КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (13), 2021
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2021.13.1628
УДК 004.946.5.056

Чубаєвський Віталій Іванович
кандидат політичних наук, доцент, доцент кафедри інженерії програмного забезпечення та кібербезпеки
Київський національний торговельно-економічний університет, м.Київ, Україна
ORCID ID: 0000-0001-8078-2652
chubaievskyi_vi@knute.edu.ua

Лахно Валерій Анатолійович
доктор технічних наук, професор, завідувач кафедри комп'ютерних систем та мереж
Національний університет біоресурсів і природокористування України, м.Київ, Україна
ORCID ID: 0000-0001-9695-4543
lva964@gmail.com

Криворучко Олена Володимирівна
доктор технічних наук, професор, завідувач кафедри інженерії програмного забезпечення та кібербезпеки
Київський національний торговельно-економічний університет, м.Київ, Україна
ORCID ID: 0000-0002-7661-9227
kryvoruchko_ev@knute.edu.ua

Касаткін Дмитро Юрійович
кандидат педагогічних наук, доцент, доцент кафедри комп'ютерних систем та мереж
Національний університет біоресурсів і природокористування України, м.Київ, Україна
ORCID ID: 0000-0002-2642-8908
dm_kasat@ukr.net

Десятко Альона Миколаївна
PhD in Computer Sciences, доцент кафедри інженерії програмного забезпечення та кібербезпеки
Київський національний торговельно-економічний університет, м.Київ, Україна
ORCID ID: 0000-0003-2860-2188
desyatko@knute.edu.ua

Блозва Андрій Ігорович
кандидат педагогічних наук, доцент, доцент кафедри комп'ютерних систем та мереж
Національний університет біоресурсів і природокористування України, м.Київ, Україна
ORCID ID: 0000-0002-4377-0916
andriy.blozva@nubip.edu.ua

Гусєв Борис Семенович
кандидат технічних наук, доцент, доцент кафедри комп'ютерних систем та мереж
Національний університет біоресурсів і природокористування України, м.Київ, Україна
ORCID ID: 0000-0003-1658-7822
gusevbs@gmail.com

МЕТОДИКА МІНІМІЗАЦІЇ ВИТРАТ НА ПОБУДОВУ БАГАТОКОНТУРНОЇ СИСТЕМИ ЗАХИСТУ НА ОСНОВІ ГЕНЕТИЧНОГО АЛГОРИТМУ

Анотація. У статті викладена методика багатокритеріальної оптимізації витрат на систему захисту інформації об'єкта інформатизації. Методика базується на застосуванні модифікованого генетичного алгоритму VEGA. Запропоновано модифікований алгоритм рішення задачі БКО параметрів багатоконтурною системи захисту інформації об'єкта інформатизації, який дозволяє обґрунтовувати оптимальні параметри компонентів СЗІ з урахуванням обраних експертом пріоритетних метрик кібербезпеки ОБІ. На відміну від існуючого класичного алгоритму VEGA, в модифікованому алгоритмі додатково застосовані принцип Парето, а також новий механізм селекції примірників популяції.

Принцип Парето застосовується для кращої точки. У цій точці рішення, трактуються як найкращі, якщо за однією з метрик кібербезпеки є поліпшення, а по інший метриці (або метриках) буде відповідно не гірше. Новий механізм селекції на відміну від традиційної, передбачає створення проміжної популяції. Формування проміжної популяції відбувається в кілька етапів. На першому етапі перша половина популяції формується на основі метрики - частка вразливостей об'єкта інформатизації, які усунуті в установлені терміни. На другому етапі друга половина проміжної популяції формується на основі метрики - частка ризиків, які неприпустимі для інформаційних активів об'єкта інформатизації. Далі ці частини проміжної популяції змішуються. Після змішування формується масив номерів і виробляється змішування. На заключному етапі селекції для схрещування будуть братися екземпляри (індивіди) за номером з цього масиву. Номери вибираються випадково. Ефективність застосування даної методики підтверджена практичними результатами

Ключові слова: захист інформації; кібербезпека; контури захисту, багатокритеріальна оптимізація; генетичний алгоритм

ВСТУП

В міру ускладнення сценаріїв кібератак на об'єкти інформатизації (ОБІ) організація функціонування багатоконтурних систем захисту інформації (СЗІ) вимагає синхронізувати роботу всіх компонентів, які складають як всю систему захисту в цілому, так і окремих її складових на кожному з рубежів захисту. Рішення такого складного завдання вимагає розробки нових і вдосконалення існуючих алгоритмів, що описують зміну ситуації з захистом ОБІ, у міру зміни поточної обстановки.

