КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (27), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.27.751
УДК 004.9, 681.3, 519.86

Лахно Валерій Анатолійович
д.т.н., професор, професор кафедри комп'ютерних систем, мереж та кібербезпеки
Національний університет біоресурсів і природокористування України, Київ, Україна
ORCID ID: 0000-0001-9695-4543
lva964@nubip.edu.ua

Криворучко Олена Володимирівна
д.т.н., професор, професор кафедри комп'ютерних систем, мереж та кібербезпеки
Національний університет біоресурсів і природокористування України, Київ, Україна
ORCID ID: 0000-0002-7661-9227
ev_kryvoruchko@ukr.net

Каламан Єрболат Тлеуханули
магістр технічних наук кафедри кібербезпеки, обробки та зберігання інформації
Сатпаєвський університет, Алмати, Казахстан
ORCID ID: 0000-0002-8607-737X
politeh.kalaman@gmail.com

ПРОГРАМНА РЕАЛІЗАЦІЯ ВИРІШЕННЯ ЗАДАЧІ ОПТИМІЗАЦІЇ ВИБОРУ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ ЕВОЛЮЦІЙНОГО АЛГОРИТМУ

Анотація. Розроблено програмну реалізацію задачі багатокритеріальної оптимізації вибору засобів захисту інформації (ЗЗІ) для університетської комп'ютерної мережі на основі еволюційного алгоритму NSGA-II. Кібернетичну модель вибору оптимального набору ЗЗІ розглянуто з урахуванням множини критеріїв, включаючи вартість впровадження, рівень надійності та покриття актуальних загроз. Визначено цільові функції оптимізації, кожна з яких є функцією від дискретних змінних, описаних в літературі, і характеризує можливі конфігурації ЗЗІ. При програмній реалізації NSGA-II було реалізовано алгоритм генерації початкової популяції рішень з механізмами кросовера, мутації та селекції, що забезпечує ефективний пошук Парето-оптимальних конфігурацій, а також проведено обчислювальні експерименти, що демонструють вплив параметрів моделі на результат оптимізації, візуалізований на графіках. Отримано фронт Парето, що візуалізує компроміси між вартістю, надійністю та рівнем захисту. Отримані в ході дослідження результати в цілому підтверджують, що використання еволюційного алгоритму NSGA-II дозволяє досягти збалансованих рішень при проєктуванні системи інформаційної безпеки університетської мережі. Програмна реалізація багатокритеріальної оптимізації параметрів ЗЗІ для університетської мережі, представлена в статті, виконана мовою Python з використанням спеціалізованих бібліотек оптимізації та аналізу даних, забезпечуючи відтворюваність обчислювальних експериментів і можливість адаптації алгоритму для різних сценаріїв захисту розподілених обчислювальних систем.

Ключові слова: інформаційна безпека; еволюційні алгоритми; багатокритеріальна оптимізація; NSGA-II; Парето-оптимальність; університетська комп'ютерна мережа; вибір засобів захисту інформації; моделювання.

ВСТУП

Для оптимізації вибору засобів захисту інформації (ЗЗІ) для університетської комп'ютерної мережі (далі КМ) необхідно використовувати методи, що сприяють ефективному вирішенню багатокритеріальних задач з урахуванням обмежень за вартістю, надійністю та функціональністю засобів забезпечення кібербезпеки (КБ). Формалізована

задача відноситься до класу NP-важких, що виключає можливість застосування детермінованих алгоритмів з поліноміальною складністю для отримання точних рішень за прийнятний час. Враховуючи складність задачі та необхідність збалансованого пошуку компромісів між різними критеріями (такими як мінімізація витрат і максимізація захисту, як обговорювалося в [11]), класичні методи точної оптимізації, наприклад, динамічне програмування та методи гілок і меж, виявляються неефективними через експоненціальне зростання обчислювальної складності. Наближені методи, що базуються на евристиках і теорії нечітких множин, можуть призводити до субоптимальних рішень, не забезпечуючи необхідного рівня гарантованого захисту.

Постановка проблеми. Вибір оптимального набору засобів захисту інформації для університетської комп'ютерної мережі являє собою задачу багатокритеріальної оптимізації, ускладнену дискретною структурою рішень, наявністю конфліктуючих вимог та обмеженістю ресурсів. Класичні методи оптимізації виявляються неефективними через експоненціальне зростання обчислювальної складності, що вимагає використання наближених методів на основі еволюційних алгоритмів.

Аналіз останніх досліджень і публікацій. Аналіз існуючих методів багатокритеріальної оптимізації, проведений в роботах [1] – [5], дозволяє виділити еволюційні алгоритми як найбільш перспективний спосіб вирішення задачі. Зокрема, генетичні алгоритми (GA) та методи рою частинок (PSO) демонструють високу адаптивність і здатні ефективно обробляти багатовимірні простори рішень. Однак алгоритм оптимізації рою частинок більше підходить для задач неперервної оптимізації, в той час як для дискретних задач вибору ЗЗІ, що включають бінарні змінні та комбінаторні обмеження, потрібне використання більш спеціалізованих еволюційних методів.

