



КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

УДК 004.056.5:656.7:519.86

DOI: <https://doi.org/10.17721/ISTS.2025.10.5-15>

Анна ІЛЬЄНКО, канд. техн. наук, доц.

ORCID ID: 0000-0001-8565-1117

e-mail: anna.ilienko@npp.kai.edu.uaДержавне некомерційне підприємство "Державний університет
«Київський авіаційний інститут»", Київ, Україна

Валентина ТЕЛЮЩЕНКО, асп.

ORCID ID: 0000-0001-6026-5105

e-mail: valentyna.teliushchenko@npp.kai.edu.uaДержавне некомерційне підприємство "Державний університет
«Київський авіаційний інститут»", Київ, Україна

МЕТОДИ ОЦІНЮВАННЯ РИЗИКІВ КІБЕРЗАГРОЗ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ ОБ'ЄКТІВ ЦИВІЛЬНОЇ АВІАЦІЇ

Вступ. Цивільна авіація належить до критичної інфраструктури, а її наземні інформаційно-комунікаційні системи (ІКС) – аеропортові операційні платформи, інтеграційні шлюзи, мережі та служби підтримки – стикаються з різноманітним ландшафтом кіберзагроз. Для керованого вибору підходів до оцінювання ризиків потрібен прозорий і відтворюваний інструмент, узгоджений із вимогами ICAO/EASA/ISO й операційними обмеженнями аеропортів та авіаперевізників.

Методи. Запропоновано коротку модель багатокритеріального аналізу (МКА) з лінійним зваженням сумуванням (WSM). Як альтернативу взято NIST SP 800-30/CSF, CRAMM, OCTAVE Allegro, EBIOS RM, TARA. Критерії моделі: відповідність стандартам, глибина аналізу, гнучкість, легкість упровадження, вартість / ресурсомісткість. Ваги моделі нормовані (сума дорівнює 1), оцінки експертні за шкалою 1–5 з "оберненою" інтерпретацією вартості. Обчислено матрицю зважених компонентів, інтегральний бал і його нормовану форму. Введено чотирирівневу шкалу прийняття рішень із трьома порогоми та проведено аналіз чутливості через сценарне варіювання ваг.

Результати. Загальне ранжування підтвердило перевагу NIST SP 800-30/CSF, тоді як EBIOS RM продемонстрував результат, близький до лідера. У безпеково-критичному сценарії перші позиції посідають NIST і CRAMM, а у бюджетному та сценарії швидкого впровадження першість переходить до EBIOS RM, за яким іде NIST. OCTAVE Allegro доцільно розглядати як "умовно рекомендований" збалансований компроміс, а TARA – як рішення для швидкої пріоритизації за обмежених ресурсів. У типових умовах експлуатації, де ключовими є вартість і оперативність, CRAMM поступається через високу ресурсомісткість. Отримані результати загалом залишаються стійкими до помірних змін ваг.

Висновки. Модель МКА/WSM забезпечує прозоре, відтворюване й інтерпретоване порівняння фреймворків ризик-менеджменту для наземних ІКС цивільної авіації і може бути інтегрована у системи підтримки рішень. Підхід поєднує нормативну відповідність із практичною реалізованістю та підтримує сценарний вибір. Перспективи – автоматизація вибору ваг і критеріїв із застосуванням методів ШІ.

Ключові слова: цивільна авіація, ІКС, кіберризик, багатокритеріальний аналіз, метод зваженої суми, NIST.

Вступ

Цивільна авіація (ЦА) відіграє ключову роль у світовій інфраструктурі, поєднуючи країни та людей через економічні й соціальні зв'язки. Її функціонування все більше залежить від складних інформаційно-керуючих систем, які підтримують планування, управління, взаємодію та моніторинг у реальному часі. У цій роботі під "об'єктами цивільної авіації" розуміємо організації та інфраструктуру, залучені до забезпечення авіаційних перевезень і наземного обслуговування, зокрема й аеропорти, авіакомпанії, провайдери наземного обслуговування та суміжні служби. Інформаційні та керуючі системи, що забезпечують критичні бізнес-процеси цих суб'єктів, становлять інформаційно-комунікаційні системи (ІКС) ЦА. Подальший аналіз обмежено наземними ІКС, які обслуговують суб'єктів ЦА. Сюди належать системи аеропортових операцій (база операційних даних аеропорту, відображення рейсової інформації для пасажирів і операційних служб, реєстрація, оформлення багажу та посадка, транспортування, сортування та відстеження багажу тощо) та їхні підсистеми керування й моніторингу (SCADA/PLC, телеметрія), інтеграційні інтерфейси й операційні сервіси підтримки, корпоративні мережі та сервіси взаємодії, а також інженерні й охоронні системи керування об'єктів інфраструктури аеропорту. Бортіві комплекси авіоніки не входять до сфери, розглянутої в цій статті (Aryanti, Anwar, & Rahmawati, 2023).

Поширення цифрових технологій розширює сукупність точок входу та векторів доступу, під якими розуміємо набір цифрових активів, інтерфейсів, мережних вузлів, точок доступу, сервісів і процесів взаємодії, через які потенційний зломисник може реалізувати загрозу. Для об'єктів цивільної авіації це охоплює як прикладні ІТ-сервіси (електронна реєстрація, обмін повідомленнями, інформаційні портали для пасажирів і партнерів), так і технологічні компоненти наземної інфраструктури (системи керування багажем, енергетичні й інженерні підсистеми, доступ і відеоспостереження, мережні сегменти взаємодії з авіакомпаніями та підрядниками). З огляду на те, що об'єкти ЦА належать до критичної інфраструктури, наслідки кіберінцидентів можуть включати переривання бізнес-процесів, часткові або повні збої в наданні послуг аеропортом і суміжними службами, фінансові та репутаційні втрати, а в граничних випадках – ризики для безпеки пасажирів і персоналу (Dobrynin et al., 2018).



Міжнародні організації, зокрема IATA (International Civil Aviation Organization, 2025), систематично окреслюють виклики, пов'язані з новими кіберзагрозами для галузі, надають рекомендації та оновлюють стандарти для складових авіаційної екосистеми, що охоплює авіакомпанії, аеропорти та наземні служби. В Україні кіберзахист об'єктів критичної інфраструктури, включно з об'єктами цивільної авіації, регламентовано Постановою КМУ від 19.06.2019 № 518, яка вимагає впровадження політики управління ризиками інформаційної безпеки та застосування методик їх оцінювання й оброблення на всіх таких об'єктах (<https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text>). Як методичну основу рекомендовано використовувати стандарт ДСТУ ISO/IEC 27005, що відповідає міжнародній практиці.

З огляду на зростання кіберзагроз і на нормативні вимоги, актуальним стає завдання обрати релевантні методи оцінювання ризиків саме для наземних ІКС цивільної авіації. У цій статті запропоновано формалізований підхід до порівняння таких методик на основі багатокритеріального аналізу з використанням методу зваженої суми, що забезпечує відтворюваний і інтерпретований вибір з урахуванням як відповідності стандартам, так і практичних обмежень упровадження в умовах реальної експлуатації.

Метою статті є розроблення математичної моделі багатокритеріального аналізу (МКА) для визначення найбільш релевантних фреймворків оцінювання кіберризиків в ІКС об'єктів ЦА на основі методу зваженої суми (WSM). Модель має забезпечувати формалізований і обґрунтований вибір методик управління ризиками шляхом порівняння різних альтернатив за системою кількісних критеріїв.