Постановка проблеми.

Розробка моделі та алгоритму мінімізації затрат на побудову багатоконтурної системи захисту інформації об’єкту інформатизації.

Аналіз останніх досліджень і публікацій. Збільшення кількості і складності успішно реалізованих кібератак на різні ОБІ [1, 2] породжує потребу в якісно нових процедурах формування складу комплексів СЗІ та кібербезпеки (КБ) для всіх контурів захисту інформаційних масивів ОБІ. Задача, що не втрачає актуальність формування ефективних контурів захисту інформації (ЗІ) та КБ ОБІ породила безліч теоретичних і прикладних досліджень, присвячених питанням оптимізації складу СЗІ та КБ [3, 4].

У подібних завданнях, необхідно знаходити допустимі парето-оптимальні рішення для комплексів СЗІ. Рішення такого завдання є невід'ємною частиною процедури побудови багатоконтурних СЗІ в умовах зростання кількості спроб деструктивних впливів на ОБІ різного масштабу. А рішення подібних задач виконується на базі не тільки класичних процедур багатокритеріальної оптимізації (БКО), але і більш універсальних методів. Зокрема, до таких методів можна віднести різні варіації генетичного алгоритму (ГА), який довів свою ефективність при вирішенні великого кола складних завдань [5, 6].

Зауважимо, що ефективність ГА залежить від ретельної настройки та контролю їх параметрів. Доцільність застосування ГА диктується ситуацією, при якій, крім традиційної БКО завдання вибору складу СЗІ для ОБІ, розглядаються і різні метрики оцінювання ефективності застосування окремих складових засобів захисту інформації по контурах кібербезпеки ОБІ. А крім того, ще необхідно враховувати величини ризиків, вартісні показники відібраних засобів захисту інформації, виходячи зі специфіки конкретних інформаційних активів - бази даних, бази знань, пошти, сайту та ін.

В [7] показано, що ГА, які можуть бути використані в ході рішення БКО завдань, є варіаціями еволюційних методів пошуку. Так, в [8], наприклад, розглянута модель,

відповідно до якої створюється популяція елементів СЗІ (особин). Для пошуку найкращого рішення автори використовують власну цільову функцію. Однак, в даному дослідженні не було вказано яким чином на практиці використовуються пропоновані рішення на практиці.

В [9, 10] були досліджені ГА, які можна віднести до двох груп. Бінарне кодування детально розглянуто в [10, 11]. Дійсне кодування розглянуто в роботах [12, 13]. Зокрема, в [12], показано, що в першій групі можна домогтися більш високої ефективності пошуку екстремального значення на безлічі допустимих рішень.

В [14] показано, що постійна мутація об'єктів використовується в більшості реалізацій ГА. В даному випадку варіювання змінними буде більш гнучким. Це дозволяє знаходити початкові рішення вже на досить ранніх стадіях роботи ГА, без великої кількості його прогонів. Однак в [12-14] програмна реалізація ГА не була представлена.

У роботах [15, 16] показано, що змінна мутація виглядає краще з точки зору пошуку глобального оптимуму. Дані роботи також не містять опис програмної реалізації.

В [17, 18] аналізуються особливості використання модифікованого ГА (МГА) в БКО завданнях. Відмінність МГА полягає в тому, що тут під час роботи алгоритму як фітнес-функції застосовувалася не сума ефективностей СЗІ, а використовувалася сума відносин ефективностей до обмежуючим характеристикам СЗІ. По суті даний МГА не що інше як диз'юнкція стандартного ГА і жодного алгоритму.

У роботах [19, 20] розглядається можливість зменшення кількості параметрів, що настроюються ГА. Пропоновані авторами рішення, на відміну від стандартних, не містять оператор схрещування. Рішення отримано на основі статистичної інформації про пошуковому просторі.

У роботах [17, 20] показано, що стандартні і модифіковані ГА досить ефективні для вирішення більшості складних оптимізаційних задач [21] і є перспективними для подальшого вивчення і вдосконалення.

Все вище сказане і зумовило релевантність нашого дослідження.