Найбільш перспективним методом є багатокритеріальний генетичний алгоритм NSGA-II (Non-dominated Sorting Genetic Algorithm II), який був розроблений для ефективного вирішення задач з багатьма конфліктуючими критеріями. На відміну від традиційних генетичних алгоритмів, NSGA-II застосовує механізм не-домінуючого сортування та архівацію рішень на елітному фронті Парето, що дозволяє забезпечувати рівномірний розподіл множини рішень на межі Парето. Це має важливе значення для вибору оптимального набору ЗЗІ, оскільки дозволяє враховувати такі параметри, як вартість впровадження, ефективність нейтралізації загроз, надійність та сумісність з існуючою архітектурою КМ. Формальна постановка задачі в аспекті застосування NSGA-II передбачає визначення множини рішень (X) [6] – [10], де кожен можливий набір засобів захисту інформації являє собою вектор дискретних змінних. Функції цілі $f_i(X)$ визначаються для кожного критерію, наприклад, ми будемо розглядати з урахуванням викладок у [11], $f_1(X)$ — вартість системи захисту; $f_2(X)$ — інтегральний показник надійності, включаючи, в [11] модель розрахунку показників уразливості КМ, в якій на відміну від існуючих рішень враховано вплив на показники КБ вагових коефіцієнтів, що характеризують ефективність, включаючи вартісні характеристики, і надійність ЗЗІ на відповідних етапах блокування загроз для ІБ університетської КМ; $f_3(X)$ — покриття актуальних загроз для університетської КМ. Оптимізація виконується в багатокритеріальному просторі з метою мінімізації та/або максимізації відповідних показників, при цьому результатом роботи алгоритму є множина недомінованих рішень, що відповідають фронту Парето.

Переваги NSGA-II в контексті розв'язуваної задачі обумовлені його обчислювальною ефективністю, що забезпечується використанням механізму сортування за недомінованістю зі складністю $O(MN^2)$, де M — кількість цільових функцій, а N — розмір популяції. Також алгоритм використовує механізм crowding distance, що запобігає

збіжності до локальних рішень і забезпечує рівномірне покриття множини рішень. На відміну від альтернативних методів багатокритеріальної оптимізації, таких як MOEA/D (Multi-Objective Evolutionary Algorithm based on Decomposition) та SPEA2 (Strength Pareto Evolutionary Algorithm 2) [6], алгоритм NSGA-II не вимагає додаткових параметрів для декомпозиції простору задач, що робить його більш універсальним для застосування в задачах проєктування ІБ КМ.

Виходячи з сказаного, припускаємо, що вибір NSGA-II для вирішення задачі оптимізації структури системи захисту університетської КМ обумовлений його здатністю обробляти багатокритеріальні задачі з дискретними змінними, ефективним балансуванням компромісних рішень та високою обчислювальною стійкістю.

Мета статті. Розробка програмної реалізації методу багатокритеріальної оптимізації вибору ЗЗІ для університетської комп'ютерної мережі з використанням еволюційного алгоритму NSGA-II, що забезпечує знаходження Парето-оптимальної множини рішень з урахуванням витрат, надійності та покриття загроз.

Методи дослідження. Застосовується еволюційний алгоритм NSGA-II вибору оптимальної конфігурації ЗЗІ для університетської КМ, заснований на механізмі недомінуючого сортування рішень та архівування Парето-оптимальних конфігурацій. Розроблений алгоритм реалізовано на мові Python з використанням бібліотек для багатокритеріальної оптимізації, аналізу даних та візуалізації результатів. Проведено обчислювальні експерименти, що дозволяють оцінити вплив параметрів моделі на отримані рішення та виявити закономірності розподілу оптимальних конфігурацій.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

З урахуванням викладок [11] будемо вважати наступне.

У рамках задачі оптимізації структури системи захисту університетської КМ, див. рис. 1, цільові функції для подальшої програмної реалізації формалізуються так. Нехай множина рішень позначена як (X), де кожен можливий набір ЗЗІ представлений вектором двійкових змінних (x_{ij}), де $x_{ij} = 1$, якщо елемент j в класі i включений у рішення, і $x_{ij} = 0$ в іншому випадку. Перед програмною реалізацією вважаємо доцільним сформувати типові дані, що відображають використовувані класи та засоби захисту інформації (ЗЗІ) для КМ університету. Тобто кожен ЗЗІ у табл. 1–2 представлений своєю вартістю та набором загроз, проти яких він ефективний.

Коефіцієнт впливу α_{ij} показує, наскільки даний ЗЗІ підвищує захищеність вузла університетської КМ, а коефіцієнт уразливості V_{ij} відображає ступінь підверженості загрозам без даного ЗЗІ у складі КМ.

Зазначимо, що в процесі забезпечення безпеки критично важливих вузлів університетської КМ, яка використовується для навчальної діяльності, необхідно враховувати вплив застосовуваних ЗЗІ на рівень уразливості ключових серверних компонентів. Аналіз даного впливу представлений у табл. 2, де кожному вузлу КМ відповідає набір ЗЗІ, що характеризується коефіцієнтами впливу (α_{ij}) та вразливості (V_{ij}).