Огляд літератури. З кожним роком оцінювання ризиків кіберзагроз в ІКС стає дедалі важливішим для цивільної авіації і є одним із ключових напрямів сучасних досліджень у сфері авіаційної безпеки, і вимагає більш обґрунтованого і комплексного підходу, що поєднує міжнародні стандарти, національне законодавство, найкращі світові практики.

Науковці приділяють значну увагу розробленню методів, моделей для своєчасного виявлення кіберзагроз, використовують різні методики для кількісного та якісного оцінювання ризиків, удосконалюють існуючі методи.

Науковими дослідженнями окремих питань у сфері оцінювання ризиків кібербезпеки інформаційних систем на об'єктах критичної інфраструктури, зокрема і в авіаційній галузі присвячено роботи таких науковців як: А. Костін, О. Корченко, С. Гнатюк, А. Ільєнко, С. Ільєнко, І. Сіє, А. Алмараді, Е. Укванду, Ш. Фей та ін.

Дослідженнями А. Костіна запропоновано концепцію створення лабораторії, яка дозволяє як "тренажер" моделювати реалістичні кіберінциденти, створювати симуляції реальних кібератак і відпрацьовувати нові методи зниження ризиків.

Науковець Сунго Чо запропонував підхід, який передбачає розроблення тестового середовища для промислових систем, із використанням методології MITRE ATT&CK, як основи для побудови сценарію атак. Це дослідження є важливим для перевірки ефективності кіберзахисту систем управління аеропортами чи іншими важливими критичними об'єктами авіаційної інфраструктури, оскільки дає змогу відтворювати реалістичні умови атак і оцінювати готовність систем до потенційних загроз.

Останні наукові дослідження та публікації окреслюють актуальні виклики у сфері оцінювання ризиків кібербезпеки та пропонують різні шляхи їх подолання. Водночас ефективний захист ІКС цивільної авіації неможливий без комплексного поєднання міжнародних стандартів і гнучких методів, адаптованих до галузевих особливостей. Такий підхід передбачає не лише впровадження перевірених практик, але й їхнє систематичне вдосконалення. Із цією метою необхідно здійснити поглиблений аналіз наявних методик оцінювання ризиків ІКС, аби забезпечити формування більш цілісної та ефективної системи захисту цих критично важливих об'єктів.

Методи

Використано поєднання теоретичних і математичних методів. Здійснено аналіз і узагальнення наукових джерел і нормативних документів (систематизація стандартів ICAO/EASA/ISO), на підставі чого побудовано кортежну модель багатокритеріального аналізу (МКА) з визначенням критеріїв і ваг. Кількісне оброблення виконано методом зваженої суми із лінійним нормуванням min-max, ранжуванням альтернатив і пороговим правилом прийняття рішень.

Результати

Авіаційна галузь, що охоплює авіакомпанії, аеропорти та пов'язані з ними служби, функціонує як критична інфраструктура з багаторівневими цифровими взаємодіями. Інтенсивна цифровізація, використання інтелектуальних систем хмарних платформ, інтернету речей, аналітики великих даних і блокчейну формує складний ландшафт кіберзагроз, тобто множину потенційних векторів і каналів впливу на ІКС.

Захист цивільної авіації від кібератак здійснюється впровадженням Стандартів і рекомендованих практик кібербезпеки Міжнародною організацією цивільної авіації ICAO (International Civil Aviation Organization, 2018). Вона розробляє Стандарти та рекомендовану практику (SARPs, Standards and Recommended Practices), які є складовою Додатків до Чиказької конвенції 1944 р. Стандарти (Standards) є обов'язковими до виконання для держав-учасниць, тоді як рекомендована практика (Recommended Practices) установлює бажані заходи, які можуть адаптуватися відповідно до національних умов.

Розроблення та впровадження методик оцінювання ризиків кіберзагроз в авіації неможливі без урахування міжнародних стандартів і регламентів, які визначають вимоги до ІКС.

Огляд ключових міжнародних стандартів і методик управління ризиками. Управління ризиками кібербезпеки в ІКС авіаційної галузі ґрунтується на міжнародних стандартах і методиках, які формують цілісну систему оцінювання, контролю та зменшення ризиків.

Міжнародна практика управління ризиками інформаційної безпеки базується на ряді стандартів і фреймворків, серед яких ключову роль відіграють ISO/IEC 27005, ISO 31000, NIST SP 800-30, NIST CSF, а також галузеві підходи EASA Part-IS, ICAO Doc 10213, CRAMM, OCTAVE, EBIOS і TARA.

Розглянемо Міжнародний стандарт ISO/IEC 27005 "Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки" (Information technology. Security techniques. Information security risk management), (ISO/IEC 27005: 2022. <https://www.iso.org/standard/80585.htm>) надає керівництво з управління ризиками інформаційної безпеки і є складовою сімейства стандартів ISO/IEC 27000. Процес включає етапи встановлення контексту, ідентифікації та аналізу ризиків, оброблення ризиків та моніторингу. Стандарт є гнучким, оскільки не встановлює конкретних методів оцінювання ризиків, що дає організаціям свободу у виборі інструментів.



ISO 31000 "Менеджмент ризиків. Принципи та настанови" (Risk management. Guidelines) (ISO 31000: 2018. <https://www.iso.org/standard/65694.html>) є загальним міжнародним документом, що визначає уніфіковані підходи до управління ризиками і містить принципи та настанови, придатні для будь-яких типів ризиків (фінансових, операційних, безпекових). Він охоплює етапи: встановлення контексту, оцінювання ризиків (ідентифікація, аналіз, оцінка), обробку, моніторинг та комунікацію ризиків. Перевага стандарту – універсальність і можливість інтеграції в будь-яку галузь.

Серед методик США особливе значення має NIST SP 800-30 "Guide for Conducting Risk Assessments" (NIST SP 800-30:2012. <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>), який описує поетапний процес оцінювання ризиків інформаційних систем: від підготовки та збору даних до аналізу загроз, вразливостей і наслідків. Комплексна система NIST охоплює також пов'язані документи, серед яких:

- NIST SP 800-37 – упровадження Risk Management Framework у життєвий цикл систем безпеки;
- NIST SP 800-39 – багаторівневе управління ризиками на рівнях організації, місії та інформаційної системи;
- NIST SP 800-53 Rev.5 – каталог контролів безпеки й приватності;
- NIST SP 800-82 Rev.2 – керівництво з безпеки щодо промислових та авіаційних ІКС.

Ці стандарти взаємно доповнюють один одного, утворюючи цілісну модель, у якій оцінювання ризику (NIST SP 800-30) інтегрується з управлінськими процесами (NIST SP 800-37, 2018), впровадженням контролів (NIST SP 800-53, 2020) та специфікою промислових і авіаційних систем. Їх об'єднує NIST Cybersecurity Framework (CSF) – узагальнювальна "рамка" з п'яти базових функцій: ідентифікація (Identify), захист (Protect), виявлення (Detect), реагування (Respond), відновлення (Recover), що використовується як практичний орієнтир для критичної інфраструктури, зокрема й авіаційних ІКС.

Європейське агентство з авіаційної безпеки (European Union Aviation Safety Agency, EASA, 2023. <https://www.easa.europa.eu/en/document-library/regulations/commission-implementing-regulation-eu-2023203>) відповідає за встановлення стандартів безпеки польотів і сертифікацію авіаційних організацій.

Особливого значення набула регуляція EASA Part-IS (Information Security, 2023), що встановлює обов'язковість систем управління кіберризиками та проводить регулярне оцінювання загроз і вразливостей для авіаційних операторів, аеропортів і виробників. Регламент набуває повної чинності з лютого 2026 р. та вимагає інтеграції оцінювання кіберзагроз в операційні процеси.

