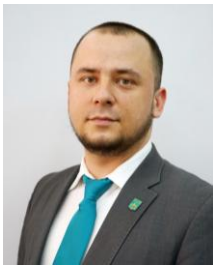
© Skladannyi P., Kostiuk Y., Korshun N., Rzaeva S., Sokolov V. Method for Optimizing Cybersecurity Strategies in Distributed Information Systems Based on NSGA-II Multi-Objective Optimization and Game Theory// *Ukrainian Scientific Journal of Information Security, 2026, vol. 32, issue 2, pp. 6-22. © This is an open access article under the CC BY 4.0 International license.*

**DOI: 10.18372/2225-5036.32.21651**

# МЕТОД ОПТИМІЗАЦІЇ СТРАТЕГІЙ КІБЕРЗАХИСТУ В РОЗПОДІЛЕНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ НА ОСНОВІ БАГАТОКРИТЕРІАЛЬНОЇ ОПТИМІЗАЦІЇ NSGA-II ТА ТЕОРІЇ ІГОР

**Павло Складанний, Юлія Костюк, Наталія Коршун, Світлана Рзаєва, Володимир Соколов**

*Київський столичний університет імені Бориса Грінченка, м. Київ, Україна*



**СКЛАДАННИЙ Павло Миколайович,** кандидат технічних наук, доцент,
*Рік та місце народження:* 1992 рік, м. Київ, Україна
*Освіта:* Державний університет телекомунікацій.
*Посада:* завідувач кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
*Наукові інтереси:* кібербезпека, криптографія, криптоаналіз, математичне моделювання.
*Публікації:* більше 100 наукових публікацій, серед яких монографії, підручники, посібники, наукові статті та тези, матеріали доповідей на конференціях.
*E-mail:* p.skladannyi@kubg.edu.ua
*Orcid ID:* 0000-0002-7775-6039.



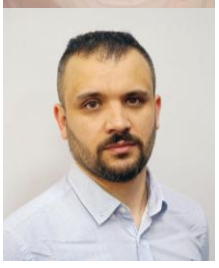
**КОСТЮК Юлія Володимирівна,** Phd in Computer Science
*Рік та місце народження:* 1980 рік, м. Київ, Україна
*Освіта:* Державний торговельно-економічний університет.
*Посада:* доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
*Наукові інтереси:* захист інформації, комп'ютерні мережі, інформаційно-комунікаційні системи, інформаційно-інтелектуальні системи, нейронні мережі.
*Публікації:* більше 100 наукових публікацій, серед яких монографія, посібник, наукові статті та тези, матеріали доповідей на конференціях.
*E-mail:* y.kostiuk@kubg.edu.ua
*Orcid ID:* 0000-0001-5423-0985.



**КОРШУН Наталія Володимирівна,** доктор технічних наук, професор
*Рік та місце народження:* 1983 рік, м. Чернігів, Україна
*Освіта:* Державний університет інформаційно-комунікаційних технологій
*Посада:* професор кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
*Наукові інтереси:* захист інформації, комп'ютерні мережі, інформаційно-комунікаційні системи, інформаційно-інтелектуальні системи, нейронні мережі.
*Публікації:* більше 150 наукових публікацій, серед яких монографія, посібник, наукові статті та тези, матеріали доповідей на конференціях.
*E-mail:* n.korshun@kubg.edu.ua
*Orcid ID:* 0000-0003-2908-970X



**РЗАЄВА Світлана Леонідівна**, кандидат технічних наук, доцент.
*Рік та місце народження:* 1968 рік, м. Київ, Україна.
*Освіта:* Севастопольський приладобудівний інститут.
*Посада:* доцент кафедри комп'ютерних наук.
*Наукові інтереси:* адміністрування і захист баз даних та сховищ даних, моделювання програмного забезпечення та його аналіз, інформаційні технології та системи.
*Публікації:* більше 100 наукових публікацій, серед яких монографії, підручники, посібники, наукові статті та тези, матеріали доповідей на конференціях.
*E-mail:* s.rzaieva@kubg.edu.ua
*Orcid ID:* 0000-0002-7589-2045



**СОКОЛОВ Володимир Юрійович**, кандидат технічних наук, доцент,
*Рік та місце народження:* 1982 рік, м. Миколаїв, Україна
*Освіта:* Національний технічний університет України "КПІ імені Ігоря Сікорського".
*Посада:* доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
*Наукові інтереси:* кібербезпека, безпроводові технології, криптографія, соціальна інженерія.
*Публікації:* більше 100 наукових публікацій, серед яких монографії, підручники, посібники, наукові статті та тези, матеріали доповідей на конференціях, патент.
*E-mail:* v.sokolov@kubg.edu.ua
*Orcid ID:* 0000-0002-9349-7946

© Skladannyi P., Kostiuk Y., Korshun N., Rzaeva S., Sokolov V. Method for Optimizing Cybersecurity Strategies in Distributed Information Systems Based on NSGA-II Multi-Objective Optimization and Game Theory// Ukrainian Scientific Journal of Information Security, 2026, vol. 32, issue 2, pp. 6-22. © This is an open access article under the CC BY 4.0 International license.

***Анотація***. *У статті розроблено метод оптимізації стратегій кіберзахисту в розподілених інформаційних системах на основі багатокритеріальної оптимізації NSGA-II та теорії ігор. Актуальність дослідження зумовлена зростанням кількості кіберзагроз, ускладненням архітектури розподілених інформаційних систем, збільшенням обсягів оброблюваних даних та необхідністю підвищення ефективності прийняття рішень щодо формування стратегій кіберзахисту в умовах обмежених ресурсів і динамічної зміни параметрів кіберсередовища. У роботі проведено аналіз сучасних підходів до забезпечення кібербезпеки розподілених інформаційних систем, методів оцінювання ризиків, багатокритеріальної оптимізації та застосування теорії ігор у задачах стратегічного планування кіберзахисту. Встановлено, що існуючі підходи недостатньо враховують одночасний вплив рівня ризику, вартості впровадження механізмів захисту, ефективності засобів кіберзахисту та можливої поведінки порушника під час формування оптимальних стратегій. Запропоновано математичну модель оптимізації стратегій кіберзахисту, яка поєднує багатокритеріальне оцінювання альтернатив із використанням алгоритму NSGA-II та ігрову модель стратегічної взаємодії між системою кіберзахисту і порушником. Розроблено систему критеріїв оптимізації, що враховує рівень ризику, витрати на реалізацію захисних заходів, рівень захищеності інформаційних ресурсів і час реагування на кіберінциденти. Запропоновано архітектуру системи підтримки прийняття рішень, алгоритм функціонування методу та процедуру формування множини Парето-оптимальних стратегій. Проведено обчислювальний експеримент для різних сценаріїв функціонування розподіленої інформаційної системи. Результати моделювання показали зниження інтегрального рівня ризику, підвищення ефективності стратегій кіберзахисту, покращення адаптивності системи до зміни умов функціонування та переваги над традиційними підходами. Отримані результати підтвердили доцільність використання поєднання багатокритеріальної оптимізації NSGA-II та теорії ігор для підтримки прийняття рішень у сфері кібербезпеки.*

***Ключові слова:*** *розподілені інформаційні системи; кібербезпека; стратегія кіберзахисту; багатокритеріальна оптимізація; NSGA-II; теорія ігор; оцінювання ризиків; система підтримки прийняття рішень; обчислювальний експеримент; інтелектуальні методи.*

## Вступ

Сучасний розвиток цифрових технологій, хмарних обчислень, інтернету речей та розподілених інформаційних систем супроводжується зростанням кількості кіберзагроз, спрямованих на порушення конфіденційності, цілісності та доступності інформаційних ресурсів [1, 14]. Розподілені інформаційні системи характеризуються складною структурою, великою кількістю взаємопов'язаних компонентів та високою динамікою функціонування [7, 17]. За таких умов забезпечення належного рівня кібербезпеки потребує формування ефективних стратегій кіберзахисту, здатних адаптуватися до зміни параметрів кіберсередовища, інтенсивності атак і поведінки порушника [2, 10].

Однією з ключових проблем сучасної кібербезпеки є вибір раціональної стратегії захисту в умовах багатокритеріальності та невизначеності [2, 8, 14]. Під час прийняття рішень необхідно одночасно враховувати рівень ризику, витрати на реалізацію захисних заходів, ефективність механізмів захисту та можливі дії атакувальної сторони [25]. Традиційні підходи переважно ґрунтуються на експертних оцінках або статичних моделях ризику, що обмежує їх адаптивність і знижує ефективність у динамічних умовах [2, 18].

Перспективним напрямом розв'язання цієї проблеми є застосування методів багатокритеріальної оптимізації та теорії ігор [4, 28]. Одним із найбільш відомих алгоритмів багатокритеріальної оптимізації є NSGA-II (Non-dominated Sorting Genetic Algorithm II генетичний алгоритм сортування за недомінуванням другого покоління), який дозволяє знаходити множину Парето-оптимальних рішень за декількома суперечливими критеріями одночасно [3-5, 30]. У задачах кіберзахисту такий підхід дає можливість одночасно враховувати рівень ризику, витрати на реалізацію захисних заходів, ефективність захисту та інші критерії прийняття рішень. Теорія ігор, у свою чергу, забезпечує формалізацію взаємодії між системою кіберзахисту та порушником [12, 19, 29]. Поєднання цих підходів створює підґрунтя для побудови адаптивних методів підтримки прийняття рішень у сфері кібербезпеки.

Наукова новизна роботи полягає у розробленні методу оптимізації стратегій кіберзахисту в розподілених інформаційних системах, який інтегрує багатокритеріальну оптимізацію NSGA-II та теорію ігор для формування множини Парето-оптимальних стратегій захисту з урахуванням рівня ризику, витрат на реалізацію заходів безпеки, ефективності захисту та можливої поведінки порушника. На відміну від існуючих підходів, запропонований метод дозволяє одночасно враховувати технічні, економічні та ризикові аспекти кіберзахисту.

Теоретичне значення дослідження полягає у розвитку моделей підтримки прийняття рішень у сфері кібербезпеки, удосконаленні підходів до багатокритеріальної оптимізації стратегій захисту та розвитку методів застосування теорії ігор для аналізу взаємодії між системою кіберзахисту і порушником.

Практичне значення роботи полягає у можливості використання запропонованого методу для формування стратегій кіберзахисту в корпоративних інформаційних системах, телекомунікаційних мережах, хмарних середовищах та інших розподілених інформаційних системах [13, 15, 22]. Використання методу дозволяє знизити рівень кіберризиків, підвищити ефективність використання ресурсів безпеки, скоротити час прийняття рішень та забезпечити адаптацію системи кіберзахисту до зміни умов функціонування і появи нових кіберзагроз [6, 16].

## Постановка проблеми

Сучасні розподілені інформаційні системи є основою функціонування корпоративних мереж, хмарних платформ, центрів обробки даних та

цифрових сервісів [13, 17]. Їх характерними особливостями є розподілене оброблення даних, велика кількість взаємопов'язаних компонентів і висока динаміка функціонування [7, 23, 27]. Одночасно зі зростанням складності таких систем збільшується кількість кіберзагроз, що підвищує вимоги до ефективності механізмів кіберзахисту.

