# ПРОГРАМНО-АЛГОРИТМІЧНА РЕАЛІЗАЦІЯ ІГРОВО-ОПТИМІЗАЦІЙНОГО МЕТОДУ ВИБОРУ ЗАСОБІВ ЗАХИСТУ РОЗПОДІЛЕНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Яскевич Ю.В.
*Київський столичний університет імені Бориса Грінченка, м. Київ*

## ВСТУП

**Актуальність і постановка проблеми.**

Поточний етап розвитку інформаційного суспільства та глобальної цифровізації супроводжується безпрецедентною та глибокою інтеграцією розподілених інформаційних систем (РІС) у критично важливі сфери життєдіяльності держави, корпоративного бізнесу та суспільства загалом. До таких складних екосистем належать корпоративні мережі з багаторівневою архітектурою, глобальні хмарні та гібридні обчислювальні середовища, масштабні системи Інтернету речей (IoT), автоматизовані системи керування технологічними процесами на промислових об'єктах (SCADA/ICS), а також різноманітні децентралізовані фінансові платформи [1; 2]. Фундаментальна специфіка подібних систем апріорі передбачає наявність надзвичайно розвинутої топології, відсутність єдиного центру обробки даних, високий ступінь взаємозалежності вузлів та розмитість або повну відсутність чітко визначеного логічного периметра безпеки. Зазначені архітектурні та функціональні особливості роблять розподілені інформаційні системи не лише пріоритетними мішенями для цілеспрямованих кібератак з боку висококваліфікованих зловмисників, а й надзвичайно складними об’єктами з погляду забезпечення їхнього надійного захисту.

Аналіз сучасних світових тенденцій у сфері кібербезпеки недвозначно свідчить про докорінну зміну парадигми загроз для розподілених систем. Відбувся остаточний перехід від масових, проте доволі хаотичних та нецілеспрямованих атак до складної цілеспрямованої стратегічної протидії, яку часто класифікують як Advanced Persistent Threats (APT). У цьому новому контексті сучасний зловмисник діє як раціональний або обмежено-раціональний суб’єкт, який керується чіткою економічною або політичною мотивацією. Такий нападник ретельно аналізує наявні уразливості системи, оцінює ефективність впроваджених засобів захисту інформації (ЗЗІ) та свідомо обирає оптимальні вектори атаки, що дозволяють максимізувати завдану шкоду за умови мінімізації витрат власних ресурсів.

У таких жорстких умовах традиційні, статичні методи вибору засобів захисту інформації виявляються концептуально та практично неспроможними забезпечити адекватний рівень захищеності. Вони принципово не враховують природної ігрової динаміки конфлікту між нападником і захисником, а також повністю ігнорують каскадні ефекти

поширення кіберінцидентів у гетерогенних мережах. Крім того, в умовах перманентно обмежених фінансових бюджетів перед адміністраторами систем безпеки та особами, які приймають рішення (ОПР), виникла гостра потреба у розв’язанні складної багатокритеріальної оптимізаційної задачі щодо побудови максимально надійного ешелонованого захисту за мінімальних витрат.

**Мета дослідження.**

Метою даного дослідження є розроблення, обґрунтування та детальний опис архітектури програмно-алгоритмічного комплексу, призначеного для автоматизації процесу багатокритеріальної оптимізації та вибору Парето-ефективних конфігурацій засобів захисту розподілених інформаційних систем в умовах баєсівської невизначеності щодо стратегій нападника.

**Аналіз останніх досліджень і публікацій.**

Значному внеску у розв’язання проблем забезпечення кібернетичної безпеки та математичного моделювання процесів захисту присвячено чимало робіт науковців. Проте сучасні підходи (2020–2025 рр.) до вибору засобів захисту мають низку специфічних обмежень.

Зокрема, у роботах [3; 4] застосовано методи дискретної та еволюційної оптимізації для вибору контрзаходів, але проігноровано каскадні ефекти поширення атак у мережі, фокусуючись переважно на локальних вузлах. У дослідженні [5] запропоновано ігрову модель (багатофакторна модель протидії), проте вона має серйозні обмеження щодо масштабованості для великих мереж та складності знаходження рівноваги у розподілених архітектурах. Моделі на основі дерев атак [6] успішно використовують багатокритеріальну оптимізацію, але залишають модель загроз статичною, не враховуючи активну адаптивність нападника. Економічні та ризик-орієнтовані моделі часто розглядають систему агреговано, не деталізуючи структурний вибір конкретних апаратно-програмних засобів.

На відміну від них, запропонований у даному дослідженні підхід системно поєднує структурний топологічний аналіз, ігрову динаміку адаптивного противника та багатокритеріальну оптимізацію. У попередній роботі автора [7] було запропоновано базову теоретичну ігрово-оптимізаційну модель, проте її програмна реалізація, специфікація параметрів та формалізований алгоритм дій для ОПР залишалися нерозкритими. Дане дослідження заповнює цю прогалину, перетворюючи теоретичний концепт на практичний інструментарій підтримки прийняття рішень (СППР).

