$ – перевагу F_j , а $a_{ij} = 1$ – їхню рівну важливість.

Матриця попарних порівнянь має властивість оберненої симетрії:

$$a_{ij} = \frac{1}{a_{ji}}, \quad a_{ii} = 1.$$

На основі матриці A визначається вектор вагових коефіцієнтів:

$$w = [w_1, w_2, \dots, w_{10}]^T,$$

який визначається як нормалізований власний вектор матриці A , що відповідає її максимальному власному значенню.

Отримані вагові коефіцієнти нормуються таким чином, щоб виконувалась умова:

$$\sum_{i=1}^{10} w_i = 1.$$

Для забезпечення коректності експертних оцінок у методі АНР додатково перевіряють узгодженість матриці попарних порівнянь. У разі перевищення допустимого рівня неузгодженості матрицю коригують.

Розрахунок вагових коефіцієнтів індикаторів на основі методу аналізу ієрархій

У межах застосування методу аналізу ієрархій визначають вагові коефіцієнти індикаторів загроз інформаційній безпеці на основі експертного порівняння їхньої відносної важливості. Інтегральна модель оцінювання безпосередньо використовує множину індикаторів. Визначення вагових коефіцієнтів доцільно здійснювати безпосередньо для цієї множини без введення додаткових ієрархічних рівнів агрегації.

Для цього формується матриця попарних порівнянь індикаторів $A = [a_{ij}]$, де елемент a_{ij} відображає відносну важливість індикатора F_i порівняно з індикатором F_j . Значення елементів матриці задаються відповідно до шкали Сааті. На основі отриманої матриці обчислюється вектор вагових коефіцієнтів:

$$w = [w_1, w_2, \dots, w_{10}]^T,$$

який відповідає нормалізованому власному вектору матриці попарних порівнянь, що відповідає її максимальному власному значенню та використовується в інтегральній моделі оцінювання.

Експертне порівняння індикаторів у матриці попарних порівнянь виконують з урахуванням їх практичної значущості для виявлення та оцінювання рівня загроз інформаційній безпеці. Більшу вагу надають індикаторам, що безпосередньо відображають поточні ознаки реалізації атаки, компрометації або активної шкідливої діяльності в ІТС. До них належать, зокрема, індикатори виявлення шкідливих файлів, використання або ескалації адміністративних привілеїв, звернень до ресурсів із негативною репутацією, фішингової активності та спроб несанкціонованої автентифікації.

Індикатори стану системи, які характеризують наявність вразливостей, застарілого програмного забезпечення, некоректного стану засобів захисту або використання неліцензійного програмного забезпечення, відображають фоновий рівень вразливості ІТС. Вони мають суттєве значення для оцінювання ризику, однак не завжди свідчать про безпосередню реалізацію загрози. Такий підхід узгоджується з сучасними практиками кіберзахисту: індикатори компрометації та потенційно несприятливі події підлягають пріоритетному виявленню й аналізу, тоді як незакриті вразливості розглядають як об'єкти підвищеної уваги, але не як пряме свідчення реалізації загрози.

Для забезпечення однозначності подальших розрахунків порядок індикаторів у матриці попарних порівнянь приймають таким самим, як і у векторі інтегральної моделі. Матрицю попарних порівнянь індикаторів загроз інформаційній безпеці наведено в таблиці 2.

Таблиця 2
Матриця попарних порівнянь індикаторів загроз

	F_{soc}	F_{ip}	F_{url}	F_{ex}	F_h	F_s	F_{lic}	F_{mal}	F_{adm}	F_{mf}
F_{soc}	1	1	1	2	1	2	5	2	1/2	1/2
F_{ip}	1	1	1	2	1	2	4	2	1/2	1/2
F_{url}	1	1	1	2	1	2	5	2	1/2	1/2
F_{ex}	1/2	1/2	1/2	1	1/2	1	2	1/2	1/3	1/3
F_h	1	1	1	2	1	2	4	2	1/2	1/2
F_s	1/2	1/2	1/2	1	1/2	1	2	1/2	1/3	1/3
F_{lic}	1/5	1/4	1/5	1/2	1/4	1/2	1	1/3	1/7	1/7
F_{mal}	1/2	1/2	1/2	2	1/2	2	3	1	1/2	1/2
F_{adm}	2	2	2	3	2	3	7	2	1	1
F_{mf}	2	2	2	3	2	3	7	2	1	1