Однією з ключових задач забезпечення кібербезпеки є формування раціональних стратегій кіберзахисту, які повинні забезпечувати належний рівень захищеності інформаційних ресурсів за умов обмежених ресурсів [25]. Під час вибору стратегії необхідно враховувати рівень кіберризику, ефективність захисних механізмів, вартість їх впровадження, вплив на продуктивність системи та можливу поведінку порушника.

Існуючі підходи переважно базуються на експертних оцінках або статичних моделях ризику, що не забезпечують комплексного врахування множини критеріїв та стратегічної взаємодії між системою кіберзахисту і порушником [2, 18, 21]. Крім того, більшість наявних моделей орієнтовані на вибір окремих засобів захисту, а не на оптимізацію цілісної стратегії кіберзахисту.

У зв'язку з цим виникає необхідність розроблення методу оптимізації стратегій кіберзахисту в розподілених інформаційних системах, який забезпечував би одночасне врахування рівня ризику, ресурсних обмежень, ефективності захисту та можливої поведінки порушника. Перспективним напрямом розв'язання цієї проблеми є поєднання багатокритеріальної оптимізації NSGA-II та теорії ігор, що дозволяє формувати множину Парето-оптимальних стратегій кіберзахисту та обирати найбільш раціональні рішення в умовах кіберпротиборства.

Отже, актуальним науковим завданням є розроблення методу оптимізації стратегій кіберзахисту в розподілених інформаційних системах на основі багатокритеріальної оптимізації NSGA-II та теорії ігор для підвищення ефективності прийняття рішень і зниження рівня кіберризиків.

**Аналіз останніх досліджень і публікацій**

Проблема оптимізації стратегій кіберзахисту в розподілених інформаційних системах привертає значну увагу дослідників у зв'язку зі зростанням складності кіберзагроз, необхідністю врахування невизначеності параметрів кіберсередовища та потребою прийняття рішень за множиною суперечливих критеріїв. Сучасні дослідження охоплюють питання застосування теорії ігор, багатокритеріальної оптимізації, оцінювання ризиків та інтелектуальних систем підтримки прийняття рішень у сфері кібербезпеки.

У роботі Abdallah et al. [1] розглянуто фундаментальні аспекти застосування теорії ігор для забезпечення безпеки розподілених систем. Автори проаналізували основні типи ігрових моделей, що використовуються для моделювання взаємодії між захисником і порушником, визначили сучасні виклики та перспективні напрями розвитку цього підходу. Дослідження підтверджує ефективність теорії ігор для аналізу стратегічної поведінки сторін, однак не розглядає питання багатокритеріальної оптимізації стратегій кіберзахисту.

У дослідженні Zhang і Malacaria [2] запропоновано підхід до підтримки прийняття рішень у сфері кібербезпеки в умовах невизначеності. Автори використовують ймовірнісні графи атак та ризик-орієнтовані моделі для оцінювання можливих сценаріїв розвитку кіберінцидентів. Запропонований підхід підвищує обґрунтованість прийняття рішень, проте не враховує оптимізацію стратегій кіберзахисту за множиною критеріїв.

Значна кількість сучасних досліджень присвячена розвитку алгоритмів багатокритеріальної оптимізації. Так, Ma та Liu [3] запропонували вдосконалену модифікацію алгоритму NSGA-II (Non-dominated Sorting Genetic Algorithm II), яка забезпечує більш ефективний пошук Парето-оптимальних рішень у задачах багатокритеріальної оптимізації. Отримані результати підтвердили високу ефективність алгоритму, однак дослідження орієнтоване на технічні задачі проєктування і не враховує специфіку кібербезпеки.

У роботі Zhao et al. [4] розроблено адаптивний багатопопуляційний алгоритм багатокритеріальної оптимізації, який дозволяє підвищити якість пошуку недомінованих рішень у складних задачах оптимізації. Автори продемонстрували переваги адаптивного керування параметрами алгоритму, проте питання стратегічного вибору засобів і механізмів кіберзахисту не розглядалися.

Дослідження Miyandoab, Rahnamayan та Bidgoli [5] присвячене компактній реалізації NSGA-II для задач багатокритеріального відбору ознак. Автори підтвердили можливість ефективного використання алгоритму в умовах обмежених обчислювальних ресурсів. Водночас запропонований підхід не враховує ризики кіберзагроз та поведінку потенційного порушника.

У роботі Yue et al. [6] запропоновано метод реагування на кіберінциденти в промислових системах керування на основі багатокритеріальної оптимізації та глибоких Q-мереж. Автори показали, що поєднання оптимізаційних методів із інтелектуальними механізмами підтримки прийняття рішень дозволяє підвищити ефективність реагування на атаки. Однак дослідження зосереджене на етапі реагування на інциденти та не розв'язує задачу формування оптимальної стратегії кіберзахисту на етапі планування.

У праці Stark, Frost та Nebel-Wenner [7] розглянуто проблему розподіленої багатокритеріальної оптимізації в кіберфізичних

© Skladannyi P., Kostiuk Y., Korshun N., Rzaeva S., Sokolov V. Method for Optimizing Cybersecurity Strategies in Distributed Information Systems Based on NSGA-II Multi-Objective Optimization and Game Theory// Ukrainian Scientific Journal of Information Security, 2026, vol. 32, issue 2, pp. 6-22. © This is an open access article under the CC BY 4.0 International license.

енергетичних системах. Автори дослідили особливості прийняття рішень у розподілених середовищах та продемонстрували переваги багатокритеріального підходу для узгодження конфліктних цілей. Разом із тим питання оцінювання кіберризиків і стратегічної взаємодії між захисником та порушником залишилися поза межами дослідження.

Проведений аналіз показав, що існуючі дослідження окремо розглядають застосування теорії ігор у кібербезпеці [1], підтримку прийняття рішень в умовах невизначеності [2], удосконалення алгоритмів NSGA-II [3–5], багатокритеріальне реагування на кіберінциденти [6] та розподілену багатокритеріальну оптимізацію [7]. Водночас недостатньо дослідженим залишається питання розроблення методу оптимізації стратегій кіберзахисту в розподілених інформаційних системах, який поєднує оцінювання кіберризиків, багатокритеріальну оптимізацію NSGA-II та теорію ігор у межах єдиної моделі підтримки прийняття рішень. Саме розв'язанню цієї невирішеної частини загальної проблеми присвячене дане дослідження.

**Мета та завдання статті**

Метою статті є розробка методу оптимізації стратегій кіберзахисту в розподілених інформаційних системах на основі багатокритеріальної оптимізації NSGA-II та теорії ігор, який забезпечує формування множини Парето-оптимальних стратегій захисту з урахуванням рівня кіберризику, витрат на реалізацію заходів безпеки, ефективності захисних механізмів і можливої поведінки порушника, а також підвищення ефективності прийняття рішень у сфері кібербезпеки в умовах динамічної зміни параметрів кіберсередовища.

Для досягнення поставленої мети у роботі необхідно вирішити такі завдання:

– провести аналіз сучасних підходів до формування стратегій кіберзахисту в розподілених інформаційних системах, методів багатокритеріальної оптимізації та теорії ігор;

– дослідити особливості застосування алгоритму NSGA-II для розв'язання задач багатокритеріальної оптимізації стратегій кіберзахисту;

– розробити математичну модель оптимізації стратегій кіберзахисту з урахуванням рівня кіберризику, ефективності захисних механізмів, витрат на реалізацію заходів безпеки та можливої поведінки порушника;

– побудувати ігрову модель стратегічної взаємодії між системою кіберзахисту та порушником;

– розробити метод оптимізації стратегій кіберзахисту на основі поєднання багатокритеріальної оптимізації NSGA-II та теорії ігор;

– розробити архітектуру системи підтримки прийняття рішень для реалізації запропонованого методу;

– провести обчислювальний експеримент для оцінювання ефективності запропонованого методу в різних сценаріях функціонування розподіленої інформаційної системи;

– виконати порівняльний аналіз отриманих результатів та оцінити ефективність запропонованого методу за показниками рівня ризику, ефективності кіберзахисту та якості прийняття рішень.

**Результати дослідження**

Для розроблення методу оптимізації стратегій кіберзахисту в розподілених інформаційних системах необхідно формалізувати процес прийняття рішень щодо вибору захисних заходів з урахуванням рівня кіберризику, ефективності засобів захисту, витрат на їх реалізацію та можливої поведінки порушника [14, 25]. Запропонований метод базується на поєднанні математичних моделей оцінювання ризику, багатокритеріальної оптимізації NSGA-II та теорії ігор, що дозволяє формувати множину Парето-оптимальних стратегій кіберзахисту в умовах невизначеності та динамічної зміни кіберзагроз [35]. Врахування невизначеності є одним із ключових напрямів розвитку сучасних багатокритеріальних оптимізаційних моделей підтримки прийняття рішень. Для реалізації зазначеного підходу виконано формалізацію задачі оптимізації, розроблено модель оцінювання ризику, багатокритеріальну модель вибору стратегій та ігрову модель взаємодії між системою кіберзахисту і порушником.

**Формалізація задачі оптимізації стратегій кіберзахисту**

Розподілена інформаційна система складається з множини інформаційних ресурсів, мережевих вузлів, сервісів, каналів передавання даних та засобів кіберзахисту, які функціонують у динамічному кіберсередовищі [1, 17-18]. У таких системах необхідно забезпечити ефективний кіберзахист за умов обмежених ресурсів, мінімізуючи ризики реалізації кіберзагроз і витрати на захисні механізми [22, 30]. Тому задачу формування стратегії кіберзахисту доцільно розглядати як задачу багатокритеріальної оптимізації.

Множину можливих стратегій кіберзахисту визначимо як:

$$S = \{s_1, s_2, \dots, s_n\}, \quad (1)$$

де $S$ – множина допустимих стратегій кіберзахисту, $s_i$ – окрема стратегія захисту, $n$ – кількість альтернативних стратегій. Кожна стратегія являє собою певну комбінацію засобів захисту, правил реагування на кіберінциденти та параметрів налаштування системи безпеки.

Для формалізації властивостей кожної стратегії введемо вектор її параметрів:

$$s_i = (R_i, C_i, E_i, T_i), \quad (2)$$

де $R_i$ – рівень кіберризику при використанні стратегії $s_i$, $C_i$ – витрати на реалізацію та підтримку стратегії, $E_i$ – ефективність захисту, $T_i$ – середній час реагування на кіберінциденти. Запропонована модель дозволяє одночасно враховувати безпекові, економічні та часові характеристики функціонування системи кіберзахисту.

Для оцінювання альтернативних стратегій сформуємо вектор критеріїв оптимізації:

$$F(s_i) = (R_i, C_i, -E_i, T_i), \quad (3)$$

де ризик $R_i$, витрати $C_i$ та час реагування $T_i$ підлягають мінімізації, а ефективність захисту $E_i$ – максимізації. Для забезпечення єдиного напрямку оптимізації використовується величина $-E_i$.