Міжнародна асоціація повітряного транспорту IATA у своїх публікаціях (Aviation Cybersecurity Fact Sheet, 2025: <https://www.iata.org/contentassets/4c51b00fb25e4b60b38376a4935e278b/compilation-of-cyber-regs.pdf>) та (Compilation of Cyber Security Regulations, 2022: <https://www.iata.org/contentassets/4c51b00fb25e4b60b38376a4935e278b/compilation-of-cyber-regs.pdf>) узагальнює міжнародні вимоги, практики й рекомендації, наголошуючи на формуванні "спільнот довіри", стандартизації підходів і підвищенні обізнаності галузі щодо кіберризиків.

ICAO у своїх документах (ICAO Doc 10108, ICAO Doc 10213) визначають підходи до інтеграції кіберризиків у загальну авіаційну систему безпеки.

Відповідно до ICAO Doc 10213 (International Civil Aviation Organization, 2025) кількісне оцінювання ризику здійснюється за формулою

$$R = L \times I \times V, \quad (1)$$

де L – імовірність (Likelihood); I – вплив (Impact); V – рівень вразливості (Vulnerability).

Цей підхід дає змогу узгоджено оцінювати вплив кіберінцидентів на безпеку польотів і безперервність процесів у аеропортах.

В Україні нормативною основою управління кіберризиками є Постанова КМУ № 518 від 19.06.2019 р., яка встановлює загальні вимоги до кіберзахисту об'єктів критичної інфраструктури і зобов'язує операторів, зокрема й авіаційні організації, упроваджувати політику управління ризиками та здійснювати регулярне оцінювання відповідно до стандарту ДСТУ ISO/IEC 27005.

Поряд із нормативними документами, у практиці ризик-менеджменту застосовують відомі спеціалізовані методи, серед яких:

- CRAMM (CCTA Risk Analysis and Management Method) забезпечує детальний покроковий аналіз активів, загроз і вразливостей із формуванням каталогу контрзаходів. Ефективна для великих інфраструктурних об'єктів, але потребує значних ресурсів.
- OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) орієнтована на організаційний рівень і поєднує технічні, людські й управлінські фактори, дає змогу будувати комплексну стратегію безпеки.
- EBIOS (Expression des Besoins et Identification des Objectifs de Securite), що розроблена агентством ANSSI, зосереджується на визначенні потреб безпеки й цілей захисту, забезпечуючи відповідність вимогам ISO 27005.
- TARA (Threat Assessment and Remediation Analysis) фокусується на аналізі актуальних загроз і пріоритизації ризиків з огляду на критичність функцій. Методика тісно пов'язана з даними розвідки загроз і застосовується як практичний інструмент "першої лінії" кіберзахисту.

Поєднання зазначених стандартів і методик формує основу інтегрованого ризик-орієнтованого підходу до управління кіберзагрозами в авіаційних ІКС, що відповідає вимогам міжнародної та національної нормативних баз і забезпечує узгодженість дій між авіаційними, технічними та кібернетичними підрозділами.

Отже, ефективна система оцінювання ризиків в авіаційних ІКС повинна ґрунтуватися на інтегрованому поєднанні нормативних (ISO, NIST, EASA, ICAO) та практичних методик (CRAMM, OCTAVE, EBIOS, TARA), що забезпечує структурованість, порівнюваність і відповідність міжнародним вимогам.

Проведений аналіз міжнародних стандартів і фреймворків (EASA Part-IS, ICAO Doc 10213, IATA Cybersecurity Framework, CRAMM, OCTAVE, EBIOS, TARA) показує, що всі вони пропонують різні рівні деталізації процесу управління ризиками, але не містять єдиного механізму кількісного порівняння та вибору найбільш релевантного підходу для конкретної організації цивільної авіації.



Зокрема, EASA Part-IS фокусується на нормативній відповідності та побудові системи управління інформаційною безпекою (СУІБ); ICAO Doc 10213 – на інтеграції кіберризиків у загальну систему авіаційних ризиків; CRAAM, OCTAVE, EBIOS, TARA провадять практичну реалізацію процесу оцінювання й управління ризиками, кожен із них має власні сильні сторони (глибина, гнучкість, структурованість) (Central Computer and Telecommunications Agency, 2001; International Civil Aviation Organization, 2018; International Civil Aviation Organization, 2025; National Agency for Information Systems Security, 2024).

У контексті авіаційної інфраструктури виникає потреба у формалізованому інструменті, який дозволяє одночасно враховувати кілька критеріїв ефективності підходів до управління ризиками (відповідність, гнучкість, вартість, масштабованість тощо) та забезпечує кількісне оцінювання їхньої придатності для конкретних ІКС.

Для цього доцільно застосовувати багатокритеріальний метод оцінювання (Multi-Criteria Analysis, MCA), що базується на методі зваженої суми (Weighted Sum Model, WSM). Такий підхід дозволяє об'єднати експертні оцінки за різними критеріями в єдину інтегральну метрику релевантності та здійснювати ранжування фреймворків за їхньою придатністю.

Метод WSM – це реалізація багатокритеріального аналізу, який дає змогу оцінювати альтернативи за сукупністю критеріїв, одночасно враховуючи відносну вагомість кожного з них. У результаті отримують інтегральний зважений бал, який використовують для кількісного порівняння варіантів і прийняття рішень (Potii et al., 2021).

Розглянемо математичну модель MCA методу визначення релевантних фреймворків для оцінювання ризиків в ІКС об'єктів цивільної авіації методом WSM.

Математична модель MCA для оцінювання ризиків в ІКС об'єктів цивільної авіації методом зваженої суми має такий узагальнений вигляд:

$$MCA = \{U_{i=1}^n MCA_i\} = \{MCA_1, MCA_2, MCA_3, \dots, MCA_n\}, \quad (2)$$

де $MCA_i \subseteq MCA$, $(1, n)$ – ключовий компонент кортежної моделі характеристик, що демонструє i -й ідентифікатор параметра оцінювання релевантного фреймворка, n – їхня кількість.

Наприклад, при $n = 8$ кортежна модель для узагальненої математичної моделі (2) виглядатиме як

$$MCA = \left\{ \bigcup_{i=1}^n MCA_i \right\} = \{MCA_1, MCA_2, MCA_3, \dots, MCA_n\} = \{M, K, W, Q, P, S, S^{norm}, D\}, \quad (3)$$

де $MCA_1 = M = \text{"Method"}$ – модуль, що містить множину альтернатив, тобто можливих фреймворків оцінювання кіберризиків; $MCA_2 = K = \text{"Criteria"}$ – модуль, що містить множину критеріїв оцінювання, за якими порівнюють альтернативи; $MCA_3 = W = \text{"Weight"}$ – модуль, який містить множину вагових коефіцієнтів критеріїв, що відображають відносну важливість кожного критерію з K в загальній оцінці; $MCA_4 = Q = \text{"Expert – assessments"}$ – модуль, який містить матрицю експертних оцінок; $MCA_5 = P = \text{"Weight – Sum"}$ – модуль матриці зважених компонентів; $MCA_6 = S = \text{"Integral – Sum"}$ – модуль сукупності підсумкових WSM-балів альтернатив (WSM – *Weighted Sum Method* – метод зваженої суми); $MCA_7 = S^{norm} = \text{"Integral – Sum – Normalized"}$ – модуль сукупності нормованих підсумкових WSM-балів альтернатив; $MCA_8 = D = \text{"Decision"}$ – модуль множин прийнятих рішень, тобто вибраних альтернатив-фреймворків, які визнані найкращими (релевантними) за результатами багатокритеріального аналізу.