На основі матриці попарних порівнянь обчислюється власний вектор, що відповідає максимальному власному значенню матриці A . Після нормування цього вектора отримуються вагові коефіцієнти індикаторів, сума яких дорівнює одиниці:

$$\sum_{i=1}^{10} w_i = 1.$$

Вагові коефіцієнти індикаторів визначаються як компоненти нормалізованого власного вектора матриці попарних порівнянь A , що відповідає її максимальному власному значенню λ_{max} . Після нормування отриманого вектора формуються значення w_i , які використовуються в інтегральній моделі оцінювання. На основі матриці попарних порівнянь $A = [a_{ij}]$ визначається власний вектор w , що відповідає максимальному власному значенню λ_{max} матриці A :

$$Aw = \lambda_{max} w.$$

Після нормування власного вектора отримуються вагові коефіцієнти індикаторів:

$$w_i^{norm} = \frac{w_i}{\sum_{i=1}^n w_i}, \quad \sum_{i=1}^n w_i^{norm} = 1.$$

Для оцінювання узгодженості експертних порівнянь обчислюється індекс узгодженості CI :

$$CI = \frac{\lambda_{max} - n}{n - 1},$$

де n – розмірність матриці попарних порівнянь. Далі визначається відношення узгодженості CR :

$$CR = \frac{CI}{RI},$$

де RI – випадковий індекс узгодженості, що визначається відповідно до табличних значень методу аналізу ієрархій та залежить від розмірності матриці попарних порівнянь [12]. Для матриці розмірності $n = 10$ використовується значення $RI = 1,49$. Якщо $CR < 0,1$, рівень узгодженості матриці попарних порівнянь вважається достатнім.

Для побудованої матриці попарних порівнянь отримано $\lambda_{max} = 10,112$, індекс узгодженості $CI = 0,012$ та відношення узгодженості $CR = 0,008$. Оскільки $CR < 0,1$, матриця попарних порівнянь характеризується достатнім рівнем узгодженості експертних оцінок. Вагові коефіцієнти, наведені в таблиці 3, є компонентами нормалізованого власного вектора матриці попарних порівнянь.

Таблиця 3
Вагові коефіцієнти індикаторів загроз

Індикатор	Ваговий коефіцієнт
F_{soc}	0,1082
F_{ip}	0,1058
F_{url}	0,1082
F_{ex}	0,0522
F_h	0,1058
F_s	0,0522
F_{lic}	0,0248
F_{mal}	0,0748
F_{adm}	0,1840
F_{mf}	0,1840

З отриманих результатів видно, що найбільші вагові коефіцієнти мають індикатори F_{adm} та F_{mf} , які відповідають використанню адміністративних привілеїв і виявленню шкідливих файлів. Це узгоджується з тим, що зазначені індикатори найбільшою мірою відображають безпосередні ознаки реалізації загроз або компрометації ІТС. Водночас індикатори F_{ex} , F_s та F_{lic} , які характеризують стан системи та наявність структурних передумов ризику, мають меншу вагу, оскільки вони не завжди свідчать про фактичну реалізацію атаки, але враховуються як важливі фонові фактори ризику.

Розрахунок інтегрального показника рівня загроз ІБ

Після визначення вагових коефіцієнтів індикаторів загроз інформаційній безпеці, запропонована інтегральна модель оцінювання набуває практичного застосування. Значення індикаторів F_i , що характеризують стан ІТС на заданому інтервалі спостереження, підставляються в інтегральну функцію оцінювання.

У результаті обчислюється узагальнений показник $S(D)$, що відображає сукупний рівень загроз інформаційній безпеці та інтерпретується відповідно до введеної шкали ризику. Для ілюстрації практичного застосування моделі розглянемо умовний приклад розрахунку інтегрального показника на основі значень нормованих індикаторів загроз. Нехай у межах інтервалу спостереження для ІТС отримано такі нормовані значення індикаторів:

$$\begin{aligned} F_{soc} &= 0,40, & F_{ip} &= 0,35, & F_{url} &= 0,30, \\ F_{ex} &= 0,45, & F_b &= 0,50, & F_s &= 0,25, \\ F_{lic} &= 0,10, & F_{mal} &= 0,30, & F_{adm} &= 0,20, & F_{mf} &= 0,15. \end{aligned}$$

Наведені значення відповідають ситуації, за якої в ІТС спостерігаються ознаки підозрілої мережевої та облікової активності, а також наявні окремі структурні передумови ризику, пов'язані зі станом програмного забезпечення та засобів захисту. Тоді інтегральний показник рівня загроз ІБ визначається шляхом підстановки наведених значень індикаторів та відповідних вагових коефіцієнтів у формулу:

$$\begin{aligned} S(D) &= 0,1082F_{soc} + 0,1058F_{ip} + 0,1082F_{url} + 0,0522F_{ex} + 0,1058F_b \\ &+ 0,0522F_s + 0,0248F_{lic} + 0,0748F_{mal} + 0,1840F_{adm} + 0,1840F_{mf}. \end{aligned}$$