Задача оптимізації полягає у знаходженні множини Парето-оптимальних стратегій:

$$S^* = \{s_i \in S \mid \nexists s_j : s_j \prec s_i\}, \quad (4)$$

де $S^*$ – множина Парето-оптимальних стратегій; символ $s_j \prec s_i$ означає, що стратегія $s_j$ домінує стратегію $s_i$ хоча б за одним критерієм без погіршення інших критеріїв.

Таким чином, задача вибору стратегії кіберзахисту зводиться до пошуку множини недомінованих рішень, які забезпечують найкращий компроміс між рівнем ризику, витратами, ефективністю захисту та швидкістю реагування на кіберінциденти. Отримана математична постановка є основою для подальшого застосування алгоритму NSGA-II та побудови ігрової моделі взаємодії між системою кіберзахисту і порушником.

**Математична модель оцінювання ризику**

Одним із ключових етапів формування стратегії кіберзахисту є оцінювання рівня ризику функціонування розподіленої інформаційної системи [14, 18, 22]. Саме величина ризику визначає необхідність застосування додаткових захисних механізмів, впливає на вибір оптимальної стратегії кіберзахисту та використовується як один із критеріїв багатокритеріальної оптимізації. Для побудови методу запропоновано математичну модель оцінювання ризику, яка враховує імовірність реалізації кіберзагроз, критичність інформаційних ресурсів та поточний рівень кіберзагроз.

Ризик для окремого інформаційного ресурсу визначається як:

$$R_j = P_j \cdot V_j \cdot I_j, \quad (5)$$

де $R_j$ – ризик для j-го інформаційного ресурсу, $P_j$ – імовірність реалізації кіберзагрози, $V_j$ – рівень вразливості ресурсу, $I_j$ – коефіцієнт критичності ресурсу. Запропонована залежність відображає класичний ризик-орієнтований підхід, відповідно до якого ризик зростає зі збільшенням імовірності атаки, рівня вразливості та важливості інформаційного ресурсу для функціонування системи. Найбільші значення ризику отримують критично важливі активи, які мають високий рівень вразливості та перебувають під впливом актуальних кіберзагроз.

Оскільки розподілена інформаційна система складається з множини взаємопов'язаних ресурсів, для оцінювання загального рівня ризику необхідно врахувати внесок кожного компонента системи. Інтегральний ризик визначається виразом:

$$R_{sys} = \sum_{j=1}^{m} w_j R_j, \quad (6)$$

де $R_{sys}$ – інтегральний ризик розподіленої інформаційної системи, $w_j$ – ваговий коефіцієнт значущості j-го ресурсу, $m$ – кількість інформаційних ресурсів у системі. Вагові коефіцієнти дозволяють врахувати різний вплив окремих компонентів на функціонування системи. Наприклад, компрометація центрального сервера або бази даних може призвести до значно більших наслідків, ніж порушення роботи окремої робочої станції, тому відповідні значення $w_j$ будуть суттєво відрізнятися.

Для врахування поточного стану кіберсередовища вводиться коефіцієнт інтенсивності кіберзагроз:

$$K_{th} = \frac{N_{att}}{N_{max}}, \quad (7)$$

де $K_{th}$ – коефіцієнт поточного рівня кіберзагроз, $N_{att}$ кількість зареєстрованих кібератак за визначений інтервал часу, $N_{max}$ – максимально допустима кількість атак, встановлена відповідно до вимог безпеки. Коефіцієнт $K_{th}$ дозволяє оцінити поточну активність порушника та адаптувати процес вибору стратегії кіберзахисту до реального стану кіберсередовища. Якщо значення $K_{th}$ наближається до одиниці, це свідчить про високий рівень загроз та необхідність переходу до більш захищених стратегій кіберзахисту. У разі зменшення інтенсивності атак система може обирати менш ресурсоємні стратегії захисту, зберігаючи прийнятний рівень безпеки.

Таким чином, запропонована математична модель оцінювання ризику дозволяє комплексно враховувати характеристики інформаційних ресурсів, їх критичність та поточний рівень кіберзагроз. Отримані значення інтегрального ризику надалі використовуються як один із ключових критеріїв у задачі багатокритеріальної оптимізації стратегій кіберзахисту на основі алгоритму NSGA-II.

**Багатокритеріальна модель оптимізації NSGA-II**

Формування ефективної стратегії кіберзахисту в розподілених інформаційних системах характеризується необхідністю одночасного врахування декількох суперечливих критеріїв [16, 21]. Подібні підходи до багатокритеріального прийняття рішень у задачах кіберзахисту активно розвиваються в

сучасних дослідженнях [33]. З одного боку, необхідно мінімізувати рівень кіберризику та час реагування на інциденти безпеки, а з іншого — обмежувати витрати на впровадження та підтримку захисних механізмів [17, 22]. Тому для пошуку оптимальних стратегій доцільно використовувати алгоритм NSGA-II (Non-dominated Sorting Genetic Algorithm II), який дозволяє формувати множину Парето-оптимальних рішень за декількома критеріями одночасно [16, 30].

Першою цільовою функцією є мінімізація інтегрального ризику функціонування системи:

$$f_1 = R_{sys}\ , \tag{8}$$

де $f_1$- критерій мінімізації ризику, $R_{sys}$ –інтегральний ризик розподіленої інформаційної системи, визначений відповідно до формули (6). Мінімізація цього критерію спрямована на зменшення ймовірності успішної реалізації кіберзагроз та зниження можливих збитків від кіберінцидентів. Зменшення значення $R_{sys}$ свідчить про підвищення загального рівня захищеності системи.

Другим критерієм є мінімізація сукупних витрат на реалізацію стратегії кіберзахисту:

$$f_2 = C_{tot}\ , \tag{9}$$

де $C_{tot}$ – загальні витрати на впровадження, налаштування, супроводження та модернізацію засобів кіберзахисту. Запропонований критерій дозволяє враховувати економічні обмеження підприємства або організації. Надмірне підвищення рівня безпеки може потребувати значних фінансових витрат, тому оптимальна стратегія повинна забезпечувати баланс між безпекою та вартістю її досягнення.

Третя цільова функція спрямована на максимізацію ефективності кіберзахисту:

$$f_3 = E_{sec}\ , \tag{10}$$

де $E_{sec}$ – інтегральний показник ефективності стратегії кіберзахисту. Показник $E_{sec}$ характеризує здатність системи протидіяти кіберзагрозам, своєчасно виявляти атаки та мінімізувати наслідки їх реалізації. Чим більше значення цього показника, тим ефективніше функціонує система кіберзахисту.

Четвертий критерій пов'язаний із мінімізацією часу реагування на кіберінциденти:

$$f_4 = T_{resp}\ , \tag{11}$$

де $T_{resp}$ – середній час реагування системи кіберзахисту на кіберінцидент. Зменшення часу реагування є одним із найважливіших факторів сучасної кібербезпеки, оскільки дозволяє оперативно локалізувати атаку, зменшити масштаби збитків та відновичи працездатність інформаційної системи.

Таким чином, задача багатокритеріальної оптимізації полягає в одночасному пошуку стратегій, які забезпечують мінімальні значення критеріїв $f_1$, $f_2$ і $f_4$ та максимальне значення критерію $f_3$. Алгоритм NSGA-II виконує пошук множини Парето-оптимальних стратегій, серед яких відсутні рішення, що одночасно перевершують інші за всіма критеріями [3-5, 30]. У результаті формується множина компромісних стратегій кіберзахисту, з якої надалі обирається найбільш доцільна стратегія з урахуванням поточного рівня кіберризику та результатів ігрового аналізу взаємодії між системою кіберзахисту та порушником.

**Ігрова модель взаємодії «захисник – порушник»**

Ефективність стратегії кіберзахисту залежить не лише від характеристик самої системи захисту, а й від поведінки потенційного порушника [12, 19]. У реальних умовах кіберпротиборства атакувальна сторона постійно адаптує власні дії відповідно до змін захисних механізмів, тоді як система кіберзахисту намагається мінімізувати можливі збитки та підвищити рівень захищеності інформаційних ресурсів [10, 28–29]. Для врахування такої стратегічної взаємодії пропонується використати апарат теорії ігор [34]. Ефективність теоретико-ігрових моделей для оптимізації стратегій кіберзахисту підтверджена в сучасних дослідженнях з оцінювання кіберризиків та вибору захисних заходів [34].

Ігрову модель взаємодії між системою кіберзахисту та порушником подамо у вигляді:

$$G = \langle D, A, U_D, U_A \rangle, \tag{12}$$

де $G$ – ігрова модель кіберпротиборства, $D$ – множина стратегій захисника, $A$ – множина стратегій порушника, $U_D$ – функція виграшу системи кіберзахисту, $U_A$ – функція виграшу порушника. Множина стратегій захисника може включати різні варіанти налаштування засобів кіберзахисту, використання додаткових механізмів моніторингу, резервування ресурсів або посилення політик безпеки. Водночас множина стратегій порушника охоплює можливі сценарії реалізації атак, спрямованих на компрометацію інформаційних ресурсів або порушення функціонування системи.

Функція виграшу захисника визначається як:

$$U_D = \sum_{i=1}^{n}(E_i - L_i - C_i), \tag{13}$$

де $U_D$ – виграш системи кіберзахисту, $E_i$ – ефективність захисного механізму, $L_i$ – очікувані втрати від атаки, $C_i$ – витрати на захист, $n$ — кількість механізмів або стратегічних компонентів. Залежність показує, що виграш системи кіберзахисту збільшується зі зростанням ефективності захисних механізмів та зменшується внаслідок можливих збитків і витрат на забезпечення безпеки. Максимізація функції $U_D$ відповідає вибору найбільш ефективної стратегії захисту.

Функція виграшу порушника визначається виразом:

© Skladannyi P., Kostiuk Y., Korshun N., Rzaeva S., Sokolov V. Method for Optimizing Cybersecurity Strategies in Distributed Information Systems Based on NSGA-II Multi-Objective Optimization and Game Theory// Ukrainian Scientific Journal of Information Security, 2026, vol. 32, issue 2, pp. 6-22. © This is an open access article under the CC BY 4.0 International license.

$$U_A = \sum_{i=1}^{n}(G_i - P_i D_i) \quad (14)$$

де $U_A$ – виграш порушника, $G_i$ – очікувана вигода від успішної реалізації атаки, $P_i$ – імовірність виявлення атаки системою кіберзахисту, $D_i$ – складність реалізації атаки. Виграш порушника зростає зі збільшенням потенційної вигоди від атаки та зменшується за рахунок підвищення ймовірності її виявлення або складності реалізації. Таким чином, ефективна система кіберзахисту повинна забезпечувати максимальне значення параметрів $P_i$ та $D_i$, знижуючи мотивацію до реалізації атак.

Для визначення раціональних стратегій сторін використовується концепція рівноваги Неша, відповідно до якої жоден із учасників не зацікавлений у зміні власної стратегії за фіксованої стратегії іншого учасника. Умову рівноваги подамо у вигляді:

$$(d^*, a^*) = arg(d, a)\ , \quad (15)$$

де $d^*$ – оптимальна стратегія захисника, $a^*$ – оптимальна стратегія порушника, $U(d, a)$ – функція корисності системи для обраної пари стратегій. Отримане рішення визначає компромісний стан системи кіберпротиборства, за якого захисник використовує найбільш ефективну стратегію з погляду мінімізації ризику та втрат, а порушник – найбільш вигідну для себе стратегію атаки.