Мета статті. Мета дослідження - розробка методики мінімізації витрат на побудову багатоконтурною системи захисту інформації шляхом підбору оптимальних параметрів окремих компонентів кібербезпеки

Завдання дослідження:

1. Розробити методику багатокритеріальної оптимізації витрат на СЗІ ОБІ на основі генетичного алгоритму.

2. Адаптація многокритеріального генетичного алгоритму VEGA до знаходження оптимальних значень цільових функцій СЗІ. Вважаємо, що цільові функції СЗІ, визначають зв'язок між ймовірними вхідними впливами на окремі компоненти захисту ОБІ і його вихідними параметрами.

МЕТОДИКА ДОСЛІДЖЕННЯ

Для вирішення сформульованої задачі запропоновано використовувати генетичний алгоритм. Рішення виконано на основі загального еволюційного алгоритму і його складових багатокритеріальних ГА. Основним при цьому став метод VEGA - Vector Evaluted Genetic Algorithm [1,2].

Даний метод передбачає розширення традиційного ГА, яке реалізовано шляхом застосування векторних оцінок ступеня придатності екземплярів (індивідуумів), а також можливостей паралельно оцінювати популяції по кожному з критеріїв окремо,

наприклад, для кожного з компонентів СЗІ це можуть бути - ефективність, масштабованість, вартість, технічна підтримка.

Таким чином можна реалізувати одночасну оптимізацію всіх контурів захисту об'єкта інформатизації відповідно до заданих цільовими функціями.

На початковому етапі роботи МГА є дві батьківські хромосоми. У двох випадковим чином вибраних місцях виконуються розриви між позиціями генів. На рисунку 1 розриви показані штрихпунктирною червоною лінією.

Рис. 1. Схема двоточкового перетину

Далі відбувається обмін частин між хромосомами. Як результат утворюються два нащадка. З нащадків вибирається випадковим чином один нащадок, який передається як результат оператора схрещування.

Далі переходимо до оператора мутації - випадкової зміни всіх нащадків популяції. Мета мутації є зробити більш різноманітним аналізовані в результаті виконання завдання індивідууми (екземпляри).

В ході мутації, схема якої показана на малюнку 2, гени кожного примірника з деякою заданою вірогідністю мутують. Гени, що мутували, показані на рисунку 2 у вигляді осередків зі світло-зеленої заливкою. Тобто в ході мутації значення біта в осередку змінилося на протилежне.

Так в першій клітинці з «0» на «1». У другій з «1» на «0». Далі формуємо нове покоління з масиву батьків і освічених нащадків. В ході формування нового покоління застосовувалися як батьків, так і нащадків вже відомі [19, 21] значення функції придатності, див. Рис. 3.