Таблиця 1

Приклади класів і ЗЗІ для типової КМ університету

Клас ЗЗІ (*i*)	Засіб захисту (*j*)	Вартість, ум. од. (P_{ij})
Міжмережеві екрани	Firewall A	500
	Firewall B	700
	Firewall C	400
	Firewall D	600
IDS/IPS системи	IDS A	600
	IDS B	800
SIEM системи	SIEM A	1000
	SIEM B	1200
Антивірусні рішення	AV A	300
	AV B	400
	AV C	500
	AV D	600

Таблиця 2

Вплив конкретного ЗЗІ на захист вузлів КМ ($f_2(X)$)

Вузол КМ (i)	Засіб захисту (j)	Коефіцієнт впливу (a_{ij})	Коефіцієнт уразливості (V_{ij})
Сервер БД	Firewall A	0.9	0.2
	IDS A	0.7	0.3
	SIEM A	0.8	0.1
Сервер застосунків	Firewall B	0.85	0.25
	IDS B	0.75	0.35
	SIEM B	0.9	0.15
І так далі	…	…	…

Сервер БД — це важливий компонент будь-якої університетської КМ, що забезпечує зберігання та обробку навчальних матеріалів, результатів успішності студентів, а також даних облікових записів користувачів. Відповідні ЗЗІ мають різні рівні впливу на зниження уразливості цього вузла. Наприклад, міжмережевий екран Firewall A демонструє високий коефіцієнт впливу при відносно низькій початковій уразливості, що зумовлено його здатністю обмежувати несанкціонований доступ на мережевому рівні.

В той же час система виявлення вторгнень IDS A характеризується дещо нижчим рівнем захисту, при цьому вразливість збільшується до 0.3, що пов’язано з її реактивним характером і залежністю від сигнатурних баз.

Засіб кореляційного аналізу подій безпеки SIEM A демонструє помірний баланс, підвищуючи стійкість системи за рахунок аналізу інцидентів, але не блокуючи атаки безпосередньо.

Сервер додатків підтримує функціонування освітніх платформ, онлайн-курсів і системи управління навчальним процесом. Його захист вимагає багаторівневого підходу, що включає фільтрацію трафіку, моніторинг активності користувачів та кореляцію подій. Тут Firewall B має підвищений рівень впливу, але при цьому початкова вразливість цього вузла вища, що зумовлено необхідністю обробки великої кількості зовнішніх запитів. IDS B характеризується меншою ефективністю, а вразливість зростає до 0.35, що пов’язано з потенційно високим рівнем хибних спрацьовувань та залежністю від повноти сигнатурних баз.

SIEM B демонструє максимальний вплив серед представлених рішень при мінімальному рівні вразливості, що зумовлено його можливістю здійснювати комплексний аналіз подій і передбачуване виявлення загроз.

Як було показано в [1], університетська КМ являє собою складну інфраструктуру, що включає безліч взаємопов'язаних вузлів, які забезпечують навчальний процес, наукові дослідження та адміністративне управління. Окрім серверів БД і серверів застосунків, критично важливими вузлами цієї системи є:

- сервер автентифікації та управління доступом, що відіграє ключову роль у забезпеченні безпеки університетської ІБ, оскільки він відповідає за ідентифікацію користувачів, управління обліковими записами та контроль прав доступу;
- сервер зберігання даних (файловий сервер, NAS, SAN), що забезпечує централізоване зберігання та доступ до навчальних матеріалів, наукових даних, резервних копій та персональних файлів користувачів;
- сервер віртуалізації та хмарної інфраструктури, для роботи з університетською хмарою;
- сервер дистанційного навчання (LMS-сервер), що підтримує платформи дистанційного навчання (Moodle, Blackboard, Canvas), забезпечуючи доступ до освітніх матеріалів, онлайн-курсів та тестування;
- мережеве обладнання (маршрутизатори, комутатори, точки доступу Wi-Fi);
- сервер наукових обчислень (HPC-кластер), що обслуговує обчислювально інтенсивні задачі, пов'язані з науковими дослідженнями, моделюванням та аналізом даних.

Тобто результати, результати аналізу даних табл. 2 показують, що застосування міжмережевих екранів ефективно знижує атаковану поверхню університетської КМ, однак для повноцінного захисту необхідна інтеграція з системами виявлення вторгнень та кореляції подій. Включення багатокомпонентного підходу дозволить нам досягти компромісу між проактивними та реактивними заходами захисту, мінімізуючи потенційні загрози для критичних вузлів системи.

Для розробки викладеного вище оптимізаційного алгоритму підбору ЗЗІ у КМ університету була обрана мова програмування Python, а як інтегроване середовище розробки (IDE) — Visual Studio Code (VS Code). Вибір обумовлений низкою факторів, що включають обчислювальну ефективність, гнучкість, розвинену екосистему, підтримку профільних бібліотек, а також зручність розробки та налагодження складних алгоритмічних конструкцій. Python є інтерпретованою високорівневою мовою програмування, широко використовуваною в наукових дослідженнях, математичному моделюванні та задачах ІБ. Його синтаксична лаконічність і потужні інструменти для роботи з даними дозволяють ефективно реалізовувати алгоритми оптимізації без надмірного ускладнення програмного коду. Для задач, пов'язаних з математичним програмуванням, оптимізацією та аналізом даних, у Python існує розвинений ансамбль спеціалізованих бібліотек, включаючи NumPy, SciPy, Pandas, PuLP, CVXPY та NetworkX, а ці інструменти забезпечують можливість розв'язання задач лінійного та нелінійного програмування, комбінаторної оптимізації, побудови моделей загроз і вразливостей, а також аналізу графів, що необхідно при моделюванні структури КМ та виявленні точок концентрації ризиків.