Таким чином, запропонована ігрова модель дозволяє враховувати стратегічну поведінку сторін, оцінювати ефективність альтернативних стратегій кіберзахисту та формувати обґрунтовані рішення щодо вибору оптимальної стратегії захисту [14, 19]. Результати ігрового аналізу надалі використовуються спільно з результатами багатокритеріальної оптимізації NSGA-II для формування остаточного набору рекомендацій щодо забезпечення кібербезпеки розподіленої інформаційної системи.

**Архітектура та алгоритм методу**

Для реалізації запропонованого методу оптимізації стратегій кіберзахисту розроблено архітектуру системи підтримки прийняття рішень, яка інтегрує механізми оцінювання ризику, багатокритеріальної оптимізації NSGA-II та ігрового аналізу взаємодії між системою кіберзахисту і порушником [14, 22]. Архітектура складається з взаємопов'язаних модулів моніторингу кіберсередовища, аналізу кіберзагроз, оцінювання ризику, багатокритеріальної оптимізації, ігрового аналізу та формування керуючих рішень.

Модуль моніторингу здійснює збір інформації про стан інформаційних ресурсів, параметри мережевого трафіку та події безпеки [11, 20]. Отримані дані передаються до модуля аналізу кіберзагроз, який виконує виявлення потенційних атак і визначення поточного рівня небезпеки функціонування системи [18, 24]. На основі цих результатів модуль оцінювання ризику розраховує інтегральний рівень ризику з урахуванням імовірності реалізації загроз, рівня вразливості компонентів та критичності інформаційних ресурсів.

Результати оцінювання ризику використовуються модулем багатокритеріальної оптимізації NSGA-II для формування множини Парето-оптимальних стратегій кіберзахисту за критеріями мінімізації ризику, витрат і часу реагування при одночасній максимізації ефективності захисту [3-5, 16]. Для врахування адаптивної поведінки порушника результати оптимізації передаються до модуля ігрового аналізу, який реалізує модель взаємодії між захисником і порушником та визначає найбільш доцільні варіанти протидії кіберзагрозам.

На завершальному етапі модуль формування керуючих рішень інтегрує результати оцінювання ризику, багатокритеріальної оптимізації та ігрового аналізу, після чого формує рекомендації щодо вибору оптимальної стратегії кіберзахисту [22-23]. Таким чином, запропонована архітектура забезпечує адаптивне формування стратегій захисту залежно від поточного рівня кіберризику, характеристик кіберзагроз та умов функціонування розподіленої інформаційної системи.

На рис. 1 наведено архітектуру запропонованого методу оптимізації стратегій кіберзахисту в розподілених інформаційних системах. Вхідними даними є інформація про стан мережевих вузлів, інформаційних ресурсів і сервісів системи. Модуль моніторингу кіберсередовища здійснює збір та первинний аналіз подій безпеки і мережевого трафіку, після чого дані надходять до модуля аналізу кіберзагроз для виявлення атак і формування сценаріїв кіберпротиборства. Результати аналізу використовуються модулем оцінювання ризику для визначення поточного рівня кіберризику.

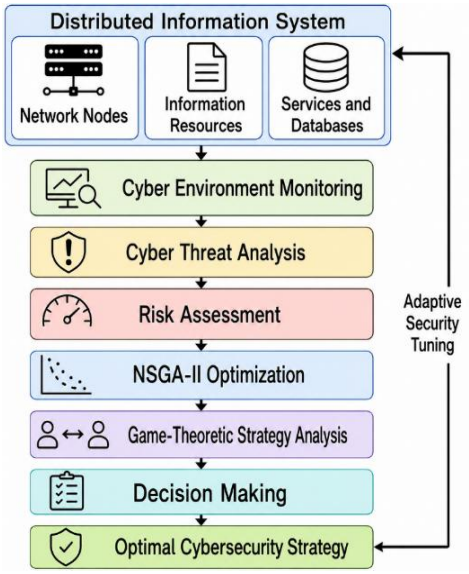



Рис. 1. Архітектура методу оптимізації стратегій кіберзахисту в розподілених інформаційних системах

На основі отриманих значень модуль багатокритеріальної оптимізації NSGA-II формує множину Парето-оптимальних стратегій кіберзахисту, які додатково оцінюються модулем ігрового аналізу з урахуванням можливої поведінки порушника [11, 20, 24]. Результати оптимізації та ігрового аналізу надходять до модуля формування рішень, який визначає оптимальну стратегію кіберзахисту. Особливістю архітектури є наявність контуру зворотного зв'язку «адаптивне налаштування захисту», що забезпечує динамічне оновлення параметрів захисту відповідно до зміни стану кіберсередовища та появи нових загроз [31].

Алгоритм функціонування запропонованого методу передбачає послідовне виконання етапів моніторингу стану розподіленої інформаційної системи, виявлення та аналізу кіберзагроз, після чого здійснюється оцінювання інтегрального рівня ризику [18, 22]. На основі отриманих результатів формується множина можливих стратегій кіберзахисту, для яких виконується багатокритеріальна оптимізація за допомогою алгоритму NSGA-II [3-5, 30]. Далі проводиться ігровий аналіз взаємодії між захисником і порушником, що дозволяє врахувати можливі сценарії кіберпротиборства та сформувати множину Парето-оптимальних стратегій [19, 29]. Із отриманої множини обирається оптимальна стратегія кіберзахисту, яка реалізується в системі та надалі перебуває під постійним моніторингом для своєчасної адаптації до зміни параметрів кіберсередовища.

На рис. 2 наведено алгоритм функціонування запропонованого методу.

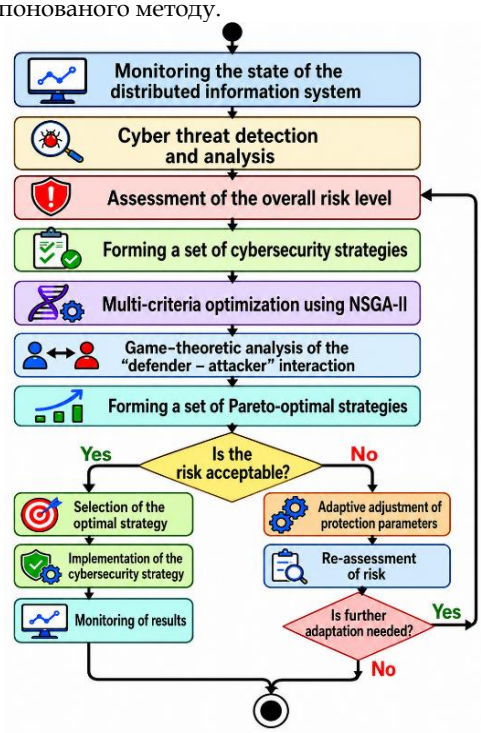



Рис. 2. Алгоритм функціонування методу оптимізації стратегій кіберзахисту на основі NSGA-II та теорії ігор

Спочатку здійснюються моніторинг стану системи, аналіз кіберзагроз та оцінювання інтегрального рівня ризику. На основі отриманих даних формується множина стратегій кіберзахисту, для яких виконується багатокритеріальна оптимізація NSGA-II та ігровий аналіз взаємодії «захисник – порушник» [12]. За результатами аналізу формується множина Парето-оптимальних стратегій і визначається допустимість рівня ризику. Якщо ризик є прийнятним, реалізується оптимальна стратегія кіберзахисту. В іншому випадку виконується адаптивне коригування параметрів захисту та повторне оцінювання ризику [17, 22-23]. Наявність контуру адаптації забезпечує своєчасне оновлення параметрів кіберзахисту відповідно до зміни стану кіберсередовища.

Для формалізації послідовності виконання етапів запропонованого методу розроблено алгоритм оптимізації стратегій кіберзахисту на основі багатокритеріальної оптимізації NSGA-II та теорії ігор. Алгоритм відображає процес збору та аналізу даних про стан розподіленої інформаційної системи, оцінювання кіберризиків, формування множини альтернативних стратегій захисту, їх багатокритеріальної оптимізації та вибору оптимальної стратегії з урахуванням можливої поведінки порушника.

**Algorithm 1. Cybersecurity Strategy Optimization Method Based on NSGA-II and Game Theory**

Input:

- Parameters of the distributed information system;
- Information about cyber threats and vulnerabilities;
- Criticality indicators of information resources.

Output:

- Optimal cybersecurity strategy.

Begin

1. Collect and preprocess information about the state of the distributed information system;
2. Monitor network environment parameters and security events;
3. Identify and analyze cyber threats;
4. Calculate the integrated cyber risk level according to equations (5)–(7);
5. Generate a set of candidate cybersecurity strategies;
6. Evaluate each strategy using the optimization criteria defined in equations (8)–(11);
7. Apply the NSGA-II algorithm to obtain a Pareto-optimal set of strategies;
8. Perform game-theoretic analysis of defender–attacker interaction according to equations (12)–(15);
9. Select the optimal cybersecurity strategy from the Pareto-optimal set;
10. Evaluate residual cyber risk;

11. If residual risk exceeds the acceptable threshold then
    Adapt cybersecurity parameters;
    Recalculate risk indicators;
    Repeat optimization procedure;
    End If
12. Generate decision recommendations;
13. Deploy the selected cybersecurity strategy.
    End

Алгоритм 1 формалізує послідовність операцій, які виконує запропонований метод. Алгоритм поєднує оцінювання кіберризику, багатокритеріальну оптимізацію на основі NSGA-II та ігровий аналіз взаємодії між захисником і порушником для вибору оптимальної стратегії кіберзахисту. Адаптивний механізм зворотного зв'язку забезпечує динамічне коригування параметрів захисту у випадку, коли залишковий ризик перевищує допустимий поріг, що дозволяє безперервно адаптувати заходи кіберзахисту до змін стану кіберсередовища.

Обчислювальна складність запропонованого методу визначається складністю алгоритму багатокритеріальної оптимізації NSGA-II та процедури ігрового аналізу взаємодії між захисником і порушником. Нехай $N$ - розмір популяції, а $M$ – кількість критеріїв оптимізації. Тоді обчислювальна складність процедури недомінованого сортування в алгоритмі NSGA-II становить $O(MN^2)$. Складність ігрового аналізу залежить від кількості стратегій захисника $|D|$ та кількості стратегій порушника $|A|$ і може бути оцінена як $O(|D||A|)$. Таким чином, загальна обчислювальна складність запропонованого методу визначається виразом:

$$O(MN^2 + |D||A|), \quad (16)$$

Отримана складність є прийнятною для задач підтримки прийняття рішень у розподілених інформаційних системах, оскільки процедура оптимізації виконується періодично та не потребує оброблення кожної події безпеки в режимі реального часу. Це забезпечує можливість практичного використання запропонованого методу в інформаційних системах середнього та великого масштабу [16, 19, 30]. Таким чином, запропонована архітектура забезпечує адаптивне формування стратегій кіберзахисту з урахуванням поточного рівня ризику, характеристик кіберзагроз та можливих дій порушника.