Після підстановки числових значень отримуємо:

$$\begin{aligned} S(D) &= 0,1082 \cdot 0,40 + 0,1058 \cdot 0,35 + 0,1082 \cdot 0,30 + 0,0522 \cdot 0,45 + 0,1058 \cdot 0,50 + \\ &+ 0,0522 \cdot 0,25 + 0,0248 \cdot 0,10 + 0,0748 \cdot 0,30 + 0,1840 \cdot 0,20 + 0,1840 \cdot 0,15 \end{aligned}$$

У результаті обчислення одержуємо: $S(D) \approx 0,292$

Отже, для наведеного прикладу інтегральний показник рівня загроз інформаційній безпеці становить 0,292°. Відповідно до прийнятої шкали інтерпретації, це значення належить інтервалу низького рівня загроз і наближається до верхньої межі цього інтервалу. Такий результат свідчить про наявність помірних ознак небезпечної активності та окремих структурних передумов ризику, проте не вказує на критичний стан захищеності інформаційно-телекомунікаційної системи.

Наведений приклад демонструє практичну придатність запропонованої моделі для узагальнення різномірних індикаторів у єдиний інтегральний показник. Внесок кожного індикатора у кінцевий результат визначається не лише його поточним значенням, а й відповідним ваговим коефіцієнтом, що дозволяє врахувати відносну значущість різних проявів загроз у загальній структурі оцінювання.

Для додаткової перевірки поведінки моделі розглянемо ще два умовні сценарії, що відповідають середнім та високим рівням загроз інформаційній безпеці. Це дає змогу простежити зміну інтегрального показника зі зростанням значень нормованих індикаторів.

Для сценарію середнього рівня приймемо такі значення нормованих індикаторів:

$$\begin{aligned} F_{soc} &= 0,60, & F_{ip} &= 0,55, & F_{url} &= 0,50, \\ F_{ex} &= 0,65, & F_b &= 0,70, & F_s &= 0,45, \\ F_{lic} &= 0,20, & F_{mal} &= 0,55, & F_{adm} &= 0,40, & F_{mf} &= 0,35. \end{aligned}$$

Тоді:

$$\begin{aligned} S(D) &= 0,1082 \cdot 0,60 + 0,1058 \cdot 0,55 + 0,1082 \cdot 0,50 + 0,0522 \cdot 0,65 + 0,1058 \cdot 0,70 + \\ &+ 0,0522 \cdot 0,45 + 0,0248 \cdot 0,20 + 0,0748 \cdot 0,55 + 0,1840 \cdot 0,40 + 0,1840 \cdot 0,35 \end{aligned}$$

У результаті обчислення одержуємо: $S(D) \approx 0,489$. Отримане значення належить інтервалу середнього рівня загроз. Це відповідає ситуації, за якої в ІТС наявні виражені ознаки небезпечної активності, проте вони ще не свідчать про критичний стан системи.

Для сценарію високого рівня приймемо такі значення нормованих індикаторів:

$$F_{soc} = 0,85, \quad F_{ip} = 0,80, \quad F_{url} = 0,75,$$

$$F_{ex} = 0,90, \quad F_b = 0,95, \quad F_s = 0,70,$$

$$F_{lic} = 0,40, \quad F_{mal} = 0,80, \quad F_{adm} = 0,70, \quad F_{mf} = 0,65.$$

Тоді:

$$S(D) = 0,1082 \cdot 0,85 + 0,1058 \cdot 0,80 + 0,1082 \cdot 0,75 + 0,0522 \cdot 0,90 + 0,1058 \cdot 0,95 + \\ + 0,0522 \cdot 0,70 + 0,0248 \cdot 0,40 + 0,0748 \cdot 0,80 + 0,1840 \cdot 0,70 + 0,1840 \cdot 0,65$$

У результаті обчислення одержуємо: $S(D) \approx 0,760$. Отримане значення належить інтервалу високого рівня загроз. Такий результат відповідає ситуації, коли в ІТС одночасно спостерігаються інтенсивні прояви атакуючої активності, ознаки зловживання привілеями, шкідлива активність і суттєві структурні передумови ризику.

Таким чином, результати сценарних розрахунків свідчать, що запропонована інтегральна модель є чутливою до змін у вхідних параметрах і адекватно відображає зростання рівня загроз інформаційній безпеці. Зі збільшенням значень нормованих індикаторів і, передусім, найбільш вагомих із них, інтегральний показник $S(D)$ закономірно переходить від низького до середнього та високого рівнів загроз.