Перший компонент узагальненої математичної моделі M – модуль сукупності альтернативних фреймворків оцінювання ризиків, допустимих для застосування в ІКС цивільної авіації визначається виразом

$$M = \{U_{i=1}^n M_i\} = \{M_1, M_2, M_3, \dots, M_n\}, \quad (4)$$

де $M_i \subseteq M$, $(1, n)$ – кожен елемент M_i репрезентує окремий фреймворк (методологію, стандарт чи підхід щодо оцінювання ризиків) із фіксованими властивостями й умовами застосування для оцінювання ризиків, релевантний для ІКС цивільної авіації. Тут n – загальна кількість таких альтернатив, надалі ці елементи підлягають порівнянню за множиною критеріїв K . Отже, M задає простір вибору для процедури ранжування та визначає перелік альтернатив, серед яких ухвалюється рішення.

Другий компонент узагальненої математичної моделі K – модуль структурованої сукупності оціночних критеріїв, за якими здійснюється зіставлення та ранжування альтернатив з M визначається виразом

$$K = \{U_{j=1}^m K_j\} = \{K_1, K_2, K_3, \dots, K_m\}, \quad (5)$$

де $K_j \subseteq K$, $(1, m)$, кожен елемент K_j описує окремий критерій (показник) якості або відповідності фреймворку (напр., охоплення технічних аспектів, відповідність міжнародним стандартам, простота впровадження, вартість застосування тощо); m – кількість вибраних критеріїв.

Третій компонент W – модуль сукупності вагових коефіцієнтів критеріїв, що відображають відносну важливість кожного критерію з K в загальній оцінці, визначається виразом

$$W = \{U_{j=1}^m W_j\} = \{W_1, W_2, W_3, \dots, W_m\}, \quad (6)$$

де $W_j \subseteq W$, $(1, m)$, кожна вага W_j зіставляється з критерієм K_j . Більше значення W_j означає, що критерій K_j більше впливає на підсумкову оцінку альтернативи, ніж критерії з меншими вагами.

Зазвичай, ваги нормуються так, що

$$\sum_{j=1}^m W_j = 1, \quad W_j \geq 0 \quad \forall j \in \{1, \dots, m\}. \quad (7)$$

Ваги є дробовими числами, сумарно рівними 1, що відображає розподіл важливості між критеріями.

Четвертий компонент Q – матриця експертних оцінок визначається виразом

$$Q := \{Q_i\}_{i=1}^n, Q_i := \langle q_{i1}, \dots, q_{im} \rangle \in \mathbb{R}^m, \quad (8)$$

де $i = \{1, \dots, n\}$ – індекси альтернатив; $j = \{1, \dots, m\}$ – індекси критеріїв; q_{ij} – відображає значення показника альтернативи M_i за критеріями K_j , сформоване на підставі експертного оцінювання або аналітичного розрахунку.



П'ятий модуль P – модуль матриці зважених компонентів визначається виразом

$$P := \{P_i\}_{i=1}^n, P_i := \langle p_{i1}, p_{i2}, \dots, p_{im} \rangle, p_{ij} := W_j q_{ij}, \quad (9)$$

де p_{ij} – зважений компонент за критерієм K_j ; W_j – вага критерію K_j (з $\sum_{j=1}^m W_j = 1, W_j \geq 0$).

Матрицю P отримують шляхом почленного множення стовпців матриці оцінок Q на відповідні ваги з W . Отже, p_{ij} кількісно відображає, наскільки альтернатива M_i задовольняє критерій K_j з урахуванням критерію K_j .

Шостий модуль S – інтегральна оцінка (сукупність інтегральних підсумкових WSM-балів альтернатив) визначається виразом

$$S := \{S_i\}_{i=1}^n, S_i := \sum_{j=1}^m p_{ij} = \sum_{j=1}^m W_j q_{ij}, \quad (10)$$

де S_i – інтегральний бал альтернативи M_i ; W_j – вага критерію K_j .

Для кожної альтернативи M_i обчислюється сумарний бал S_i як сума всіх зважених оцінок за всіма критеріями. Модуль S містить інтегральні (узагальнені) оцінки всіх альтернатив і слугує основою для їх порівняння. Більше значення S_i означає кращу сукупну відповідність фреймворка M_i заданим критеріям.

Сьомий модуль S_i^{norm} нормованих інтегральних балів визначається виразом

$$S_i^{norm} = \{S_i^{norm}\}_{i=1}^n, S_i^{norm} = \frac{S_i - S_{min}}{S_{max} - S_{min}} \in [0, 1], I = \{1, \dots, n\}, \quad (11)$$

де S_i^{norm} – нормований інтегральний бал альтернативи M_i ; S_{max} – максимум підсумкових інтегральних балів; S_{min} – мінімум підсумкових інтегральних балів.

Восьмий модуль D – модуль прийняття рішень, тобто фреймворків-альтернатив, відібраних як оптимальні (релевантні) за підсумками багатокритеріального оцінювання, визначається виразом

$$D = \{M_i \in M | S_i^{norm} \geq \tau_{min}\}, \quad (12)$$

де S_i^{norm} – нормований інтегральний бал альтернативи M_i ; τ_{min} – поріг прийняття рішень.

Для прийняття рішень уведемо три впорядковані порогові значення інтегральної оцінки S_i^{norm} . $S_i^{norm} \in [0, 1]$:

$$0 \leq \tau_{acc} \tau_{rec} \tau_{min}, \quad (13)$$

де τ_{rec} – поріг рекомендації: рівень, з якого фреймворк вважається безумовно доцільним; τ_{acc} – поріг прийнятності: мінімальний рівень якості / релевантності, з якого варіант можна рекомендувати умовно; τ_{min} – поріг мінімальної доцільності: нижня межа, нижче якої варіант не рекомендується.

Задаємо чотири рівні рішення, у кожному з яких визначимо порогові значення. Задані рівні представлено в табл. 1.

Таблиця 1

Рівні прийняття рішень

Діпазон	Категорія	Опис
$D^4 = \{M_i S_i^{norm} \geq \tau_{rec}\}$	Безумовно рекомендовані	Фреймворк має дуже високий рівень безпеки, продуктивності й ефективності. Рекомендується для використання у критичних системах
$D^3 = \{M_i \tau_{acc} \leq S_i^{norm} < \tau_{rec}\}$	Умовно рекомендовані	Алгоритм загалом ефективний, але може мати окремі недоліки (напр., потребує додаткових налаштувань або оптимізації). Використання можливе, але бажано провести аудит або додаткове тестування
$D^2 = \{M_i \tau_{acc} \tau_{min} \leq S_i^{norm} < \tau_{acc}\}$	Обмежене використання	Алгоритм має помірну ефективність або окремі недоліки, які роблять його менш придатним у критичних середовищах. Використання можливе лише за відсутності кращих альтернатив
$D^1 = \{M_i S_i^{norm} < \tau_{min}\}$	Не рекомендовані	Алгоритм має низьку ефективність або потенційні вразливості, що роблять його небезпечним або малоефективним для використання у сучасних системах. Слід уникати його впровадження

Якщо дві чи більше альтернативи мають однакові нормовані інтегральні оцінки S_i^{norm} в тому самому рівні, вибір здійснюємо порівнянням векторів зважених компонент P_i за порядком важливості за критеріями.

Зазначений практичний підхід допоможе приймати рішення на основі конкретного значення S_i^{norm} , наприклад, чи фреймворк рекомендований, чи краще його уникати у критичних системах.