Ще одним ключовим аспектом є інтеграція Python з інструментами машинного навчання (МН) та аналізу великих даних, такими як Scikit-learn, TensorFlow, PyTorch і XGBoost, що надає нам потенційні можливості для застосування методів інтелектуального аналізу даних (ІАД) та автоматизованого виявлення аномалій у мережевому трафіку університету, і необхідно для задач ІБ університетських КМ. Крім того, підтримка багатопотокового та асинхронного програмування дозволить ефективно

ISSN 2663 - 4023

управляти обчислювальними ресурсами при обробці складних симуляційних сценаріїв та моделюванні атак на КМ.

Вибір середовища розробки VS Code, див. рис. 2, був обумовлений її високою продуктивністю, розширюваністю та підтримкою широкого спектра інструментів для Python-розробки. VS Code має вбудовану підтримку Jupyter Notebook, що значно спрощує прототипування та налагодження, наприклад, оптимізаційних математичних моделей, розглянутих у статті. Розширення для роботи з контейнерами Docker та віртуальними оточеннями (наприклад, venv, Conda) дозволяють нам ізолювати залежності проєкту та забезпечувати відтворюваність обчислювальних експериментів (ОЕ), представлених нижче у статті. Інтеграція з системами контролю версій (Git) полегшить ведення нашого дослідницького проєкту, а вбудований термінал і підтримка налагоджувачів (PDB, Debugpy) дозволять аналізувати поведінку алгоритму NSGA-II на різних етапах їх виконання.

Вважаємо, що поєднання Python і VS Code — це оптимальний вибір для реалізації описаного оптимізаційного алгоритму підбору ЗЗІ в КМ університету, що забезпечує баланс між обчислювальною потужністю, зручністю розробки та можливостями інтеграції з інструментами аналізу даних і кібербезпеки.

Загальний вигляд вікна VS Code в процесі розробки програмного продукту (ПП) для вирішення задачі оптимізації вибору ЗЗІ для університетської КМ, показаний на рис. 1.

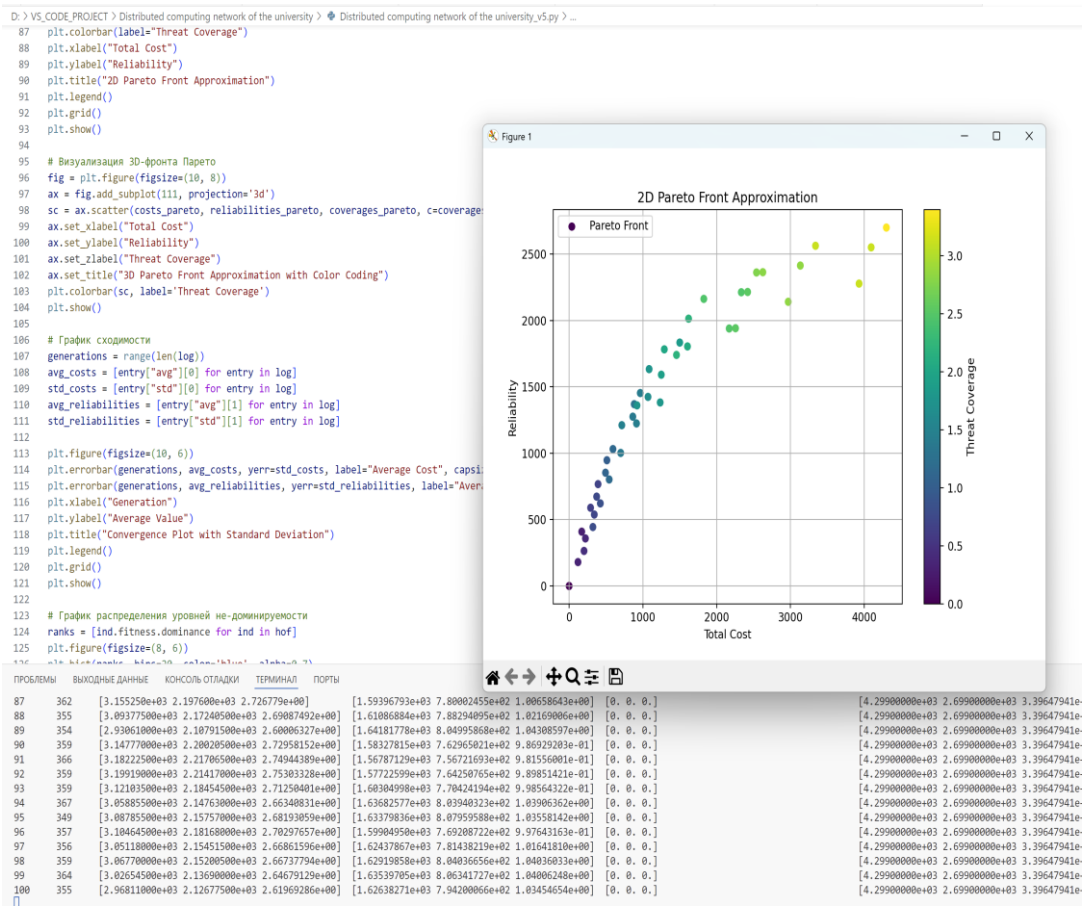

Рис. 1. Загальний вигляд вікна VS Code в процесі розробки програмного продукту для вирішення задачі оптимізації вибору засобів захисту інформації університетської розподіленої обчислювальної мережі