ISSN 2663 - 4023

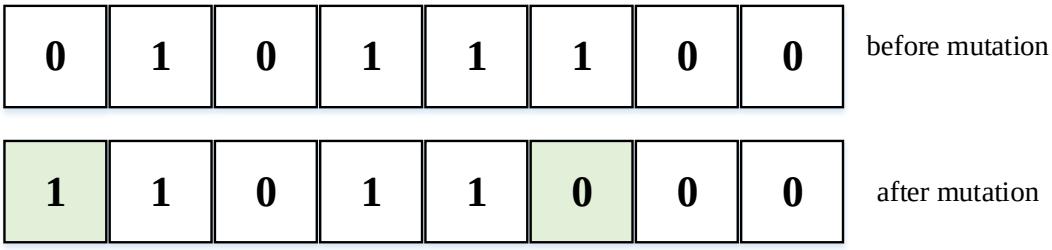


Рис. 2. Схема мутації

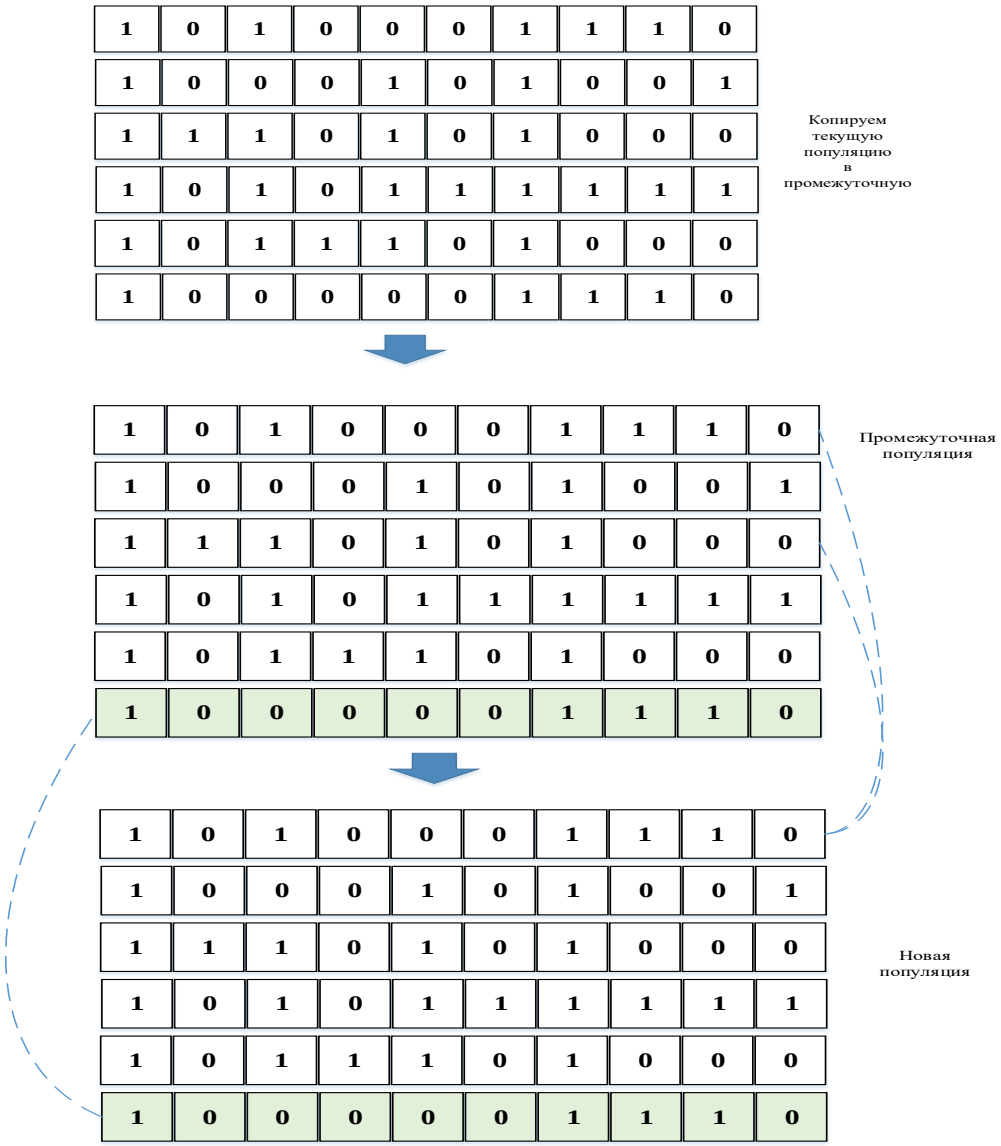


Рис. 3. Схема формування нової популяції

Порядок роботи з модифікованим алгоритмом розв'язання задачі багатокритеріальної оптимізації параметрів багатоконтурною СЗІ об'єкта інформатизації такий:

Крок 1. Вибираємо області визначення для всіх змінних (метрик кібербезпеки ОБІ), див. Таблицю 1:

Таблиця 1

Перемінні для ГА

Номер біта в хромосомі	Метрики кібербезпеки для об'єкта інформатизації, що аналізується
0	Частка інцидентів з кібербезпекою (КБ) на ОБІ (за типами)
1	Частка інцидентів з КБ на ОБІ з дотриманням термінів реагування
2	Середня тривалість часу реагування на інциденти з КБ (за рівнями критичності)
3	Частка вразливостей на ОБІ, які усунуті у встановлений термін
4	Середній час, який витрачено на усунення вразливостей ОБІ
5	Частка ризиків для інформаційних активів ОБІ (неприпустимого рівня для кожного активу)
6	Частка ризиків для КБ ОБІ, за якими були вжиті відповідні заходи
7	Індекс відповідності стандарту (стандартів) ІБ
8	Ефективність навчання співробітників заходам щодо дотримання правил КБ
9	Показники достатності ресурсів (фінансових, технічних, організаційних та ін.) для виконання завдань ІБ і КБ ОБІ

Крок 2. Введення установок ГА. Задаємо: розмір популяції; число поколінь (від 100 до 2000); тип мутації: число прогонів.