Приклад застосування. Розглянемо використання наведеної моделі на прикладі. Для обґрунтованого вибору найкращого підходу в оцінюванні ризиків кіберзагроз проведемо MCA методом WSM, що враховує найважливіші критерії ефективності методики у сфері ЦА.

Згідно з формулою (4) назначимо множину альтернативних фреймворків (M), де кожен елемент M_i репрезентує окремий фреймворк. Множину фреймворків зазначено в табл. 2.

Таблиця 2

Множина фреймворків

Множина M_i	Назва альтернативних фреймворків
M_1	NIST SP 800-30/NIST CSF
M_2	CRAMM
M_3	OCTAVE
M_4	EBIOS
M_5	TARA



Для порівняння фреймворків визначимо п'ять оціночних критеріїв (K_j), кожному з яких призначимо ваговий коефіцієнт W_j ($\sum_{j=1}^m W_j = 1$) згідно з формулами (5) і (6). Дані представлено в табл. 2.

В табл. 3 відображено вагові коефіцієнти для п'яти критеріїв, які визначають відносну важливість кожного критерію в інтегральній оцінці. Сума ваг дорівнює 1, що забезпечує коректну інтерпретацію підсумкових балів як зваженої "середньої корисності".

Таблиця 3

Розподіл вагових коефіцієнтів за критеріями

Критерій, K_j	Назва критерію	Пояснення (коротко)	Вагові коефіцієнти, W_j
K_1	Відповідність міжнародним стандартам	Ступінь сумісності / узгодження методики з міжнародно визнаними підходами (ICAO/EASA/ISO)	0,25
K_2	Гнучкість застосування	Адаптивність до масштабу / типів ІКС, сумісність з іншими практиками	0,20
K_3	Глибина аналізу ризиків	Рівень деталізації: загрози, вразливості, сценарії, контролю	0,25
K_4	Легкість упровадження	Складність запуску, потреба в експертизі / команді	0,15
K_5	Вартість / ресурсомісткість	Умовна інтегральна "ціна" (час, люди, бюджет)	0,15

У табл. 4 наведено результати оцінювання з урахуванням вагових коефіцієнтів, тобто подано вихідну матрицю Q – матрицю експертних оцінок, де q_{ij} – експертна оцінка методики M_i за критерієм K_j за шкалою від 1 до 5 балів за кожним критерієм (5 – найвищий рівень відповідності критерію, 1 – найнижчий). Усі критерії трактують як вигравні (чим більше, тим краще), а для K_5 застосовано "обернену" інтерпретацію (5 означають нижчі витрати / вища віддача, 1 – дорогий підхід).

Таблиця 4

Матриця експертних оцінок кожної методики

Фреймворк, M_i	q_{i1}	q_{i2}	q_{i3}	q_{i4}	q_{i5}
NIST SP 800-30 / CSF	3	4	5	4	3
CRAMM	2	3	5	1	1
OCTAVE (Allegro)	3	4	4	3	3
EBIOS RM	4	4	5	2	2
TARA	2	3	3	5	5

Скориставшись формулою (9), розрахували зважені компоненти p_{ij} за кожним фреймворком, що кількісно показують внесок кожного критерію у підсумкову оцінку відповідного фреймворка з урахуванням його ваги. Надалі ці компоненти підсумовують для отримання інтегрального бала S_i і порівняння методик між собою. Результати представлено в табл. 5.

Таблиця 5

Зважені компоненти (внесок критерію)

Фреймворк, M_i	p_{i1}	p_{i2}	p_{i3}	p_{i4}	p_{i5}
NIST SP 800-30 / CSF	0,75	0,80	1,25	0,60	0,45
CRAMM	0,50	0,60	1,25	0,15	0,15
OCTAVE (Allegro)	0,75	0,80	1,00	0,45	0,45
EBIOS RM	1,00	0,80	1,25	0,30	0,30
TARA	0,50	0,60	0,75	0,75	0,75

Зважені компоненти демонструють, завдяки яким критеріям методики отримують перевагу. Для NIST максимальний внесок дає критерій K_3 (глибина аналізу) (1,25), що узгоджується з практичною орієнтацією SP 800-30/CSF. Для EBIOS RM провідними критеріями є K_1 (відповідність) і K_3 (глибина) (1,00 та 1,25), однак сумарний бал знижується через менші компоненти критеріїв K_4 (легкості) та K_5 (вартості) (по 0,30 кожен). OCTAVE (Allegro) демонструє збалансованість (усі компоненти близькі до середніх значень), що формує стабільний інтегральний результат.

TARA отримує найвищі компоненти за K_4 (легкості) та K_5 (вартість) (по 0,75 кожен), тому добре підходить для швидкої пріоритизації дій за обмежених ресурсів, але поступається за глибиною іншим фреймворкам. CRAMM має найбільший компонент глибини (1,25), проте дуже низькі компоненти K_4 (легкості) та K_5 (вартості) (по 0,150 кожен).

Компонентна подача полегшує аудит і аргументацію, тобто можна відразу бачити, чи відповідає домінування певної методики стратегічним пріоритетам (напр., $K_3 > K_1$ чи навпаки).

Скориставшись формулою (10), обрахували зважену суму S_i (інтегральний бал для кожної альтернативи M_i та згідно з формулою (11) розрахували нормований інтегральний бал S_i^{norm} альтернативи M_i . Результати підсумкових зважених WSM (інтегральних балів) і нормованих інтегральних балів представлено в табл. 6 ранжування методик. Ранжування виконано за спаданням інтегрального бала S_i .



Таблиця 6

Підсумкові та нормовано інтегральні бали (WSM)

Фреймворк, M_i	Інтегральний бал, S_i	Нормовано інтегральний бал, S_i^{norm}
NIST SP 800-30 / CSF	3,85	1,00
CRAMM	2,65	0,00
OCTAVE (Allegro)	3,45	0,67
EBIOS RM	3,65	0,83
TARA	3,35	0,58

Скориставшись формулою (12), введемо три впорядковані порогові значення.

Нехай $\tau_{i_{rec}} = 80$ – поріг рекомендації;

$\tau_{i_{acc}} = 0,55$ – поріг прийнятності;

τ_{min} – поріг мінімальної доцільності.

Тоді відповідно до табл. 1, задаємо чотири рівні рішення, у кожному з яких визначено порогові значення. Задані рівні прийняття рішень представлено в табл. 7.

Таблиця 7

Рівні прийняття рішень за заданих порогових значень

Діпазон, D^i	Категорія	Опис
$D^4 = \{M_i S_i^{norm} \geq 0,80\}$	Безумовно рекомендовані	Фреймворк має дуже високий рівень безпеки, продуктивності й ефективності. Рекомендується для використання у критичних системах
$D^3 = \{M_i 0,55 \leq S_i^{norm} < 0,80\}$	Умовно рекомендовані	Алгоритм загалом ефективний, але може мати окремі недоліки (напр., потребує додаткових налаштувань або оптимізації). Використання можливе, але бажано провести аудит або додаткове тестування
$D^2 = \{M_i 0,30 \leq S_i^{norm} < 0,55\}$	Обмежене використання	Алгоритм має помірну ефективність або окремі недоліки, які роблять його менш придатним у критичних середовищах. Використання можливе лише за відсутності кращих альтернатив
$D^1 = \{M_i S_i^{norm} < 0,30\}$	Не рекомендовані	Алгоритм має низьку ефективність або потенційні вразливості, що роблять його небезпечним або малоефективним для використання в сучасних системах. Слід уникати його впровадження

Скориставшись табл. 7, кожній з альтернатив визначили рівні прийняття рішень. Результати представлено в табл. 8.