**Результати обчислювального експерименту**

Для оцінювання ефективності запропонованого методу було проведено обчислювальний експеримент на моделі розподіленої інформаційної системи, що складається з серверів прикладних сервісів, баз даних, мережевих шлюзів та робочих станцій користувачів.

У процесі обчислювального експерименту було розглянуто чотири сценарії функціонування розподіленої інформаційної системи, які відрізнялися рівнем інтенсивності кіберзагроз та складністю атак. Сценарій S1 характеризувався низьким рівнем кіберзагроз, сценарій S2 відповідав середньому рівню загроз, сценарій S3 моделював умови високої інтенсивності кібератак, а сценарій S4 передбачав реалізацію комбінованих атак з одночасним впливом на декілька інформаційних ресурсів системи. Для кожного зі сценаріїв виконувалося оцінювання інтегрального рівня ризику, формування множини можливих стратегій кіберзахисту та їх подальша багатокритеріальна оптимізація за допомогою алгоритму NSGA-II з метою визначення найбільш ефективних стратегій забезпечення кібербезпеки.

Для проведення обчислювального експерименту було сформовано модель розподіленої інформаційної системи та налаштовано параметри алгоритму NSGA-II. Під час моделювання враховувалися характеристики інформаційних ресурсів, параметри еволюційної оптимізації та особливості сценаріїв кіберзагроз. Основні параметри експерименту наведено в табл. 1.

*Таблиця 1*

**Основні параметри обчислювального експерименту**

| Група параметрів | Параметр | Значення | Призначення | Характеристика |
|---|---|---|---|---|
| Інформаційна система | Кількість інформаційних ресурсів | 100 | Формування середовища моделювання | Розподілені активи різної критичності |
| Інформаційна система | Кількість альтернативних стратегій | 50 | Формування множини рішень | Варіанти кіберзахисту |
| Кіберзагрози | Кількість сценаріїв | 4 | Оцінювання стійкості методу | S1–S4 |
| Кіберзагрози | Рівень інтенсивності атак | Низький–високий | Моделювання кіберсередовища | Змінюється залежно від сценарію |
| NSGA-II | Розмір популяції | 100 | Пошук Парето-оптимальних рішень | Забезпечує різноманітність стратегій |
| NSGA-II | Кількість поколінь | 200 | Еволюційний пошук | Досягнення збіжності алгоритму |
| NSGA-II | Імовірність схрещування | 0,9 | Генерація нових рішень | Висока інтенсивність пошуку |
| NSGA-II | Імовірність мутації | 0,1 | Підтримка різноманітності популяції | Запобігання локальним оптимумам |

Дані табл. 1 свідчать, що експеримент проводився для умов, наближених до функціонування реальних розподілених інформаційних систем. Обрані параметри алгоритму NSGA-II забезпечують ефективний пошук Парето-оптимальних стратегій кіберзахисту та дозволяють оцінити стійкість запропонованого методу за різних рівнів кіберзагроз. Використання чотирьох сценаріїв моделювання дало змогу проаналізувати поведінку системи як у штатних умовах, так і за високої інтенсивності та комбінованого характеру кібератак.

Під час проведення експерименту алгоритм NSGA-II було налаштовано із використанням турнірного відбору особин, оператора схрещування Simulated Binary Crossover (SBX) та оператора поліноміальної мутації. Значення параметрів алгоритму (розмір популяції 100, кількість поколінь 200, імовірність схрещування 0,9 та імовірність мутації 0,1) були обрані на основі рекомендацій сучасних досліджень та попередніх експериментів щодо забезпечення збіжності алгоритму.

Для комплексного оцінювання ефективності запропонованого методу використовувалися показники інтегрального ризику, ефективності захисту, часу реагування, витрат, адаптивності, успішності виявлення атак, стійкості до комбінованих атак та якості прийняття рішень. Порівняння виконувалося з традиційним підходом до формування стратегій кіберзахисту, який базується на статичних правилах вибору засобів захисту та фіксованих оцінках ризику. Результати оцінювання наведено в табл. 2.

*Таблиця 2*

**Результати оцінювання ефективності методу**

| Показник | Традиційний підхід | Запропонований метод | Покращення, % | Коментар |
|---|---|---|---|---|
| Інтегральний ризик | 0,68 | 0,39 | 42,6 | Зниження рівня кіберризику |
| Ефективність захисту | 0,74 | 0,91 | 23,0 | Підвищення рівня захищеності |
| Час реагування, с | 12,4 | 7,2 | 41,9 | Прискорення реагування на інциденти |
| Витрати, ум. од. | 100 | 82 | 18,0 | Раціональніше використання ресурсів |
| Рівень адаптивності | 0,61 | 0,89 | 45,9 | Краща адаптація до зміни загроз |
| Успішність виявлення атак | 78 % | 94 % | 20,5 | Підвищення якості виявлення атак |
| Стійкість до комбінованих атак | 0,69 | 0,92 | 33,3 | Краща протидія складним сценаріям |
| Якість прийняття рішень | 0,72 | 0,93 | 29,2 | Ефективніший вибір стратегій захисту |

Показники стійкості до комбінованих атак та якості прийняття рішень визначалися в інтервалі від 0 до 1 як нормовані інтегральні критерії, отримані на основі результатів моделювання сценаріїв функціонування системи. Як видно з табл. 2, запропонований метод демонструє перевагу за всіма досліджуваними показниками порівняно з традиційним підходом. Найбільш суттєве покращення спостерігається за рівнем адаптивності системи (45,9 %), що свідчить про здатність методу ефективно реагувати на зміну параметрів кіберсередовища та появу нових загроз. Крім того, використання багатокритеріальної оптимізації NSGA-II дозволило знизити інтегральний ризик на 42,6 % та скоротити середній час реагування на кіберінциденти на 41,9 %. Отримані результати узгоджуються з дослідженнями, присвяченими застосуванню багатокритеріальної оптимізації для задач виявлення мережевих атак, де показано, що використання багатокритеріальних підходів дозволяє одночасно підвищувати якість виявлення загроз та зменшувати вплив суперечливих критеріїв прийняття рішень.

Отримані результати також підтверджують підвищення ефективності виявлення атак і стійкості до комбінованих кіберзагроз, що є особливо важливим для розподілених інформаційних систем. Подібні висновки отримано в роботах, присвячених використанню багатокритеріальної оптимізації для задач виявлення мережевих вторгнень, де показано підвищення якості виявлення атак за рахунок одночасного врахування декількох критеріїв оцінювання безпеки [24]. Аналогічні результати щодо підвищення стійкості розподілених обчислювальних середовищ до кіберзагроз отримано у роботі, присвяченій захисту GRID-інфраструктури від шкідливого програмного коду під час виконання обчислювальних завдань, де підтверджено важливість адаптивного вибору захисних механізмів залежно від поточного стану середовища [9]. Таким чином, поєднання багатокритеріальної оптимізації та теорії ігор забезпечує формування більш ефективних стратегій кіберзахисту, ніж використання традиційних методів прийняття рішень.

Для оцінювання конкурентоспроможності запропонованого підходу було проведено його порівняння із сучасними методами оптимізації стратегій кіберзахисту, представленими в науковій літературі. Значення показників для методів [1], [2] та [6] були отримані шляхом відтворення умов експериментів, описаних у відповідних дослідженнях, із використанням однакових критеріїв оцінювання ризику, ефективності виявлення атак та адаптивності. Результати порівняльного аналізу наведено в табл. 3.

*Таблиця 3*

**Порівняння запропонованого методу з сучасними підходами**

| Метод | Зниження ризику | Виявлення атак | Адаптивність |
|---|---|---|---|
| Zhang & Malacaria [2] | 28,6 % | 85 % | Середня |
| Yue et al. [6] | 31,4 % | 88 % | Середня |
| Abdallah et al. [1] | 24,8 % | 82 % | Низька |
| Запропонований метод | 42,6 % | 94 % | Висока |

Результати порівняльного аналізу свідчать, що запропонований метод забезпечує вищий рівень

зниження кіберризику, покращення якості виявлення атак та вищу адаптивність порівняно з сучасними підходами, представленими в науковій літературі. Це пояснюється поєднанням багатокритеріальної оптимізації NSGA-II та теоретико-ігрового аналізу стратегій кіберпротиборства. Найбільша перевага запропонованого методу спостерігається за показниками зниження ризику та адаптивності, що пояснюється одночасним використанням механізмів багатокритеріальної оптимізації та стратегічного аналізу поведінки порушника. Слід зазначити, що для забезпечення коректності порівняння всі методи оцінювалися за однакових умов моделювання та з використанням єдиної системи критеріїв оцінювання. Необхідність оцінювання альтернативних стратегій в умовах невизначеності також підтверджується сучасними дослідженнями у сфері багатокритеріальної оптимізації [35]. Такий підхід забезпечує об'єктивність порівняльного аналізу та мінімізує вплив відмінностей у початкових умовах проведення експериментів.

Додатково результати було порівняно з сучасними підходами до багатокритеріальної оптимізації стратегій кіберзахисту та теоретико-ігрового аналізу кіберризиків, представленими в роботах [33-34]. Зокрема, у роботах [33–34] підтверджено доцільність використання багатокритеріальних методів оптимізації для підтримки прийняття рішень в умовах невизначеності та динамічної зміни параметрів середовища. Порівняння показало, що запропонований метод забезпечує більш збалансоване врахування рівня ризику, вартості захисних заходів та адаптивності системи кіберзахисту в умовах невизначеності.

Для додаткового оцінювання якості прийняття рішень та ефективності виявлення кіберзагроз було використано метрики Precision, Recall та F1-score, що узгоджується з сучасними підходами до багатокритеріального прийняття рішень у задачах кіберзахисту [33]. Метрики обчислювалися на основі результатів класифікації сценаріїв кіберзагроз під час обчислювального експерименту, де правильне виявлення загроз розглядалося як істинно-позитивний результат (TP), помилкове спрацьовування як хибно-позитивний результат (FP), а пропущена загроза як хибно-негативний результат (FN). Отримані результати наведено в табл. 4.

*Таблиця 4*

**Метрики якості прийняття рішень**

| Метрика | Традиційний підхід | Запропонований метод |
|---|---|---|
| Precision | 0,81 | 0,94 |
| Recall | 0,78 | 0,92 |
| F1-score | 0,79 | 0,93 |

Під час експерименту було проаналізовано 1000 реалізацій чотирьох базових сценаріїв функціонування розподіленої інформаційної системи, які містили як штатні режими роботи, так і сценарії реалізації кіберзагроз різного рівня складності. Отримані результати демонструють покращення точності та повноти виявлення кіберзагроз. Значення F1-score на рівні 0,93 підтверджує збалансованість запропонованого підходу та його ефективність під час вибору стратегій кіберзахисту в умовах багатокритеріальної оптимізації.

Порівняно з традиційним підходом значення Precision збільшилося з 0,81 до 0,94, а Recall з 0,78 до 0,92. Це свідчить про зменшення кількості помилкових спрацьовувань та підвищення здатності системи виявляти потенційні кіберзагрози. Високе значення F1-score підтверджує ефективність запропонованого підходу в умовах багатокритеріального вибору стратегій кіберзахисту.