Відзначимо, що проведення обчислювальних експериментів (ОЕ) є необхідним етапом для верифікації та апробації розробленої моделі та ПП для оптимізації вибору ЗЗІ в університетській КМ. Дані ОЕ загалом дозволяють не лише оцінювати коректність та ефективність запропонованої моделі та ПП, але й виявити закономірності, що визначають вплив різних факторів на прийняті рішення. В умовах багатокритеріальної оптимізації, що включає параметри вартості, надійності та рівня покриття загроз, математичне моделювання з варіюванням вхідних даних забезпечить нам можливість вивчення компромісів між цими показниками.

Необхідність ОЕ також була обумовлена специфікою захищуваної системи. Університетська КМ за своєю природою є відкритою, накладаючи додаткові вимоги до адаптивності засобів захисту, їх масштабованості та здатності функціонувати в умовах високої змінності користувацької активності. Тому дослідження різних сценаріїв ефективності ЗЗІ в таких умовах вимагає побудови параметризованих моделей, що забезпечують відтворюваність і формалізацію прийнятих рішень. Також ОЕ дозволили в ході дослідження протестувати різні версії ПП, виявляючи їх ефективність на реальних даних, наданих університетами РК. Відповідно, формування за допомогою розробленого ПП множини Парето та аналіз отриманих компромісних рішень надали нам можливість адаптивного вибору оптимального набору ЗЗІ, що враховує специфіку університетської мережі.

У табл. 3 представлені основні етапи проведених ОЕ.

Таблиця 3

Основні етапи проведених ОЕ

Етап	Опис	Результат
1	Формування множини альтернативних рішень на основі доступних засобів захисту інформації (ЗЗІ).	Список можливих конфігурацій ЗЗІ із заданими параметрами.
2	Визначення множини загроз, характерних для університетської розподіленої мережі.	Класифікація загроз та їх відповідність категоріям атак.
3	Формування багатокритеріальної функції вартості, надійності та покриття загроз.	Чітка формалізація критеріїв оптимізації.
4	Застосування методу багатокритеріальної оптимізації (наприклад, NSGA-II) для знаходження Парето-оптимальних рішень.	Набір компромісних рішень, що забезпечують баланс між вартістю, надійністю та покриттям загроз.
5	Візуалізація результатів у вигляді 3D-графіка та їх інтерпретація.	Аналіз компромісних рішень, виявлення закономірностей.
6	Валідація отриманих рішень на реальних даних.	Підтвердження застосовності моделі для вибору ЗЗІ в університетській мережі.

У табл. 4 наведені варійовані параметри та їх діапазони під час обчислювальних експериментів.

Як зазначалося в попередньому параграфі, у процесі багатокритеріальної оптимізації вибору ЗЗІ для КМ ми використовували різні критерії. Діапазони їх значень визначалися на основі апріорного аналізу характеристик системи, експертних оцінок і методик нормалізації, що дозволяють привести дані до зручного для аналізу масштабу.

Таблиця 4

Основні етапи проведених ОЕ

Параметр	Діапазон значень	Пояснення (в задачі вибору ЗЗІ для університетської мережі)
Загальна вартість впровадження ($)	0 – 5000	Залежить від бюджету університету на ІБ.
Надійність (дні до відмови ЗЗІ у складі РВС)	0 – 3000	Напрацювання до відмови у функціонуванні ЗЗІ
Покриття загроз (індекс)	0 – 5	Рівень захищеності від специфічних загроз, див. таблицю 3.5.
Кількість вузлів мережі	10 – 500	Кількість кінцевих пристроїв і серверів. Залежить від масштабу навчального закладу.
Число активних користувачів	500 – 20 000	Кількість студентів, викладачів та співробітників, які працюють у мережі. (допоміжні дані, що впливають на максимізацію покриття актуальних загроз для університетської КМ).
Процент шкідливого трафіку	0.1 – 5	Визначає рівень фонових атак та аномальної поведінки

Перший критерій — вартість — вимірюється в умовних одиницях і варіюється в межах від 0 до 5000 у.о. Такий діапазон обумовлений тим, що він відображає типові витрати на реалізацію системи захисту в розглянутому класі об’єктів, таких як університетські КМ. Верхня межа в 5000 у.о. відповідає граничному рівню фінансових вкладень, за яким економічна ефективність додаткових заходів захисту суттєво знижується, а також враховує бюджетні обмеження подібних організацій. Нижня границя в 0 представляє гіпотетичний випадок відсутності витрат, що дозволяє розглядати повне ігнорування заходів безпеки як одну з граничних точок рішення. Інтегральний показник надійності змінюється в межах від 0 до 3000 (у днях). Такий діапазон обрано в результаті аналізу захищеності КМ, де надійність є функцією від характеристик системи захисту інформації, ймовірності успішного функціонування механізмів виявлення та блокування загроз, а також загального рівня стійкості до атак. Використання шкали з верхньою межею 3000 дозволяє враховувати градієнт змін надійності між різними наборами засобів захисту, при цьому забезпечуючи адекватну чутливість методу до змін параметрів. Значення 0 означає повну ненадійність системи, коли заходи захисту відсутні або не функціонують.