Таблиця 8

Прийняття рішень щодо використання фреймворків

Фреймворк, M_i	Нормовано інтегральний бал, S_i^{norm}	Рівні прийняття рішень, D^i
NIST SP 800-30 / CSF	1,00	Безумовно рекомендовані
CRAMM	0,00	Не рекомендовані
OCTAVE (Allegro)	0,67	Умовно рекомендовані
EBIOS RM	0,83	Безумовно рекомендовані
TARA	0,58	Умовно рекомендовані

NIST SP 800-30/CSF має найвищий показник $S_i^{norm} = 1,00$ й віднесений до рівня "безумовно рекомендовані". Це зумовлено поєднанням максимальної глибини аналізу ризиків і високої відповідності вимогам і стандартам за збереження прийнятної легкості впровадження й витрат.

EBIOS RM має $S_i^{norm} = 0,83$ і також потрапляє до рівня "безумовно рекомендовані". Завдяки сильним компонентам відповідності та глибини він є близьким до лідера, однак поступається NIST через вищу ресурсомісткість / складність практичної реалізації (Intel Corporation, 2018; National Institute of Standards and Technology (NIST), 2018; National Institute of Standards and Technology (NIST), 2020).

OCTAVE (Allegro) віднесено до рівня "умовно рекомендовані". Методика демонструє стабільний, збалансований профіль за критеріями, однак величини відповідності і глибина недостатні, щоб перейти у верхній рівень за наявних ваг. Аналогічно,

TARA класифікується як "умовно рекомендовані". Попри те, що її перевагою є практичність і відносно низькі витрати / швидкість, упровадження обмеженості глибини та відповідності не дозволяє досягти порога рекомендації.

CRAMM отримує найнижчу нормовану оцінку та належить до рівня "не рекомендовані": попри високу глибину, метод є ресурсомістким і менш гнучким, що суттєво знижує інтегральний результат за зваженою сумою.



Оскільки WSM припускає адитивність і компенсаторність (слабкість за одним критерієм частково компенсується силою за іншим), для перевірки стійкості результатів (ранжування) до зміни пріоритетів виконано аналіз чутливості (варіювання ваг на $\pm 10\text{--}20\%$).

Аналіз чутливості виконано за рахунок перерозподілу ваг критеріїв відповідно до зміни пріоритетів (безпека / витрати / швидкість впровадження) для перевірки стійкості ранжування до змін. Для кожного сценарію перерозподілено ваги так, щоб $\sum_{j=1}^m W_j = 1$, і перераховано WSM-бали.

Виокремимо три сценарії, на які робиться практичний фокус: "безпеково-критичний", "бюджетно-орієнтований", "швидке впровадження". І кожному сценарію за нашими критеріями призначимо ваги. Дані представлено в табл. 9.

Таблиця 9

Альтернативні сценарії ваг критеріїв

Сценарій	W_1	W_2	W_3	W_4	W_5
A (безпеково-критичний)	0,25	0,15	0,35	0,15	0,10
B (бюджетно-орієнтований)	0,15	0,10	0,25	0,20	0,30
C (швидке впровадження)	0,15	0,10	0,20	0,30	0,25

Для безпеково-критичного сценарію підсилили вагу критерію K_3 (стійкість), для бюджетно-орієнтованого сценарію підсилили вагу критерію K_5 (вартість), для швидкого впровадження підсилили критерії K_4 (легкості) та K_5 (вартості) й повторно обчислили WSM-компоненти S_i для кожного сценарію і по кожному фреймворку M_i . Результати представлено в табл. 10–12. Для розрахунку матрицю експертних оцінок залишили незмінною, згідно з табл. 4.

Таблиця 10

WSM-компоненти, інтегральний і нормовано інтегральний бал для безпеково-критичного сценарію (ваги 0,25 / 0,15 / 0,35 / 0,15 / 0,10)

Фреймворк, M_i	p_{i1}	p_{i1}	p_{i2}	p_{i3}	p_{i4}	Інтегральний бал, S_i^{s-c}	Нормовано інтегральний бал, $S_i^{norm(s-c)}$
NIST SP 800-30 / CSF	0,75	0,60	1,75	0,60	0,30	4,00	1,00
CRAMM	1,00	0,60	1,75	0,30	0,20	3,85	0,86
OCTAVE (Allegro)	0,75	0,60	1,40	0,45	0,30	3,50	0,52
EBIOS RM	0,50	0,45	1,05	0,75	0,50	3,25	0,29
TARA	0,50	0,45	1,75	0,15	0,10	2,95	0,00

S_i^{s-c} – інтегральний бал по кожному фреймворку для безпеково-критичного сценарію;

$S_i^{norm(s-c)}$ – нормований інтегральний бал по кожному фреймворку для безпеково-критичного сценарію.

Таблиця 11

WSM-компоненти, інтегральний і нормовано інтегральний бал для бюджетно-орієнтованого сценарію (ваги 0,15 / 0,10 / 0,25 / 0,20 / 0,30)

Фреймворк, M_i	p_{i1}	p_{i2}	p_{i3}	p_{i4}	p_{i5}	Інтегральний бал, S_i^{b-or}	Нормовано інтегральний бал, $S_i^{norm(b-or)}$
NIST SP 800-30 / CSF	0,45	0,40	1,25	0,80	0,90	3,80	0,92
CRAMM	0,60	0,40	1,25	0,40	0,60	3,25	0,00
OCTAVE (Allegro)	0,45	0,40	1,00	0,60	0,90	3,35	0,17
EBIOS RM	0,30	0,30	0,75	1,00	1,50	3,85	1,00
TARA	0,45	0,40	1,25	0,80	0,90	3,80	0,92

S_i^{b-or} – інтегральний бал по кожному фреймворку для бюджетно-орієнтованого сценарію;

$S_i^{norm(b-or)}$ – нормований інтегральний бал по кожному фреймворку для бюджетно-орієнтованого сценарію.

Таблиця 12

WSM-компоненти, інтегральний і нормовано інтегральний бал для сценарію швидкого впровадження (ваги 0,15 / 0,10 / 0,20 / 0,30 / 0,25)

Фреймворк, M_i	p_{i1}	p_{i2}	p_{i3}	p_{i4}	p_{i5}	Інтегральний бал, S_i^{r-imp}	Нормовано інтегральний бал, $S_i^{norm(r-imp)}$
NIST SP 800-30 / CSF	0,45	0,40	1,00	1,20	0,75	3,80	0,92
CRAMM	0,60	0,40	1,00	0,60	0,50	3,10	0,53
OCTAVE (Allegro)	0,45	0,40	0,80	0,90	0,75	3,30	0,64
EBIOS RM	0,30	0,30	0,60	1,50	1,25	3,95	1,00
TARA	0,30	0,30	1,00	0,30	0,25	2,15	0,00



S_i^{r-imp} – інтегральний бал по кожному фреймворку для сценарію швидкого впровадження;

$S_i^{norm(r-imp)}$ – нормований інтегральний бал по кожному фреймворку для сценарію швидкого впровадження.

Скориставшись табл. 7, кожний з альтернатив визначили рівні прийняття рішень за трьома сценаріями: безпечно-критичним, бюджетно-орієнтованим, швидкого впровадження. Результати занесено в табл. 13–15 відповідно.