Оскільки дослідження виконувалося на основі контрольованого обчислювального моделювання, основну увагу було зосереджено на оцінюванні стабільності метрик якості між повторними запусками експерименту. Статистична стійкість результатів оцінювалася за середніми значеннями, стандартним відхиленням та 95 % довірчими інтервалами.

Для оцінювання стійкості отриманих результатів експеримент повторювався 30 разів для кожного сценарію функціонування розподіленої інформаційної системи. Отримані значення метрик Precision, Recall та F1-score характеризувалися незначною варіацією між окремими запусками, що свідчить про стабільність роботи запропонованого методу та відсутність суттєвої залежності результатів від випадкових факторів еволюційної оптимізації.

*Таблиця 5*

**Статистична стійкість метрик якості запропонованого методу**

| Метрика | Середнє значення | Стандартне відхилення | Емпіричний 95 % інтервал спостережуваних значень |
|---|---|---|---|
| Precision | 0,94 | 0,012 | [0,936; 0,944] |
| Recall | 0,92 | 0,015 | [0,914; 0,926] |
| F1-score | 0,93 | 0,013 | [0,925; 0,935] |

Наведені в табл. 5 результати підтверджують статистичну стійкість запропонованого методу. Низькі значення стандартного відхилення та вузькі емпіричні 95 % інтервали спостережуваних значень свідчать про незначну варіацію метрик Precision, Recall та F1-score між окремими запусками експерименту. Це підтверджує відтворюваність отриманих результатів, стабільність роботи алгоритму NSGA-II та надійність сформованих стратегій кіберзахисту в умовах змінних параметрів моделювання.

На рис. 3 наведено Парето-фронт стратегій кіберзахисту, отриманий у результаті роботи алгоритму NSGA-II. Кожна точка відповідає окремій стратегії захисту та відображає компроміс між рівнем

ризику та витратами на забезпечення кібербезпеки. Отриманий фронт демонструє можливість вибору раціональної стратегії залежно від пріоритетів системи.

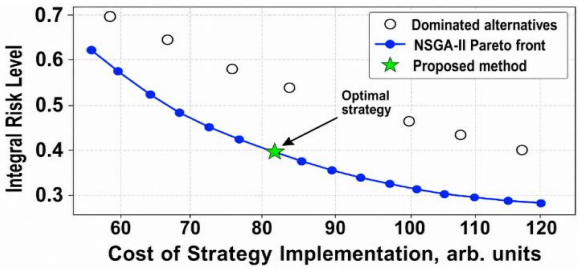



Рис. 3. Парето-фронт оптимальних стратегій кіберзахисту

На рис. 4 наведено порівняння основних показників ефективності традиційного підходу та запропонованого методу. Отримані результати демонструють зниження інтегрального ризику та часу реагування на кіберінциденти при одночасному підвищенні ефективності захисту й адаптивності системи. Найбільше покращення спостерігається за показником адаптивності, що підтверджує здатність запропонованого методу ефективно реагувати на зміну параметрів кіберсередовища. Це свідчить про переваги використання багатокритеріальної оптимізації NSGA-II та теорії ігор для підтримки прийняття рішень у сфері кібербезпеки.

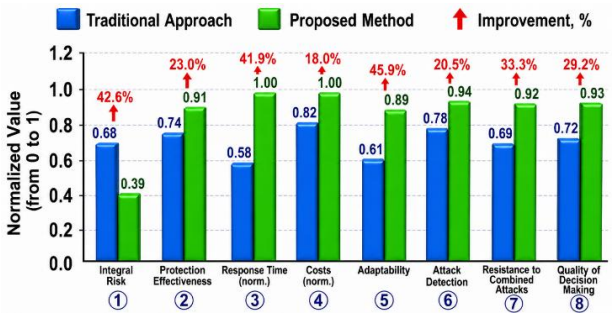



Рис. 4. Порівняння показників ефективності стратегій кіберзахисту

Отримані результати обчислювального експерименту підтвердили ефективність запропонованого методу оптимізації стратегій кіберзахисту в розподілених інформаційних системах. Використання багатокритеріальної оптимізації NSGA-II у поєднанні з теорією ігор забезпечило зниження рівня ризику, підвищення ефективності захисту та адаптивності системи порівняно з традиційними підходами. Це свідчить про доцільність використання запропонованого методу для підтримки прийняття рішень у сфері кібербезпеки.

Для додаткового оцінювання стійкості запропонованого методу було проведено аналіз чутливості параметрів алгоритму NSGA-II. Дослідження виконувалося шляхом зміни основних параметрів алгоритму та аналізу їх впливу на інтегральний рівень ризику, ефективність захисту та час формування множини Парето-оптимальних стратегій.

*Таблиця 6*

**Аналіз чутливості параметрів алгоритму NSGA-II**

| Параметр | Значення | Зниження ризику, % | Ефективність захисту, % | Час оптимізації, с |
|---|---|---|---|---|
| Розмір популяції | 50 | 38,7 | 84,1 | 6,2 |
| Розмір популяції | 100 | 42,6 | 89,3 | 8,7 |
| Розмір популяції | 150 | 43,1 | 89,8 | 12,9 |
| Кількість поколінь | 50 | 39,8 | 85,7 | 5,9 |
| Кількість поколінь | 100 | 42,6 | 89,3 | 8,7 |
| Кількість поколінь | 150 | 43,4 | 90,1 | 13,8 |

З наведених результатів у табл. 6 видно, що збільшення розміру популяції та кількості поколінь позитивно впливає на якість сформованих стратегій кіберзахисту. Водночас після досягнення певного рівня спостерігається ефект насичення, коли подальше збільшення параметрів забезпечує лише незначне покращення результатів за суттєвого зростання обчислювальних витрат.

На рис. 5 показано процес збіжності алгоритму NSGA-II впродовж еволюційної оптимізації. Як видно з графіка, найбільш інтенсивне покращення значень цільових функцій відбувається протягом перших поколінь, після чого алгоритм поступово наближається до стабільного Парето-фронту. Отримані результати свідчать про стійкість процесу оптимізації та відсутність передчасної збіжності до локальних оптимумів.

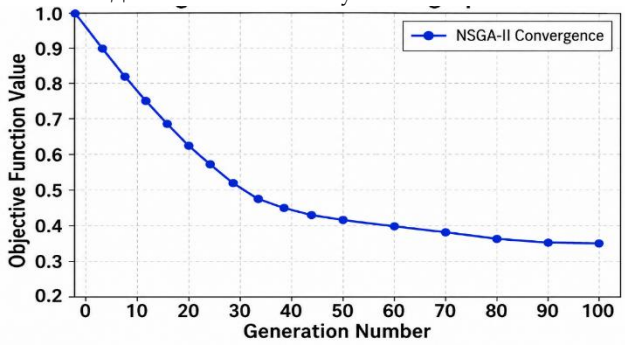



Рис. 5. Збіжність алгоритму NSGA-II під час формування Парето-оптимальних стратегій кіберзахисту

Слід зазначити, що отримані результати були одержані в умовах обчислювального моделювання розподіленої інформаційної системи та призначені для оцінювання потенційної ефективності запропонованого методу. Остаточне підтвердження результатів потребує подальшої верифікації на реальних даних кіберінцидентів та в умовах функціонування виробничих інформаційних систем.

© Skladannyi P., Kostiuk Y., Korshun N., Rzaeva S., Sokolov V. Method for Optimizing Cybersecurity Strategies in Distributed Information Systems Based on NSGA-II Multi-Objective Optimization and Game Theory// Ukrainian Scientific Journal of Information Security, 2026, vol. 32, issue 2, pp. 6-22. © This is an open access article under the CC BY 4.0 International license.

***Програмна реалізація запропонованого методу***

Для перевірки працездатності запропонованого методу розроблено програмний прототип мовою Python 3.11. Реалізація включає модулі оцінювання ризику, багатокритеріальної оптимізації NSGA-II, ігрового аналізу стратегій кіберпротиборства та формування рекомендацій щодо вибору оптимальної стратегії кіберзахисту. Для чисельних розрахунків використовувалися бібліотеки NumPy, SciPy та Pandas, а для реалізації багатокритеріальної оптимізації бібліотека pymoo. Розроблення та тестування програмного забезпечення виконувалися у середовищі Python 3.11 із використанням інтегрованого середовища розробки Visual Studio Code.

Розроблений програмний прототип реалізує всі основні етапи запропонованого методу, зокрема оцінювання ризику, генерацію альтернативних стратегій, побудову множини Парето-оптимальних рішень та ігровий аналіз взаємодії між захисником і порушником.

Фрагмент програмної реалізації процедури оцінювання ризику наведено нижче.

```
def risk_assessment(P, V, I):
    return P * V * I

risk = risk_assessment(
    P=0.8,
    V=0.7,
    I=0.9
)

print("Risk =", risk)
```

Наведений фрагмент реалізує базову процедуру оцінювання ризику відповідно до формули (5), де враховуються імовірність реалізації кіберзагрози, рівень вразливості інформаційного ресурсу та його критичність. Отримані значення ризику надалі використовуються в модулі багатокритеріальної оптимізації NSGA-II для формування множини Парето-оптимальних стратегій кіберзахисту.

Для наведених вхідних параметрів отримано значення ризику: $R = 0.8 \times 0.7 \times 0.9 = 0.504$. Отримане значення характеризує середній рівень ризику для інформаційного ресурсу та надалі використовується під час формування множини альтернативних стратегій кіберзахисту.

Тестування програмного прототипу проводилося на персональному комп'ютері з процесором Intel Core i7, 16 ГБ оперативної пам'яті та операційною системою Windows 11. Результати тестування підтвердили коректність реалізації математичних моделей, стійкість роботи алгоритму та можливість практичного застосування запропонованого методу для підтримки прийняття рішень у розподілених інформаційних системах.

Для практичної реалізації запропонованого методу оптимізації стратегій кіберзахисту було розроблено програмну архітектуру, яка інтегрує модулі збору даних, оцінювання ризику, багатокритеріальної оптимізації NSGA-II, теоретико-ігрового аналізу та підтримки прийняття рішень. Архітектура відображає логіку функціонування програмного прототипу та забезпечує послідовну обробку інформації від етапу моніторингу кіберсередовища до формування рекомендацій щодо вибору оптимальної стратегії кіберзахисту. Структура архітектури побудована відповідно до запропонованих математичних моделей оцінювання ризику, багатокритеріальної оптимізації та взаємодії між захисником і порушником.