Висновки

У статті розв'язано задачу формалізації індикаторів загроз інформаційній безпеці в інформаційно-телекомунікаційних системах на основі даних SIEM-систем. Запропоновано підхід до формування системи індикаторів, який передбачає їх поділ на події та індикатори стану з приведенням до уніфікованої шкали значень. Події індикатори визначаються як нормовані агреговані оцінки подій з урахуванням їхніх вагових коефіцієнтів, тоді як індикатори стану формуються як відносні показники, що характеризують частку компонентів ІТС із відповідними ознаками ризику. На основі сформованої системи індикаторів побудовано математичну модель інтегрального оцінювання рівня загроз ІБ у вигляді зваженої лінійної згортки. Вагові коефіцієнти індикаторів визначено методом аналізу ієрархій із перевіркою узгодженості експертних оцінок. Розрахунки для типових сценаріїв підтвердили адекватність моделі та її чутливість до змін у значеннях індикаторів. Подальші дослідження передбачають апробацію запропонованої моделі на реальних даних SIEM-систем, а також уточнення складу індикаторів і процедур визначення їхніх вагових коефіцієнтів.

Література

1. Verizon. 2025 Data Breach Investigations Report. URL: <https://www.verizon.com/business/resources/reports/dbir/>
2. Microsoft. Digital Defense Report 2025. URL: <https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report>
3. CrowdStrike. Global Threat Report 2026. URL: <https://www.crowdstrike.com/global-threat-report/>
4. ENISA. Threat Landscape 2024. URL: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024>
5. IBM. X-Force Threat Intelligence Index 2026. URL: <https://www.ibm.com/reports/threat-intelligence6>. Писарчук, О. О., & Кошара, А. В. (2024). Аналіз індикаторів загроз інформаційній безпеці в інформаційно-телекомунікаційних системах за результатами застосування SIEM-систем. Інфокомунікаційні та комп'ютерні технології, 1(07), с. 79–84. <https://doi.org/10.36994/2788-5518-2024-01-07-11>
7. Писарчук О.О., Соколов К.О., Гудима О.П. Розроблення багатокритеріальної методики ситуаційного управління структурою і параметрами системи забезпечення інформаційної безпеки. Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. 2016. № 3. С. 24–32.
8. NIST. Guide for Conducting Risk Assessments (SP 800-30 Rev.1). URL: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>
9. FIRST. Common Vulnerability Scoring System v3.1: Specification Document. URL: <https://www.first.org/cvss/v3.1/specification-document>
10. Saaty T.L. Decision Making with the Analytic Hierarchy Process. *International Journal of Services Sciences*, 2008, Vol. 1, No. 1, pp. 83–98. <https://doi.org/10.1504/IJSSCI.2008.017590>
11. Hwang C.L., Yoon K. Multiple Attribute Decision Making: Methods and Applications. Springer, 1981.
12. Saaty T. L. The Analytic Hierarchy Process: What It Is and How It Is Used // *Mathematical Modelling*. – 1987. – Vol. 9. – P. 161–176.

References

1. Verizon. 2025 Data Breach Investigations Report. URL: <https://www.verizon.com/business/resources/reports/dbir/>
2. Microsoft. Digital Defense Report 2025. URL: <https://www.microsoft.com/en-us/corporate-responsibility/cybersecurity/microsoft-digital-defense-report-2025/>
3. CrowdStrike. Global Threat Report 2025. URL: <https://www.crowdstrike.com/global-threat-report/>
4. ENISA. Threat Landscape 2024. URL: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024>
5. IBM. X-Force Threat Intelligence Index 2026. URL: <https://www.ibm.com/reports/threat-intelligence>
6. Pysarchuk O.O., & Koshara A.V. (2024). Analysis of indicators of information security threats in information and telecommunication systems according to the results of the application of SIEM systems. Infocommunication and computer technologies, 1(07), 79–84. <https://doi.org/10.36994/2788-5518-2024-01-07-11>
7. Pysarchuk O.O., Sokolov K.O., Gudyma O.P. Development methods multi situational management structure and parameters of information security system / O.O. Pysarchuk, Collection of scientific works of the Center for Military and Strategic Research of the National University of Defense of Ukraine Ivan Chernyakhovskyi. - 2016. No. 3. P. 24–32.
8. NIST. Guide for Conducting Risk Assessments (SP 800-30 Rev.1). URL: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>
9. FIRST. Common Vulnerability Scoring System v3.1: Specification Document. URL: <https://www.first.org/cvss/v3.1/specification-document>
10. Saaty T.L. Decision Making with the Analytic Hierarchy Process. International Journal of Services Sciences, 2008, Vol. 1, No. 1, pp. 83–98. <https://doi.org/10.1504/IJSSCI.2008.017590>
11. Hwang C.L., Yoon K. Multiple Attribute Decision Making: Methods and Applications. Springer, 1981.
12. Saaty T. L. The Analytic Hierarchy Process: What It Is and How It Is Used // Mathematical Modelling. – 1987. – Vol. 9. – P. 161–176.

Дата першого надходження статті до видання: 15.05.2026
Дата прийняття статті до друку після рецензування: 14.08.2026
Дата публікації (оприлюднення) статті: 05.10.2026