Таблиця 13

Прийняття рішень щодо використання фреймворків
для безпечно-критичного сценарію

Фреймворк, M_i	Нормовано інтегральний бал, $S_i^{norm(s-c)}$	Рівні прийняття рішень, D^i
NIST SP 800-30 / CSF	1,00	Безумовно рекомендовані
CRAMM	0,86	Безумовно рекомендовані
OCTAVE (Allegro)	0,52	Обмежене використання
EBIOS RM	0,29	Не рекомендовані
TARA	0,00	Не рекомендовані

Лідерами для безпечно-критичного сценарію є фреймворки NIST SP 800-30 / CSF і CRAMM. Вони мають найвищі ваги за критеріями глибини аналізу і відповідність стандартам. CRAMM втрачає у практичності, але це не критично за цього профілю ваг.

Таблиця 14

Прийняття рішень щодо використання фреймворків
для бюджетно-орієнтованого сценарію

Фреймворк, M_i	Нормований інтегральний бал, $S_i^{norm(b-or)}$	Рівні прийняття рішень, D^i
NIST SP 800-30 / CSF	0,92	Безумовно рекомендовані
CRAMM	0,00	Не рекомендовані
OCTAVE (Allegro)	0,17	Не рекомендовані
EBIOS RM	1,00	Безумовно рекомендовані
TARA	0,92	Безумовно рекомендовані

Лідерами для бюджетно-орієнтованого сценарію є фреймворки EBIOS RM, NIST SP 800-30 / CSF TARA. EBIOS очолює лідерство завдяки хорошему компромісу "глибина-практичність"; NIST SP 800-30 / CSF – завдяки стабільно високим таким критеріям: відповідність, гнучкість і глибина; TARA – через сильні критерії – легкість впровадження та вартість.

Таблиця 15

Прийняття рішень щодо використання фреймворків
для сценарію швидкого впровадження

Фреймворк, M_i	Нормовано інтегральний бал, $S_i^{norm(r-imp)}$	Рівні прийняття рішень, D^i
NIST SP 800-30 / CSF	0,92	Безумовно рекомендовані
CRAMM	0,53	Обмежене використання
OCTAVE (Allegro)	0,64	Умовно рекомендовані
EBIOS RM	1,00	Безумовно рекомендовані
TARA	0,00	Не рекомендовані

Лідерами сценарію швидкого впровадження є фреймворки NIST SP 800-30 / CSF, EBIOS RM. Ці методики забезпечують достатню глибину при прийнятній операційній "легкості".

Узагальнюючи питання вибору "найкращої методики", можна сказати, що NIST SP 800-30/CSF є стійким лідером (топівень у всіх сценаріях), коли в пріоритеті відповідність і глибина; оптимальний для безпечно-критичних систем і як базовий корпоративний підхід.

За потреби швидкого або економного розгортання у разі збереження достатньої глибини краще використовувати EBIOS RM. Він є лідером у сценаріях бюджет / швидкість.

Якщо потрібна операційна простота й економність, то раціонально використовувати методику TARA, але вона програє за глибиною та відповідністю.

Компромисним, переважно "умовним" вибором є OCTAVE (Allegro), CRAMM доречно використовувати у "вузьких" випадках, коли прийнятна висока ресурсомісткість заради формалізованої глибини.

Узагальнюючи результати, зазначимо, що застосування побудованої кортежної моделі MCA з обчисленням інтегрального бала за методом WSM продемонструвало свою практичну ефективність для вибору фреймворків оцінювання кіберризиків в ІКС авіації. На етапі обчислень підхід залишається простим і зрозумілим. Підсумковий бал S_i для кожної методики обраховують як суму добутків "оцінка × вага" за всіма критеріями, тож внесок кожного критерію легко побачити у векторі зважених компонент P_i . Для вхідних даних достатньо узгодженої експертної



шкали (напр., 1–5), а подальше нормування зводить результати до єдиної шкали [0,1]. Це спрощує інтерпретацію для керівництва, внутрішнього аудиту та регуляторних органів і робить аргументацію вибору прозорою.

Ключовою перевагою моделі є керована гнучкість. Критерії та їхні ваги W_i легко переналаштовуються під управлінський контекст: безпеково-критичний, бюджетно-орієнтований або сценарій швидкого впровадження. Саме це показано в отриманих нами результатах: за пріоритету відповідності та глибини (безпеково-критичний сценарій) найкращими виявилися NIST SP 800-30/CSF (лідер) і CRAMM, якщо спостерігаємо зсув ваг у бік вартості та швидкості імплементації, то верхні позиції посідають EBIOS RM і NIST, тоді як OCTAVE і TARA проявляють себе як раціональні компромісні варіанти залежно від обмежень.

Запроваджена чотирирівнева шкала прийняття з трьома порогами перетворює числові бали на чіткі управлінські висновки, такі як "безумовно рекомендовано", "умовно рекомендовано", "обмежене застосування", "не рекомендовано" й уможливорює єдине правило вибору переможця в межах рівня (Swan, 2019).

Дискусія і висновки

Застосування багатокритеріального аналізу за методом WSM продемонструвало ефективність як інструмент для обґрунтованого порівняння та ранжування методик оцінювання кіберризиків в ІКС ЦА. Метод забезпечує прозору логіку прийняття рішень, оскільки дозволяє кількісно врахувати внесок кожного критерію та вагового коефіцієнта у підсумкову оцінку.

Перевага підходу полягає у простоті реалізації, відсутності складних вимог до оброблення даних і можливості швидкої адаптації вагових коефіцієнтів до контексту завдання, наприклад, посилення критерію "глибина аналізу" для критичних систем безпеки або підвищення ваги "легкості впровадження" за потреби оперативного розгортання.

Проведення аналізу чутливості підвищує достовірність результатів, дозволяючи оцінити стабільність отриманого ранжування у разі зміни вагових коефіцієнтів. Такий підхід сприяє сценарному аналізу та мінімізує суб'єктивність у прийнятті управлінських рішень.

У контексті ІКС ЦА використання методу WSM є доцільним завдяки його узгодженості з вимогами міжнародних стандартів ISO/IEC 27005, ISO 31000 та NIST CSF. Отримані результати можуть слугувати основою для формування комбінованої системи управління ризиками, де WSM використовують як базовий інструмент для попередньої пріоритизації методик або сценаріїв ризику.

Отже, запропонований підхід поєднує простоту, гнучкість і аналітичну обґрунтованість, що робить його придатним для практичного застосування в системах кібербезпеки авіаційної інфраструктури, а також перспективним для подальшого розвитку, зокрема і шляхом інтеграції елементів штучного інтелекту для автоматизації вибору критеріїв і динамічного оновлення вагових коефіцієнтів.

Внесок авторів: Анна Ільєнко – концептуалізація, методологія; Валентина Телющенко – аналіз джерел, підготовка огляду літератури, теоретичних засад дослідження, проведення дослідження.

Джерела фінансування. Це дослідження не отримало жодного гранту від фінансової установи в державному, комерційному або некомерційному секторах.