На відміну від існуючого класичного алгоритму VEGA [5, 19], в модифікованому алгоритмі додатково застосовані принцип Парето.

Приймемо наступні змінні: поточна популяція; проміжна популяція; розмір популяції; кількість примірників в порівняльному безлічі; відстань між екземплярами.

У процедурі селекції використовується ранжування примірників на основі Парето-домінування [21]. Ранг примірника, по відношенню до якого жоден з альтернативних примірників, аналізованої популяції, не володіє переважаючими критеріями оптимальності, вважаємо рівним 1.

Для інших примірників ранг знаходимо так:

$$rank(I_k) = 1 + N_{a_k}, \tag{1}$$

N_{a_k} – кількість примірників поточної популяції, характеристики яких краще поточної.

Механізм формування примірників забезпечується при виконанні наступної умови:

$$X = M(I) \in CS, \tag{2}$$

де $M(I)-$ функція для відображення примірника $I \in CS_I$

$CS-$ простір критеріїв, за якими реалізується відбір екземплярів.

Ранг примірників, для яких порушено обмеження (2) призначаємо в залежності від того, яким чином порушені ці обмеження. Ранг кожного з примірників, для яких порушено обмеження (2), буде більше рангу кожного з примірників, для яких це (2) виконується.

Функцію придатності будуємо на основі виразу:

$$\gamma(I) = 1 + \sum_{k=1}^{rank(I)-1} h(k), \tag{3}$$

ISSN 2663 - 4023

де $h(k)-$ кількість примірників з рангом (k).

Функцію придатності можна записати інакше:

$$f(I_1)=z(I_1)\cdot\gamma(I_1), \tag{4}$$

де $z(I_1)-$ кількість примірників I_1 обчислюємо так:

$$z(I_1)=\sum_{I_k\in PO_t} Sh(d(I_1,I_k)), \tag{5}$$

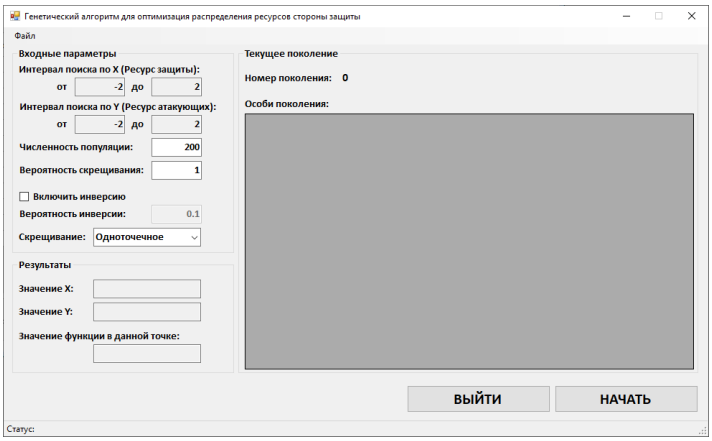
Де $Sh(d)-$ функція поділу обчислюється так:

$$Sh(d)=\begin{cases}1-\dfrac{d}{S_{po}}, & d<S_{po},\\ 0, & d\geq S_{po}.\end{cases} \tag{6}$$

Принцип Парето застосовується для кращої точки. У цій точці рішення, трактуються як краще, якщо за однією з метрик кібербезпеки є поліпшення, а по інший метриці (або метрик) буде строго не гірше.

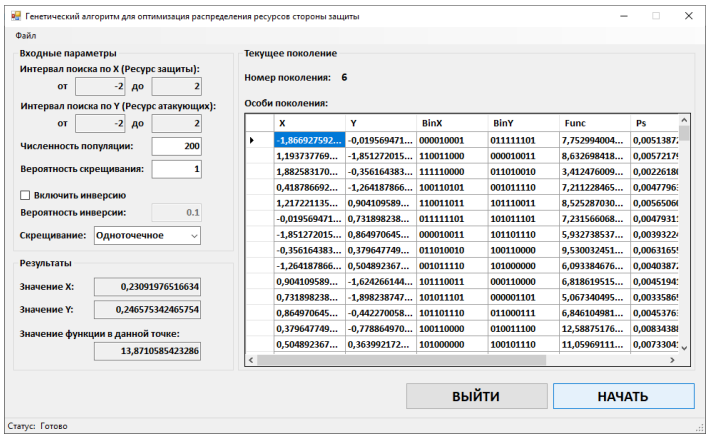
Описаний вище ГА був програмно реалізований у вигляді окремих модулів системи підтримки прийняття рішень (СППР) для задачі багатокритеріальної оптимізації витрат на СЗІ ОБІ. Середовище програмування - Visual Studio, див. Рис. 4.