**Короткий опис дослідження, його методів і засобів**

Для розв'язання поставленої оптимізаційної задачі було спроєктовано та створено спеціалізований програмний продукт мовою Python (версія 3.10). Архітектура програмного комплексу побудована за

модульним принципом і складається з трьох ключових блоків: генерації топології, симуляції баєсівської гри та еволюційної оптимізації на основі алгоритму NSGA-II.

Перший функціональний модуль відповідає за автоматизовану генерацію топології РІС та параметризацію уразливостей. В експериментах РІС моделювалася як масштабно-вільна мережа з конфігурацією із 30 вузлів та 56 інформаційних зв'язків зі щільністю графа 0,129, що найкраще відображає наявність комунікаційних хабів у реальних інфраструктурах. Критичність вузла $C_i$ задається в діапазоні від 1 до 10 залежно від його функціональної ролі (наприклад, сервери баз даних мають найвищий пріоритет, периферійні IoT-пристрої — найнижчий). Базова уразливість $V_i$ генерується як випадкова величина, розподілена згідно зі статистикою баз оцінок CVSS (Common Vulnerability Scoring System) за останній рік.

Другий функціональний модуль забезпечує симуляцію ігрової взаємодії. У ньому реалізовано баєсівську гру з трьома типами гравців (нападників): $\theta_1$ (APT-угруповання), $\theta_2$ (опортуніст), $\theta_3$ (інсайдер). Апріорний розподіл типів $P(\theta) = [0.2, 0.5, 0.3]$ задається на основі даних Threat Intelligence. Функція корисності нападника в умовах неповної інформації формалізується як $U^{att}(z, a) = -L(z, a)$ , де загальні втрати системи $L(z, a)$ розраховуються як зважена сума локальних втрат з урахуванням коефіцієнтів критичності вузлів $\omega_v$. Критичною інновацією цього модуля є використання граф-моделі для розрахунку мережевого каскадного ефекту: шкода від зламу периферійного пристрою екстраполюється на суміжні критичні вузли через коефіцієнти латерального поширення $a_{u,v}$.

Третій функціональний модуль автоматизує процес пошуку найкращих конфігурацій ЗЗІ за допомогою генетичного алгоритму NSGA-II, оперуючи конфліктними критеріями: мінімізацією фінансових витрат, максимізацією покриття та мінімізацією інтегрального ризику (очікуваних втрат). Хромосоми (конфігурації захисту) піддаються процедурі недомінованого сортування (non-dominated sorting) та турнірній селекції, утворюючи фронт Парето-оптимальних рішень для особи, яка приймає рішення.

Практична імплементація методу для ОПР (CISO) формалізована у вигляді чіткого 11-етапного алгоритму: від формалізації топологічної структури РІС (Етап 1), оцінювання критичності (Етап 2) та задання бюджетних обмежень (Етап 4) до моделювання баєсівської поведінки зловмисника (Етап 5), запуску NSGA-II (Етап 9) та фінального вибору компромісного рішення з візуалізованого Парето-фронту (Етап 11).

**РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ**

Експериментальна перевірка працездатності комплексу здійснювалася шляхом серії масштабних обчислювальних симуляцій. Для кожної досліджуваної конфігурації та топології проводилося

50 незалежних запусків стохастичного алгоритму NSGA-II. Наведені нижче результати відображають середні значення показників. При цьому стандартне відхилення не перевищувало ± 0,02, що підтверджує високу статистичну значущість та стабільність отриманих розв'язків.

Головним критерієм оцінювання виступав інтегральний ризик *R*, нормований до діапазону від 0 до 1. Він обчислюється як середньозважена сума очікуваних втрат за всіма баєсівськими сценаріями атак, поділена на максимальні потенційні втрати (теоретичний стан системи без жодного захисту).

Завдяки програмному комплексу для кожної мережі генерувалася множина з 10–13 Парето-оптимальних конфігурацій ЗЗІ. На екстремальному полюсі максимальної безпеки (стратегія з максимальною вартістю захисту) інтегральний ризик знижується до мінімального значення 0,229. Водночас середній інтегральний ризик при оптимальному збалансованому розподілі ресурсів становить 0,42–0,43. На протилежному полюсі розташовані економічно орієнтовані стратегії, які дозволяють суттєво заощадити фінансові ресурси організації, забезпечуючи при цьому покриття критичних активів на рівні до 82%.

Порівняльний аналіз із типовими евристичними стратегіями («Criticality First» та «Vulnerability First») статистично підтвердив перевагу запропонованого ігрово-оптимізаційного методу (Таблиця 1).