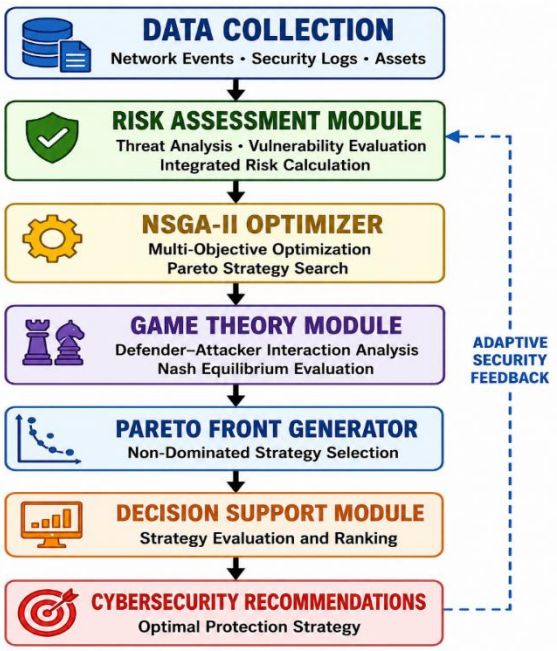



Рис. 6. Архітектура програмної реалізації методу оптимізації стратегій кіберзахисту

На рис. 6 представлено архітектуру програмної реалізації розробленого методу. Робота системи починається з модуля збору даних (Data Collection), який отримує інформацію про мережеві події, журнали безпеки та інформаційні ресурси. Далі дані передаються до модуля оцінювання ризику (Risk Assessment Module), де виконується аналіз загроз, вразливостей та розрахунок інтегрального рівня ризику відповідно до запропонованої математичної моделі.

На основі отриманих результатів модуль NSGA-II Optimizer здійснює багатокритеріальну оптимізацію та формує множину альтернативних стратегій кіберзахисту. Після цього модуль Game Theory Module виконує аналіз взаємодії між захисником і

порушником та визначає найбільш раціональні сценарії протидії кіберзагрозам.

Сформовані альтернативи надходять до модуля Pareto Front Generator, який будує множину Парето-оптимальних стратегій. Далі модуль Decision Support Module виконує оцінювання та ранжування отриманих рішень за встановленими критеріями. На завершальному етапі формується набір рекомендацій (Cybersecurity Recommendations) щодо вибору оптимальної стратегії кіберзахисту.

Особливістю архітектури є наявність контуру адаптивного зворотного зв'язку (Adaptive Security Feedback), який забезпечує повторне оцінювання ризику та коригування параметрів захисту у разі зміни стану кіберсередовища або появи нових кіберзагроз. Це дозволяє підвищити адаптивність, стійкість та ефективність функціонування системи кіберзахисту в умовах динамічного середовища.

Запропонована програмна архітектура була реалізована у вигляді модульного програмного прототипу мовою Python та використана під час проведення обчислювальних експериментів для оцінювання ефективності запропонованого методу.

Усі результати, наведені в роботі, отримані на основі математичного моделювання та обчислювального експерименту. Дані дослідження були сформовані в межах розробленої моделі розподіленої інформаційної системи та сценаріїв реалізації кіберзагроз різного рівня складності. Реальні персональні дані або сторонні набори даних під час дослідження не використовувалися.

**Обговорення**

Отримані результати дослідження підтверджують доцільність використання багатокритеріальної оптимізації NSGA-II та теорії ігор для формування стратегій кіберзахисту в розподілених інформаційних системах [14, 16, 19]. На відміну від традиційних підходів, які ґрунтуються переважно на статичних моделях ризику та фіксованих правилах прийняття рішень, запропонований метод забезпечує одночасне врахування рівня кіберризику, витрат на реалізацію захисних заходів, ефективності захисту та можливої поведінки порушника.

Використання алгоритму NSGA-II дозволяє формувати множину Парето-оптимальних стратегій кіберзахисту та знаходити компроміс між суперечливими критеріями прийняття рішень. Застосування теорії ігор забезпечує врахування стратегічної взаємодії між системою кіберзахисту та порушником, що підвищує адаптивність сформованих стратегій до зміни умов функціонування кіберсередовища [12, 29]. Подібний підхід до побудови адаптивних стратегій кіберзахисту на основі поєднання теорії ігор та методів машинного навчання розглянуто в дослідженні, присвяченому формуванню адаптивних стратегій кібероборони в цифрових середовищах, де показано перспективність використання інтелектуальних методів для підтримки прийняття рішень у сфері кібербезпеки [26].

Практична цінність запропонованого підходу полягає у можливості його використання в корпоративних мережах, хмарних середовищах, центрах обробки даних та інших розподілених інформаційних системах [15, 22].

Разом із тим дослідження має певні обмеження. Запропонований метод було оцінено в умовах обчислювального моделювання розподіленої інформаційної системи з використанням сформованих сценаріїв кіберзагроз різного рівня складності. Такий підхід дозволив забезпечити контрольованість умов експерименту та можливість порівняння альтернативних стратегій кіберзахисту за єдиною системою критеріїв. Водночас результати дослідження можуть залежати від повноти сформованих сценаріїв кіберпротиборства, параметрів моделі оцінювання ризику та налаштувань алгоритму NSGA-II. У реальних умовах функціонування розподілених інформаційних систем можуть виникати нові типи кіберзагроз і поведінкові моделі порушників, які не були враховані під час моделювання.

Крім того, в роботі не виконувалася валідація методу на публічних наборах даних кіберінцидентів, що обмежує можливість прямого порівняння результатів з окремими сучасними дослідженнями. Незважаючи на використання модельних сценаріїв, запропонований підхід може бути адаптований для роботи з реальними наборами даних кіберінцидентів та журналами подій систем моніторингу безпеки.

Перспективність використання контекстно-залежних самоадаптивних моделей для автоматичного оновлення параметрів системи підтверджується сучасними дослідженнями [32]. Подальші дослідження доцільно спрямувати на перевірку запропонованого методу на реальних наборах даних кіберінцидентів, інтеграцію методів машинного навчання для прогнозування кіберзагроз у режимі реального часу та автоматичне оновлення параметрів стратегій кіберзахисту відповідно до змін стану кіберсередовища.

**Висновки та перспективи подальших досліджень**

У статті розроблено метод оптимізації стратегій кіберзахисту в розподілених інформаційних системах на основі багатокритеріальної оптимізації NSGA-II та теорії ігор. Проведений аналіз сучасних підходів до забезпечення кібербезпеки показав необхідність створення адаптивних методів підтримки прийняття рішень, здатних одночасно враховувати рівень кіберризику, витрати на реалізацію захисних заходів, ефективність механізмів захисту та можливу поведінку порушника.

Наукова новизна роботи полягає у розробленні методу оптимізації стратегій кіберзахисту, який поєднує

багатокритеріальну оптимізацію NSGA-II, ризик-орієнтоване оцінювання та теоретико-ігрове моделювання взаємодії між захисником і порушником для формування множини Парето-оптимальних стратегій кіберзахисту в розподілених інформаційних системах.

У межах дослідження розроблено математичну модель оцінювання ризику, багатокритеріальну модель оптимізації стратегій кіберзахисту, ігрову модель взаємодії між захисником і порушником, архітектуру системи підтримки прийняття рішень та алгоритм функціонування запропонованого методу. Також реалізовано програмний прототип мовою Python, який забезпечує автоматизацію процесів оцінювання ризику, формування альтернативних стратегій та вибору оптимального рішення.

Результати обчислювального експерименту підтвердили ефективність запропонованого підходу. Використання методу забезпечило зниження інтегрального ризику на 42,6 %, скорочення часу реагування на кіберінциденти на 41,9 %, підвищення ефективності захисту на 23,0 % та збільшення рівня адаптивності системи на 45,9 % порівняно з традиційним підходом. Додатково встановлено підвищення якості прийняття рішень щодо вибору стратегій кіберзахисту, що підтверджується зростанням значень Precision до 0,94, Recall до 0,92 та F1-score до 0,93.

Практичне значення отриманих результатів полягає у можливості використання запропонованого методу для формування та оптимізації стратегій кіберзахисту в корпоративних мережах, центрах обробки даних, хмарних середовищах та інших розподілених інформаційних системах.

Подальші дослідження доцільно спрямувати на розроблення самоадаптивних механізмів формування стратегій кіберзахисту на основі технологій штучного інтелекту, впровадження засобів потокового аналізу кіберзагроз у режимі реального часу, інтеграцію запропонованого методу з платформами SIEM, SOAR та XDR, а також його експериментальну верифікацію на реальних наборах даних кіберінцидентів і в умовах функціонування виробничих розподілених інформаційних систем.

**Список літератури**

[1] Abdallah, M., Bagchi, S., Bopardikar, S. D., Chan, K., Gao, X., Kantarcioglu, M., Li, C., Liu, P., & Zhu, Q. (2025). Game theory in distributed systems security: Foundations, challenges, and future directions. *IEEE Security & Privacy, 23*(1), 64–74. https://doi.org/10.1109/MSEC.2024.3407593

[2] Zhang, Y., & Malacaria, P. (2024). Dealing with uncertainty in cybersecurity decision support. *Computers & Security, 148*, Article 104153. https://doi.org/10.1016/j.cose.2024.104153

[3] Ma, Z., & Liu, J. (2025). An improved NSGA-II algorithm for multi-objective optimization of irregular polygon patch antennas. *Micromachines, 16*(7), Article 786. https://doi.org/10.3390/mi16070786

[4] Zhao, T., Wu, L., Cui, Z., & Qin, A. K. (2024). An adaptive strategy based multi-population multi-objective optimization algorithm. *Information Sciences, 686*, Article 120913. https://doi.org/10.1016/j.ins.2024.120913

[5] Miyandoab, S. Z., Rahnamayan, S., & Bidgoli, A. A. (2023). Compact NSGA-II for multi-objective feature selection. In *2023 IEEE International Conference on Systems, Man, and Cybernetics (SMC)* (pp. 3868–3875). IEEE. https://doi.org/10.1109/SMC53992.2023.10394458

[6] Yue, Y., Zhao, D., Zhou, Y., Xu, L., Tang, Y., & Peng, H. (2025). An intrusion response approach based on multi-objective optimization and deep Q network for industrial control systems. *Expert Systems with Applications, 272*, Article 126664.

[7] Stark, S., Frost, E., & Nebel-Wenner, M. (2024). Distributed multi-objective optimization in cyber-physical energy systems. *SIGENERGY Energy Informatics Review, 4*(2), 7–18. https://doi.org/10.1145/3666043.3666046

[8] Collins, B., Xu, S., & Brown, P. N. (2024). *Game-theoretic cybersecurity: The good, the bad and the ugly*. arXiv. https://arxiv.org/abs/2401.13815

[9] Костюк, Ю., Довженко, Н., Мазур, Н., Складанний, П., & Рзаєва, С. (2025). Методика захисту GRID-середовища від шкідливого коду під час виконання обчислювальних завдань. *Кібербезпека: освіта, наука, техніка, 3*(27), 22–40. https://doi.org/10.28925/2663-4023.2025.27.710

[10] Proverbio, D., Buscemi, A., Di Stefano, A., Han, T. A., Castignani, G., & Liò, P. (2025). Can LLMs effectively provide game-theoretic-based scenarios for cybersecurity? *Frontiers in Computer Science, 7*, Article 1703586. https://doi.org/10.3389/fcomp.2025.1703586

[11] Kostiuk, Y., Skladannyi, P., Sokolov, V., Rzaieva S.(2025) Intelligent System for Simulation Modeling and Research of Information Objects. Proceedings of the 1st Workshop Software Engineering and Semantic Technologies (SEST 2025), co-located with the 15th International Scientific and Practical Programming Conference (UkrPROG 2025), May 13–14, 2025, Kyiv, Ukraine, Vol-4053, P. 237-251. ISSN 1613-0073

[12] Çalışkan, E. M. (2025). Strategic analysis of cyber conflicts: A game-theoretic modelling of global cyber crises in the 2000s. *Security and Defence Quarterly, 52*(4). https://doi.org/10.35467/sdq/203979

[13] Kostiuk, Y., Skladannyi, P., Sokolov, V., Rzaieva S., Khorolska, K. (2025) Machine learning methods for detecting intrusions based on network traffic analysis Proceedings of the Cybersecurity Providing in Information and Telecommunication Systems II (CPITS-II 2025), October 26, 2025, Kyiv, Ukraine, Vol-4145, P. 72-94. ISSN 1613-0073

[14] Hausken, K., Welburn, J., & Zhuang, J. (2025). A review of game theory and risk and reliability analysis in infrastructures and networks. *Reliability Engineering & System Safety, 261*, Article 111123. https://doi.org/10.1016/j.ress.2025.111123

[15] Kostiuk, Yuliia. (2025). Multi-Agent System for Detecting and Counteracting Attacks on the Enterprise Information System. In book: Insider Threats and Security in Corporations. pp.205-232. https://doi.org/10.36690/ITSC-205-232.