Список використаних джерел

- Aryanti, U., Anwar, M. T., & Rahmawati, T. (2023). Information security risk management using OCTAVE Allegro method at university. *International Journal of Engineering & Education Research (IJEER)*, 3(4). <https://doi.org/10.46336/ijeer.v3i4.506>
- Dobrynin, I., Radivilova, T., Maltseva, N., & Ageev, D. (2018). Use of approaches to the methodology of factor analysis of information risks for the quantitative assessment of information risks based on the formation of cause-and-effect links. <https://doi.org/10.1109/INFOCOMMST.2018.8632022>
- Central Computer and Telecommunications Agency (CCTA). (2001). *CRAMM User Guide Issue 2.0*. London: CCTA – The Stationery Office. <https://www.scribd.com/document/670786636/CRAMMGuide>
- International Civil Aviation Organization (ICAO). (2018). *Doc 10108: Global Risk Context Statement*. Montreal: ICAO. <https://www.scribd.com/document/688824651/DOC-10108-ICAO-RISK-CONTEXT-STATEMENT>
- International Civil Aviation Organization (ICAO). (2025). *Doc 10213: Global Cyber Risk Considerations (Advance Unedited Edition)*. Montreal: ICAO. <https://www.icao.int/Security/Pages/Cybersecurity.aspx>
- Intel Corporation. (2018). *Threat Assessment & Remediation Analysis (TARA)*. <https://www.intel.com/content/www/us/en/security/threat-assessment-remediation-analysis.html>
- National Agency for Information Systems Security. (2024). *EBIOS Risk Manager – The method (Version 1.5, English edition)*. Paris: ANSSI. Retrieved from https://cyber.gouv.fr/sites/default/files/document/20240901_Guide-EBIOS-RM-V1.5.pdf
- National Institute of Standards and Technology (NIST). (2018). *SP 800-37 Rev.2: Guide for Applying the Risk Management Framework to Federal Information Systems*. Gaithersburg, MD: NIST. <https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final>
- National Institute of Standards and Technology (NIST). (2020). *SP 800-53 Rev.5: Security and Privacy Controls for Information Systems and Organizations*. Gaithersburg, MD: NIST. <https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final>
- Potil, O. V., Horbenko, Yu. I., Zamula, O. A., & Isirova, K. V. (2021). Analysis of methods for assessing and managing cyber and information security risks. *Radiotekhnika*, 206, 5–24. <https://doi.org/10.30837/rt.2021.3.206.01>
- Swan, D. (2019). *Assessing Primary Cyber Threats to an International Airport's Critical Information Systems*. University of Maryland University College. Retrieved from https://www.academia.edu/1460287/Assessing_Primary_Cyber_Threats_to_an_International_Airport_s_Critical_Information_Systems

References

- Aryanti, U., Anwar, M. T., & Rahmawati, T. (2023). Information security risk management using OCTAVE Allegro method at university. *International Journal of Engineering & Education Research (IJEER)*, 3(4). <https://doi.org/10.46336/ijeer.v3i4.506>
- Dobrynin, I., Radivilova, T., Maltseva, N., & Ageev, D. (2018). Use of approaches to the methodology of factor analysis of information risks for the quantitative assessment of information risks based on the formation of cause-and-effect links. <https://doi.org/10.1109/INFOCOMMST.2018.8632022>
- Central Computer and Telecommunications Agency (CCTA). (2001). *CRAMM User Guide Issue 2.0*. London: CCTA – The Stationery Office. <https://www.scribd.com/document/670786636/CRAMMGuide>
- International Civil Aviation Organization (ICAO). (2018). *Doc 10108: Global Risk Context Statement*. Montreal: ICAO. <https://www.scribd.com/document/688824651/DOC-10108-ICAO-RISK-CONTEXT-STATEMENT>
- International Civil Aviation Organization (ICAO). (2025). *Doc 10213: Global Cyber Risk Considerations (Advance Unedited Edition)*. Montreal: ICAO. <https://www.icao.int/Security/Pages/Cybersecurity.aspx>
- Intel Corporation. (2018). *Threat Assessment & Remediation Analysis (TARA)*. <https://www.intel.com/content/www/us/en/security/threat-assessment-remediation-analysis.html>
- National Agency for Information Systems Security. (2024). *EBIOS Risk Manager – The method (Version 1.5, English edition)*. Paris: ANSSI. Retrieved from https://cyber.gouv.fr/sites/default/files/document/20240901_Guide-EBIOS-RM-V1.5.pdf



- National Institute of Standards and Technology (NIST). (2018). *SP 800-37 Rev.2: Guide for Applying the Risk Management Framework to Federal Information Systems*. Gaithersburg, MD: NIST. <https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final>
- National Institute of Standards and Technology (NIST). (2020). *SP 800-53 Rev.5: Security and Privacy Controls for Information Systems and Organizations*. Gaithersburg, MD: NIST. <https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final>
- Potii, O. V., Horbenko, Yu. I., Zamula, O. A., & Isirova, K. V. (2021). Analysis of methods for assessing and managing cyber and information security risks. *Radiotekhnika*, 206, 5–24. <https://doi.org/10.30837/rt.2021.3.206.01>
- Swan, D. (2019). *Assessing Primary Cyber Threats to an International Airport's Critical Information Systems*. University of Maryland University College. Retrieved from https://www.academia.edu/1460287/Assessing_Primary_Cyber_Threats_to_an_International_Airport_s_Critical_Information_Systems.

Отримано редакцією журналу / Received: 09.12.25

Прорецензовано / Revised: 20.12.25

Схвалено до друку / Accepted: 25.12.25

Anna ILIENKO, PhD (Engin.), Assoc. Prof.

ORCID ID: 0000-0001-8565-1117

e-mail: anna.ilienko@npp.kai.edu.ua

State Non-Commercial Company "State University «Kyiv Aviation Institute»", Kyiv, Ukraine

Valentyna TELIUSHCHENKO, PhD Student

ORCID ID: 0000-0001-6026-5105

e-mail: valentyna.teliushchenko@npp.kai.edu.ua

State Non-Commercial Company "State University «Kyiv Aviation Institute»", Kyiv, Ukraine

METHODS FOR ASSESSING THE RISKS OF CYBER THREATS IN INFORMATION AND COMMUNICATION SYSTEMS OF CIVIL AVIATION FACILITIES

Background. Civil aviation is a critical infrastructure, and its ground-based information and communication systems (ICS) – airport operating platforms, integration gateways, networks, and support services – face a diverse landscape of cyber threats. A transparent and reproducible tool aligned with ICAO/EASA/ISO requirements and the operational constraints of airports and air carriers is needed to guide the selection of risk assessment approaches.

Methods. A tuple model of multicriteria analysis (MCA) with linear weighted summation (WSM) is proposed. NIST SP 800-30/CSF, CRAMM, OCTAVE Allegro, EBIOS RM, TARA are taken as alternatives. Criteria: compliance with standards, depth of analysis, flexibility, ease of implementation, cost/resource intensity. The weights are normalized (the sum is 1), the expert estimates are on a scale of 1-5 with an "inverse" interpretation of the cost. The matrix of weighted components, the integral score and its normalized form are calculated. A four-level decision-making scale with three thresholds is introduced. The sensitivity analysis is carried out by means of scenario variation of weights.

Results. The overall ranking confirmed the superiority of NIST SP 800-30/CSF, while EBIOS RM demonstrated a close second. In the security-critical scenario, NIST and CRAMM take the top positions, while in the budget and rapid implementation scenarios, EBIOS RM takes the lead, followed by NIST. OCTAVE Allegro should be considered as a "conditionally recommended" balanced compromise, and TARA as a solution for rapid prioritization with limited resources. In typical operating conditions where cost and efficiency are key, CRAMM is inferior due to its high resource intensity. The results obtained generally remain robust to moderate changes in weights.

Conclusions. The MCA/WSM model provides a transparent, reproducible, and interpretable comparison of risk management frameworks for civil aviation ground-based ICS and can be integrated into decision support systems. The approach combines regulatory compliance with practical feasibility and supports scenario-based selection. Prospects include automating the selection of weights and criteria using AI methods.

Keywords: cybersecurity, civil aviation, ICS, risk assessment, multi-criteria analysis, WSM, frameworks.

Автори заявляють про відсутність конфлікту інтересів. Спонсори не брали участі в розробленні дослідження; у зборі, аналізі чи інтерпретації даних; у написанні рукопису; в рішенні про публікацію результатів.

The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript; in the decision to publish the results.