Покриття актуальних загроз для університетської розподіленої обчислювальної системи приймає значення в діапазоні від 0 до 5. На відміну від класичних бінарних метрик (наприклад, «загроза усунена» або «не усунена»), тут застосовується шкала, що враховує ступінь покриття атак, виражену через комплексну оцінку ефективності застосовуваних рішень. При цьому нульове значення означає повну відсутність захисту від загроз, тоді як верхнє значення 5 відповідає максимальному покриттю атак, визначеному на основі експертизи в області кібербезпеки університетських ІТ-систем. Такий діапазон враховує специфіку освітніх обчислювальних середовищ, де загрози можуть мати різну критичність залежно від категорії користувачів та використовуваних сервісів.

Вибір зазначених діапазонів також пов’язаний з необхідністю приведення показників до зручного масштабу, що дозволяє коректно застосовувати алгоритми багатокритеріальної оптимізації, включаючи NSGA-II. Ці діапазони відповідають результатам нормалізації вихідних даних, забезпечують зручну інтерпретацію рішень і дозволяють уникнути перекосу ваг критеріїв у процесі обчислень.

ISSN 2663 - 4023

На рис. 2 показана отримана за допомогою розробленого програмного продукту (ПП) двовимірна апроксимація фронту Парето для множини рішень, що характеризуються показниками загальної вартості та надійності ЗЗІ для університетської КМ. По осі абсцис відкладено значення загальної вартості ЗЗІ, вимірюване в умовних одиницях (щоб не прив'язуватися до національних валют), а по осі ординат — показник надійності, виражений у відповідних числових значеннях. Кожна точка на графіку представляє одне з оптимальних рішень, що належать до фронту Парето, означаючи, що кожне з цих рішень є не покращуваним одночасно за обома критеріями.

Кольорове кодування точок на рис. 2 здійснюється відповідно до додаткової метрики, позначеної в легенді як «Threat Coverage», що інтерпретується як ступінь покриття загроз, характерних для КМ університету.

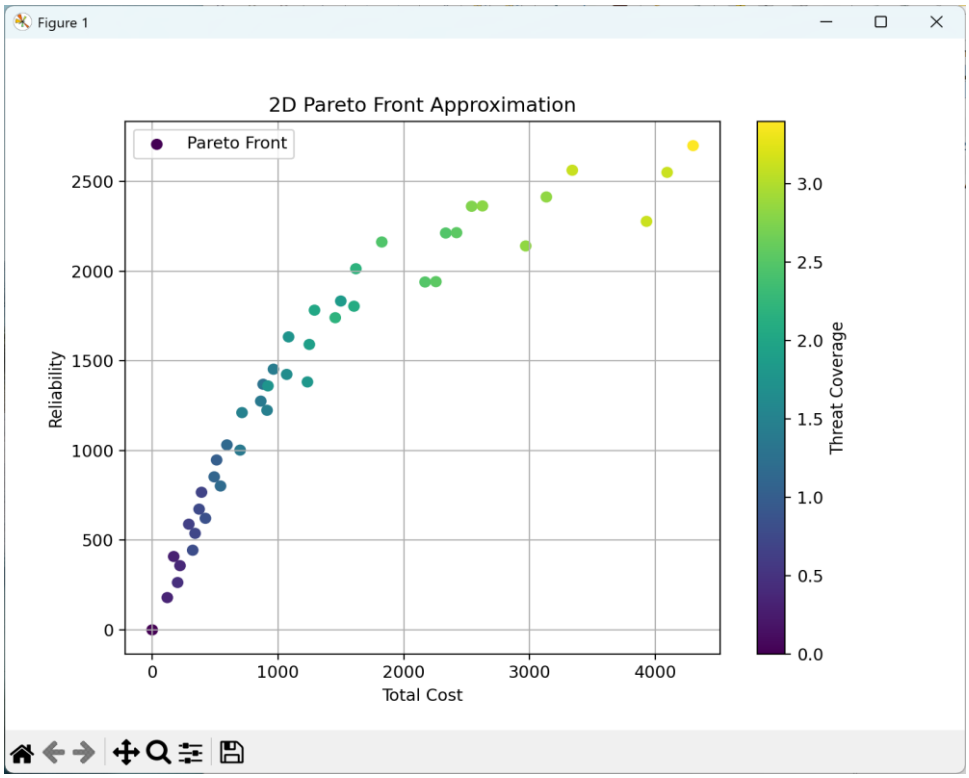

Рис. 2. Двовимірна апроксимація фронту Парето для множини рішень, що характеризуються показниками загальної вартості та надійності ЗЗІ для університетської КМ

Градієнтна шкала від фіолетового до жовтого кольорів демонструє рівень цієї метрики, дозволяючи аналітично оцінити розподіл рішень не лише в просторі витрат і надійності, але й з урахуванням рівня покриття загроз для КМ. Аналіз графіка дозволив зробити висновок про наявність характерного компромісу, тобто збільшення надійності супроводжується зростанням витрат, при цьому рішення з вищим покриттям загроз, як правило, розташовуються в області з найбільшими значеннями загальної вартості ЗЗІ на КМ.