На рисунку 4 а) показаний загальний вигляд інтерфейсу модуля СППР.



а) загальний вигляд інтерфейсу модуля СППР

ISSN 2663 - 4023



б) приклад рішення

Рис. 4. Загальний вигляд модуля 2 - Генетичний алгоритм для оптимізації витрат на СЗІ ОБІ

На рисунку 4б) показаний приклад рішення задачі пошуку раціональних параметрів співвідношення показників ефективності конкретних СЗІ для ОБІ і показників витрат на їх придбання, обслуговування, модернізацію), що входять в цільову функцію, і залежать від переліку робіт із забезпечення захисту інформації на ОБІ (зокрема , проектування, розробка та розгортання комплексної СЗІ, вдосконалення системи забезпечення інформаційної безпеки, та ін.

На відміну від існуючого класичного алгоритму VEGA, в модифікованому алгоритмі додатково застосовані принцип Парето, а також новий механізм селекції.

Новий механізм селекції, передбачає створення проміжної популяції - PO_m. Ця проміжна популяція PO_m формується так:

1. Перша половина популяції PO_m формується на основі метрики - частка вразливостей ОБІ, які усунуті в установлені терміни.

2. Друга половина проміжної популяції PO_m формується на основі метрики - частка ризиків, які неприпустимі рівням для інформаційних активів ОБІ.

3. Частини проміжної популяції змішуються.

4. Після змішування формується масив номерів і виробляється змішування.

5. Для схрещування будуть братися екземпляри (індивіди) за номером з цього масиву. Номери вибираються випадково.

Для того щоб перевірити ефективність запропонованого алгоритму були проведені обчислювальні експерименти, зокрема, для оцінки часу, що витрачається різними алгоритмами для пошуку рішення в ході оптимізації витрат на СЗІ ОБІ. На основі серії з 500 обчислювальних експериментів було встановлено, що для остаточної версії алгоритму і його програмної реалізації в СППР досить брати 25 хромосом в популяції.

Запропонований підхід дозволяє не тільки вирішувати багатокритиріальне завдання по оптимізації набору СЗІ по кожному з вузлів контурів захисту ОБІ, але і дає можливість оперативно проводити аналіз доцільності перерозподілу ресурсів боку захисту в умовах обмеженості ресурсів, що виділяються на СЗІ ОБІ.

Час, витрачений на вирішення завдання при використанні ГА, приблизно в 16-25 разів менше в порівнянні з показниками методу гілок і меж. Жадібний алгоритм поступається як ГА, так і методу гілок і меж з точки зору пристосованості до вирішення

багатокритеріальної оптимізаційної задачі з урахуванням накладених обмежень і кількості змінних.

До певних недоліків дослідження, на цьому етапі його проведення, слід віднести той факт, що були проаналізовані не всі можливі алгоритми вирішення поставленого завдання.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Викладена методика багатокритеріальної оптимізації витрат на систему захисту інформації об'єкта інформатизації. Методика базується на застосуванні генетичного алгоритму.

Запропоновано модифікований алгоритм рішення задачі БКО параметрів багатоконтурною системи захисту інформації об'єкта інформатизації, який дозволяє обґрунтовувати оптимальні параметри компонентів СЗІ з урахуванням обраних експертом пріоритетних метрик кібербезпеки ОБІ.

На відміну від існуючого класичного алгоритму VEGA, в модифікованому алгоритмі додатково застосовані принцип Парето, а також новий механізм селекції.

Принцип Парето застосовується для кращої точки. У цій точці рішення, трактуються як краще, якщо за однією з метрик кібербезпеки є поліпшення, а по інший метриці (або метрик) буде строго не гірше.