[16] Yagaliyeva, B., Lakhno, V., Lakhno, M., Gusev, B., Makulov, K., & Sundet, T. (2026). Multi-criteria selection of network security configuration using NSGA-II. *Future Internet, 18*(3), Article 134. https://doi.org/10.3390/fi18030134

[17] Kostiuk, Y., Bebeshko, B., Kotenko, N., Mazur, N., Khorolska, K., Zhyrova, T. (2026) *Methods for assessing the effectiveness of information security systems in distributed information systems* International Journal of Electronics and Telecommunications (72). pp. 1-10. ISSN 2081-8491

[18] Kostiuk, Y., Skladannyi, P., Sokolov, V., Hulak, N., & Korshun, N. (2024). Models and algorithms for analyzing information risks during the security audit of personal data information system. In *Proceedings of the Third International Conference on Cyber Hygiene & Conflict Management in Global Information Networks (CH&CMiGIN'24)* (Vol. 3925, pp. 155–171). CEUR-WS.

[19] Zarreh, A., Zarreh, M., Wan, H.-D., & Saygin, C. (2024). Optimizing cybersecurity in cyber-physical manufacturing systems: A game-theoretic approach and quantal response equilibrium study. *Journal of Future Sustainability, 5*, 179–194. https://doi.org/10.5267/j.jfs.2025.9.002

[20] Kostiuk, Y., Skladannyi, P., Samoilenko, Y., Khorolska, K., Bebeshko, B., Sokolov, V. A system for assessing the interdependencies of information system agents in information security risk management using cognitive maps. Workshop on Third International Conference on Cyber Hygiene & Conflict Management in Global Information Networks, (CH&CMiGIN'24) January 24–27, 2024. Aachen: CEUR, 2024. Vol. 3925. P. 249-264. ISSN 1613-0073.

[21] Sezgin, A., Ulaş, M., & Boyacı, A. (2025). Multi-objective feature selection for intrusion detection systems: A comparative analysis of bio-inspired optimization algorithms. *Sensors, 25*(19), Article 6099. https://doi.org/10.3390/s25196099

[22] Skladannyi, P., Kostiuk Y., Khorolska, K., Bebeshko, B., Sokolov, V. Model and methodology for the formation of adaptive security profiles for the protection of wireless networks in the face of dynamic cyber threats. Proceedings of the Workshop Cyber Security and Data Protection, July 31, 2025, Lviv, Ukraine (CSDP 2025). Vol. 4042. P. 17–36. ISSN 1613-0073.

[23] Dwivedi, S., Shukla, A. K., Mishra, A., et al. (2026). Building robust internet of things defense system using multi-objective nature-inspired framework. *Discovery Computing, 29*, Article 11. https://doi.org/10.1007/s10791-025-09860-3

[24] Raeisi, Z., Maleki, H. R., & Akbari, R. (2025). An entropy-based multi-objective feature selection method for network intrusion detection. *Cluster Computing, 28*.

[25] Abdallah, M., Woods, D., Naghizadeh, P., Khalil, I., Cason, T., Sundaram, S., & Bagchi, S. (2021). Morshed: Guiding behavioral decision-makers towards better security investment in interdependent systems. In *Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security* (pp. 378–392).

[26] Kostiuk Y., Skladannyi P., Sokolov V., Zhyltsov O., Ivanichenko Y. Effectiveness of Information Security Control using Audit Logs. Proceedings of the Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS 2025), 2025. Aachen: CEUR, 2025. Vol. 3991. P. 524-538. ISSN 1613-0073

[27] Chen, Jing & Du, Tiantian & Xiao, Gongyi. (2021). A multi-objective optimization for resource allocation of emergent demands in cloud computing. Journal of Cloud Computing. 10. 10.1186/s13677-021-00237-7.

[28] Gorbachuk, V., Golotsukov, G., Dunaievskyi, M., Syrku, A., & Suleimanov, S.-B. (2023). Game theory and optimization models and methods to increase security of cyberinfrastructures. *Problems of Control and Informatics, 67*(2), 92–105. https://doi.org/10.34229/2786-6505-2022-2-6

[29] Tanak, S. K. (2025). Game theory applications in cybersecurity: An operations research approach. *Journal of Al-Qadisiyah for Computer Science and Mathematics, 17*(2), 96–109. https://doi.org/10.29304/jqcsm.2025.17.22213

[30] Doerr, B., & Qu, Z. (2023). A first runtime analysis of the NSGA-II on a multimodal problem. *IEEE Transactions on Evolutionary Computation, 27*(5), 1288–1297.

[31] Sokolov, V., Kostiuk, Y., Skladannyi, P., Korshun, N. (2025). Adaptation of Network Traffic Routing Policy to Information Security and Network Protection Requirements. Proceedings of the 13th International Scientific and Practical Conference "Information Control Systems and Technologies", ICST 2025, Vol-4048, P. 397 - 411. ISSN 1613-0073

[32] Zhengyin Chen, Jialong Li, Nianyu Li, Wenpin Jiao, and Eunsuk Kang. 2026. Context-Aware Proactive Self-Adaptation: A Two-Layer Model Predictive Control Approach. ACM Trans. Auton. Adapt. Syst. 21, 2, Article 13 (June 2026), 35 pages. https://doi.org/10.1145/3708998

[33] Yao, A., Huang, C., Zhang, W. *et al.* Enhancing cyber defense strategies with discrete multi-dimensional Z-numbers: a multi-attribute decision-making approach. *Complex Intell. Syst.* **11**, 216 (2025). https://doi.org/10.1007/s40747-025-01786-z

[34] Chen, L., Yang, J., Wang, P., Zhang, J., Wang, Q., Diao, X., & Dou, Z. (2025). Game-theoretic approach to cybersecurity risk assessment and protective strategy optimization in process industry production systems. *Computers & Chemical Engineering, 194*, Article 109034. https://doi.org/10.1016/j.compchemeng.2025.109034

[35] Ricciardi, L. A., Maddock, C. A., & Vasile, M. (2021). Multi-Objective Optimisation under Uncertainty with Unscented Temporal Finite Elements. *Mathematics*, *9*(23), 3010. https://doi.org/10.3390/math9233010

**УДК 004.056.**

***Skladannyi P., Kostiuk Y., Korshun N., Rzaeva S., Sokolov V.*** **Method for Optimizing Cybersecurity Strategies in Distributed Information Systems Based on NSGA-II Multi-Objective Optimization and Game Theory**

***Abstract.*** This paper presents a method for optimizing cybersecurity strategies in distributed information systems based on NSGA-II multi-objective optimization and game theory. The relevance of the study is driven by the growing number of cyber threats, the increasing complexity of distributed information system architectures, the continuous growth of processed data volumes, and the need to improve decision-making efficiency when developing cybersecurity strategies under resource constraints and dynamically changing cyber environment conditions. The study analyzes current approaches to ensuring cybersecurity in distributed information systems, risk assessment methods, multi-objective optimization techniques, and the application of game theory to strategic cybersecurity planning. It is established that existing approaches do not sufficiently consider the simultaneous influence of risk level, implementation cost of security mechanisms, effectiveness of cybersecurity measures, and potential attacker behavior when forming optimal cybersecurity strategies. A mathematical model for cybersecurity strategy optimization is proposed, combining multi-objective evaluation of alternatives using the NSGA-II algorithm with a game-theoretic model of strategic interaction between the cybersecurity system and the attacker. A system of optimization criteria is developed that takes into account risk level, costs of implementing security measures, the level of information resource protection, and incident response time. The architecture of a decision support system, the operational algorithm of the proposed method, and a procedure for generating a set of Pareto-optimal strategies are presented. A computational experiment was conducted for different operating scenarios of a distributed information system. The simulation results demonstrated a reduction in the overall risk level, improved effectiveness of cybersecurity strategies,

enhanced system adaptability to changing operating conditions, and advantages over traditional approaches. The obtained results confirm the feasibility of combining NSGA-II multi-objective optimization and game theory to support decision-making in the field of cybersecurity.
***Keywords:*** distributed information systems; cybersecurity; cybersecurity strategy; multi-objective optimization; NSGA-II; game theory; risk assessment; decision support system; computational experiment; intelligent methods.

**Складанний Павло Миколайович**, кандидат технічних наук, доцент, завідувач кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Київського столичного університету імені Бориса Грінченка.
**Pavlo Skladannyi**, PhD, Associate Professor, Head of the Department of Information and Cyber Security named after Professor Volodymyr Buryachok Borys Grinchenko Kyiv Metropolitan University.

**Костюк Юлія Володимирівна**, PhD, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Київського столичного університету імені Бориса Грінченка.
**Yuliia Kostiuk**, PhD, Associate Professor of the Department of Information and Cyber Security named after Professor Volodymyr Buriachok Borys Grinchenko Kyiv Metropolitan University.

**Коршун Наталія Володимирівна**, доктор технічних наук, професор, професор кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Київського столичного університету імені Бориса Грінченка.
**Nataliia Korshun**, PhD, Professor, Professor Department of Information and Cyber Security named after Professor Volodymyr Buryachok Borys Grinchenko Kyiv Metropolitan University.

**Рзаєва Світлана Леонідівна**, кандидат технічних наук, доцент, доцент кафедри комп'ютерних наук Київського столичного університету імені Бориса Грінченка.
**Rzaeva Svitlana,** Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of Computer Science Borys Grinchenko Kyiv Metropolitan University.

**Соколов Володимир Юрійович**, кандидат технічних наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Київського столичного університету імені Бориса Грінченка.
**Sokolov Volodymyr**, PhD, Associate Professor, Associate Professor Department of Information and Cyber Security named after Professor Volodymyr Buryachok Borys Grinchenko Kyiv Metropolitan University.

| Дата надходження: | Дата прийняття: | Дата публікації: |
|---|---|---|
| 19.06.2026 | 09.07.2026 | 21.08.2026 |