Таблиця 1

Порівняльна характеристика ефективності стратегій захисту РІС

| **Показник оцінювання** | **Базові евристичні стратегії** | **Ігрово-оптимізаційний метод (NSGA-II)** | **Відносний приріст ефективності** |
|---|---|---|---|
| Рівень зниження інтегрального ризику | 48 – 55 % | 56 – 58 % (± 1.2%) | + 12 – 18 % |
| Досягнутий мінімум ризику (*R*) | Не менше 0,35 | До 0,23 (± 0.01) | Суттєве покращення |
| Показник ефективності витрат (зниження ризику на 1000 ум. од. бюджету) | 0,10 | 0,15 | + 50 % |
| Покриття критичних активів в умовах обмеженого бюджету | 60 – 70 % | До 82 % | + 12 – 22 % |
| Стійкість до баєсівської невизначеності типу нападника | Низька (статична модель) | Висока (мінімаксне оцінювання) | Концептуальна перевага |

Цей економічний феномен (показник ефективності інвестицій 0,15 проти 0,10) має фундаментальне практичне значення. Завдяки математично обґрунтованому розподілу засобів захисту з урахуванням каскадних ефектів, організація здатна отримати вищий рівень захищеності без збільшення загального фінансового бюджету на кібербезпеку, оскільки кошти спрямовуються на перекриття найбільш критичних ігрових сценаріїв, ігноруючи економічно невигідні для нападника вектори.

**ВИСНОВКИ**

1. Розроблено та програмно реалізовано мовою Python архітектуру системи підтримки прийняття рішень для CISO, яка повністю автоматизує багатокритеріальну оптимізацію засобів захисту для розподілених інформаційних систем. Працездатність та ефективність комплексу експериментально підтверджено на прикладі масштабно-вільної мережі модель Барабаші-Альберт із 30 вузлів, де для ініціалізації вразливостей використано актуальні CVSS-метрики.
2. Вперше деталізовано формалізовану баєсівську гру (Ua) з урахуванням апріорних ймовірностей різних типів порушників (APT, інсайдер, опортуніст), що дозволило відійти від статичних моделей загроз та оцінювати стійкість захисту в умовах стратегічної невизначеності.
3. Формалізовано 11-етапний алгоритм дій для особи, яка приймає рішення, що інтегрує еволюційний алгоритм NSGA-II у практичний бізнес-процес управління кібербезпекою.
4. Доведено на основі 50 незалежних запусків симуляції, що запропонований ігрово-оптимізаційний метод у середньому знижує інтегральний ризик PIC до рівня 0,42–0,43 (з досягненням абсолютного мінімуму 0,229 на полюсі максимальної безпеки). Кількісна оцінка розриву в ефективності засвідчила, що оптимізаційні заходи перевершують найкращі традиційні евристичні підходи («Criticality First» та «Cost-effective») на 12–18%.

**ДЖЕРЕЛА**

1. Додонов О. Г., Никифоров О. В., Путятін В. Г. та ін. Територіально-розподілені інформаційні комп’ютерні системи у єдиному інформаційному просторі: базові поняття та визначення. Реєстрація, зберігання і обробка даних. 2024. Т. 26, № 1. С. 89–112.

2. Palko D., Babenko T., Bigdan A. et al. Cyber security risk modeling in distributed information systems. Applied Sciences. 2023. Vol. 13, No. 4. P. 2393.

3. Пшеничних С. В., Добринін І. С., Клочкова Д. Ю. Математична модель оптимального вибору засобів захисту інформації при проектуванні комплексної системи захисту на об’єкті інформатизації. Проблеми телекомунікацій. 2023. № 1 (32). С. 45–58. https://doi.org/10.30837/pt.2023.1.04

4. Лахно, В., Криворучко, О., & Каламан, Є. (2025). Програмна реалізація вирішення задачі оптимізації вибору засобів захисту інформації на основі еволюційного алгоритму. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, *3*(27), 257–268. https://doi.org/10.28925/2663-4023.2025.27.751

5. Lakhno, Valerii & Malyukov, Volodimir & Oleksii, Smirnov & Bebeshko, Bohdan & Chubaievskiy, V. & Zhumadilova, Meiramgul & Malyukova, I. & Smirnov, S.. (2024). Multifactorial Model for Targeted Attacks Counteracting Within the Framework of a Multi-Step Quality Game with Fuzzy Information. 10.1007/978-981-97-2147-4_2

6. Dewri, Rinku & Poolsappasit, Nayot & Ray, Indrajit & Whitley, Darrell. (2007). Optimal security hardening using multi-objective optimization on attack tree models of networks. 204-213. 10.1145/1315245.1315272.

7. Яскевич, Ю. (2025). Ігрово-оптимізаційна модель вибору засобів захисту розподілених інформаційних систем. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, *2*(30), 715–726. https://doi.org/10.28925/2663-4023.2025.30.913

8. Abramov, V., Astafieva, M., Boiko, M., Bodnenko, D., Bushma, A., Vember, V., Hlushak, O., Zhyltsov, O., Ilich, L., Kobets, N., Kovaliuk, T., Kuchakovska, H., Lytvyn, O., Lytvyn, P., Mashkina, I., Morze, N., Nosenko, T., Proshkin, V., Radchenko, S., & Yaskevych, V. (2021). Theoretical and practical aspects of the use of mathematical methods and information technology in education and science. https://doi.org/10.28925/9720213284km