Загальний аналіз даних дозволяє нам зробити висновок про те, що підвищення витрат на систему захисту КМ сприяє як збільшенню охоплення загроз, так і підвищенню надійності, проте при досягненні певного рівня приріст показників починає сповільнюватися, підтверджуючи необхідність балансування інвестицій у захисні заходи, оптимізуючи їх з урахуванням граничної ефективності ЗЗІ для університетської КМ.

ВИСНОВКИ

Виконана програмна реалізація моделі для багатокритеріальної оптимізації ЗЗІ для університетської КМ з використанням алгоритму NSGA-II на мові Python, що забезпечує можливість автоматизованого вибору оптимального набору ЗЗІ для університетської КМ і задіяний алгоритм генерації початкової популяції рішень, що реалізує механізми кросовера, мутації та селекції з урахуванням бюджетних обмежень і структурних особливостей університетських КМ. Виконані обчислювальні експерименти (ОЕ), в ході яких проведено аналіз динаміки збіжності рішення, розподілу Парето-оптимальних конфігурацій та впливу різних факторів на результати оптимізації. В ході ОЕ встановлено, що збільшення витрат на ЗЗІ корелює з підвищенням рівня надійності та покриття загроз, однак спостерігається ефект насичення, при якому подальше збільшення вкладень у захист КМ не призводить до значного покращення захисних характеристик системи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Lakhno, V., Maliukov, V., Komarova, L., Kasatkin, D., Osypova, T., & Chasnovskyi, Y. (2022). Optimization of information protection means placement based on the application of genetic algorithm. *Electronic professional scientific publication "Cybersecurity: education, science, technology", 1(17),* 6–20. https://doi.org/10.28925/2663-4023.2022.17.620
2. Androschuk, O. S., & Kudin, A. M. (2012). Multi-criteria model for choosing the architecture of a fuzzy logical inference system when analyzing information security risks in cloud computing and other complex systems. *Artificial Intelligence*, 529–534.
3. Yezhova, L. F., Skachek, L. M., & Khoroshko, V. O. (2013). Multi-criteria optimization of information security systems. *Modern Special Technology, (1),* 108–114.
4. Zhdanova, Yu., Shevchenko, S., Spasitelyeva, S., & Sokulsky, O. (2024). Decision-making based on linear optimization in the process of information security risk management. *Electronic professional scientific publication "Cybersecurity: education, science, technology", 1(25),* 330–343. https://doi.org/10.28925/2663-4023.2024.25.330343
5. Kornienko, B. Ya., & Galata, L. P. (2019). Optimization of the corporate network information protection system. Mathematical and computer modeling. *Series: Technical Sciences,* 56–62. https://doi.org/10.32626/2308-5916.2019-19.56-62
6. Junior, M. A. B., de Lima Neto, F. B., & Marwala, T. (2012, June). Optimizing risk management using NSGA-II. *2012 IEEE Congress on Evolutionary Computation*, 1–8.
7. Tamimi, A., Naidu, D.S., & Kavianpour, S. (2015). An Intrusion detection system based on NSGA-II Algorithm. *2015 Fourth International Conference on Cyber Security, Cyber Warfare, and Digital Forensic (CyberSec),* 58-61.
8. Verma, S., Pant, M., & Snasel, V. (2021). A comprehensive review on NSGA-II for multi-objective combinatorial optimization problems. *IEEE Access, 9,* 57757–57791.
9. De Almeida, E. M., & Asada, E. N. (2015). NSGA-II applied to the multi-objective Distribution System Expansion Planning problem. *2015 18th International Conference on Intelligent System Application to Power Systems (ISAP),* 1–6.
10. Fang, X., Wang, W., He, L., Huang, Z., Liu, Y., & Zhang, L. (2018). Research on Improved NSGA-II Algorithm and Its Application in Emergency Management. *Mathematical Problems in Engineering, 2018(1),* 1306341.
11. Lakhno, V., Alimseitova, Z., Kalaman, Y., Kryvoruchko, O., Desiatko, A., & Kaminskyi, S. (2023). Development of an information security system based on modeling distributed computer network vulnerability indicators of an informatization object. *International Journal of Electronics and Telecommunications, 69.* http://dx.doi.org/10.24425/ijet.2023.146495
12. Hulak, H. M., Zhiltsov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2024). *Information and cyber security of the enterprise. Textbook.* Lviv: Publisher Marchenko T. V.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (27), 2025
ISSN 2663 - 4023

Valerii Lakhno
Doctor of Technical Sciences, Professor
Department of Computer Systems, Networks and Cybersecurity
National University of Life and Environmental Sciences of Ukraine, Kiev, Ukraine
ORCID ID: 0000-0001-9695-4543
lva964@nubip.edu.ua

Olena Kryvoruchko
Doctor of Technical Sciences, Professor
Department of Computer Systems, Networks and Cybersecurity
National University of Life and Environmental Sciences of Ukraine, Kiev, Ukraine
ORCID ID: 0000-0002-7661-9227
kryvoruchko_ev@knute.edu.ua

Yerbolat Kalaman
Master of engineering and technology, Master of Technical Sciences
Department of Cybersecurity, Information Processing and Storage
Satpayev University, Almaty, Kazakhstan
ORCID ID: 0000-0002-8607-737X
politeh.kalaman@gmail.com

SOFTWARE IMPLEMENTATION OF THE PROBLEM OF OPTIMIZING THE CHOICE OF INFORMATION PROTECTION MEANS BASED ON AN EVOLUTIONARY ALGORITHM

Abstract. A software implementation of the problem of multi-criteria optimization of the selection of information protection means (IPS) for a university computer network has been developed based on the evolutionary algorithm NSGA-II. A cybernetic model for selecting the optimal set of IPS has been considered taking into account a set of criteria, including the cost of implementation, the level of reliability, and coverage of current threats. Optimization objective functions have been determined, each of which is a function of discrete variables described in the literature and characterizes possible IPS configurations. In the software implementation of NSGA-II, an algorithm for generating the initial population of solutions with crossover, mutation, and selection mechanisms was implemented, which provides an effective search for Pareto-optimal configurations, and computational experiments were also conducted to demonstrate the influence of model parameters on the optimization result visualized on graphs. A Pareto front was obtained, which visualizes the trade-offs between cost, reliability, and level of protection. The results obtained during the study generally confirm that the use of the evolutionary algorithm NSGA-II allows achieving balanced solutions when designing an information security system for a university network. The software implementation of multi-criteria optimization of the ISI parameters for a university network, presented in the article, is implemented in the Python language using specialized optimization and data analysis libraries, ensuring the reproducibility of computational experiments and the ability to adapt the algorithm for various scenarios of protecting distributed computing systems.

Keywords: information security; evolutionary algorithms; multi-criteria optimization; NSGA-II; Pareto-optimality; university computer network; selection of information protection tools; modeling.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Lakhno, V., Maliukov, V., Komarova, L., Kasatkin, D., Osypova, T., & Chasnovskyi, Y. (2022). Optimization of information protection means placement based on the application of genetic algorithm. *Electronic professional scientific publication "Cybersecurity: education, science, technology", 1(17),* 6–20. https://doi.org/10.28925/2663-4023.2022.17.620
2. Androschuk, O. S., & Kudin, A. M. (2012). Multi-criteria model for choosing the architecture of a fuzzy logical inference system when analyzing information security risks in cloud computing and other complex systems. *Artificial Intelligence*, 529–534.

3. Yezhova, L. F., Skachek, L. M., & Khoroshko, V. O. (2013). Multi-criteria optimization of information security systems. *Modern Special Technology, (1),* 108–114.
4. Zhdanova, Yu., Shevchenko, S., Spasitelyeva, S., & Sokulsky, O. (2024). Decision-making based on linear optimization in the process of information security risk management. *Electronic professional scientific publication "Cybersecurity: education, science, technology", 1(25),* 330–343. https://doi.org/10.28925/2663-4023.2024.25.330343
5. Kornienko, B. Ya., & Galata, L. P. (2019). Optimization of the corporate network information protection system. Mathematical and computer modeling. *Series: Technical Sciences,* 56–62. https://doi.org/10.32626/2308-5916.2019-19.56-62
6. Junior, M. A. B., de Lima Neto, F. B., & Marwala, T. (2012, June). Optimizing risk management using NSGA-II. *2012 IEEE Congress on Evolutionary Computation*, 1–8.
7. Tamimi, A., Naidu, D.S., & Kavianpour, S. (2015). An Intrusion detection system based on NSGA-II Algorithm. *2015 Fourth International Conference on Cyber Security, Cyber Warfare, and Digital Forensic (CyberSec),* 58-61.
8. Verma, S., Pant, M., & Snasel, V. (2021). A comprehensive review on NSGA-II for multi-objective combinatorial optimization problems. *IEEE Access, 9,* 57757–57791.
9. De Almeida, E. M., & Asada, E. N. (2015). NSGA-II applied to the multi-objective Distribution System Expansion Planning problem. *2015 18th International Conference on Intelligent System Application to Power Systems (ISAP),* 1–6.
10. Fang, X., Wang, W., He, L., Huang, Z., Liu, Y., & Zhang, L. (2018). Research on Improved NSGA-II Algorithm and Its Application in Emergency Management. *Mathematical Problems in Engineering, 2018(1),* 1306341.
11. Lakhno, V., Alimseitova, Z., Kalaman, Y., Kryvoruchko, O., Desiatko, A., & Kaminskyi, S. (2023). Development of an information security system based on modeling distributed computer network vulnerability indicators of an informatization object. *International Journal of Electronics and Telecommunications, 69.* http://dx.doi.org/10.24425/ijet.2023.146495
12. Hulak, H. M., Zhiltsov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2024). *Information and cyber security of the enterprise. Textbook.* Lviv: Publisher Marchenko T. V.