Новий механізм селекції на відміну від традиційної, передбачає створення проміжної популяції. Ця проміжна популяція формується в кілька етапів. На першому етапі перша половина популяції формується на основі метрики - частка вразливостей ОБІ, які усунуті в установлені терміни. На другому етапі друга половина проміжної популяції формується на основі метрики - частка ризиків, які неприпустимі для інформаційних активів ОБІ. Далі ці частини проміжної популяції змішуються. Після змішування формується масив номерів і виробляється змішування. На заключному етапі селекції для схрещування будуть братися екземпляри (індивіди) за номером з цього масиву. Номери вибираються випадково.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Okutan, A., Yang, S. J., McConky, K., & Werner, G. (2019). CAPTURE: Cyberattack Forecasting Using Non-Stationary Features with Time Lags. In 2019 IEEE Conference on Communications and Network Security (CNS) (pp. 205–213). IEEE.

2 Barreto, C., & Koutsoukos, X. (2019, October). Design of Load Forecast Systems Resilient Against Cyber-Attacks. In International Conference on Decision and Game Theory for Security (pp. 1–20). Springer, Cham.

3 Chandra, Y., & Mishra, P. K. (2019). Design of cyber warfare testbed. In Software Engineering (pp. 249–256). Springer, Singapore.

4 Sándor, H., Genge, B., Szántó, Z., Márton, L., & Haller, P. (2019). Cyber attack detection and mitigation: Software Defined Survivable Industrial Control Systems. International Journal of Critical Infrastructure Protection, 25, pp. 152–168.

5 Chiba, Z., Abghour, N., Moussaid, K., El Omri, A., & Rida, M. (2019). New Anomaly Network Intrusion Detection System in Cloud Environment Based on Optimized Back Propagation Neural Network Using Improved Genetic Algorithm. International Journal of Communication Networks and Information Security, 11(1), 61–84.

6 Nozaki, Y., & Yoshikawa, M. (2019). Security evaluation of ring oscillator puf against genetic algorithm based modeling attack. In International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (pp. 338–347). Springer, Cham.

7 Dwivedi, S., Vardhan, M., & Tripathi, S. (2020). Incorporating evolutionary computation for securing wireless network against cyberthreats. The Journal of Supercomputing, 1–38.
8 Zhang, F., Kodituwakku, H. A. D. E., Hines, J. W., & Coble, J. (2019). Multilayer Data-Driven Cyber-Attack Detection System for Industrial Control Systems Based on Network, System, and Process Data. IEEE Transactions on Industrial Informatics, 15(7), 4362–4369.
9 Sureshkumar, T., Anand, B., & Premkumar, T. (2019). Efficient Non-Dominated Multi-Objective Genetic Algorithm (NDMGA) and network security policy enforcement for Policy Space Analysis (PSA). Computer Communications, 138, 90–97.
10 Shang, Q., Chen, L., Wang, D., Tong, R., & Peng, P. (2019). Evolvable Hardware Design of Digital Circuits Based on Adaptive Genetic Algorithm. In International Conference on Applications and Techniques in Cyber Security and Intelligence (pp. 791–800). Springer, Cham.
11 Yang, Y. (2019). Research on Hybrid Quantum Genetic Algorithm Based on Cross-Docking Delivery Vehicle Scheduling. In The International Conference on Cyber Security Intelligence and Analytics (pp. 893–900). Springer, Cham.
12 Saenko, I., & Kotenko, I. (2019). A role-base approach and a genetic algorithm for VLAN design in large critical infrastructures. In Proceedings of the Genetic and Evolutionary Computation Conference Companion (pp. 1643–1650).
13 Aleksieva, Y., Valchanov, H., & Aleksieva, V. (2019). An approach for host based botnet detection system. In 2019 16th Conference on Electrical Machines, Drives and Power Systems (ELMA) (pp. 1–4). IEEE.
14 Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., Al-Nemrat, A., & Venkatraman, S. (2019). Deep learning approach for intelligent intrusion detection system. IEEE Access, 7, 41525–41550.
15 Malarvizhi, N., Selvarani, P., & Raj, P. (2019). Adaptive fuzzy genetic algorithm for multi biometric authentication. Multimedia Tools and Applications, 1–14.
16 Alhijawi, B., Kilani, Y., & Alsarhan, A. (2020). Improving recommendation quality and performance of genetic-based recommender system. International Journal of Advanced Intelligence Paradigms, 15(1), 77–88.
17 Baroudi, U., Bin-Yahya, M., Alshammari, M., & Yaqoub, U. (2019). Ticket-based QoS routing optimization using genetic algorithm for WSN applications in smart grid. Journal of Ambient Intelligence and Humanized Computing, 10(4), 1325–1338.
18 Llansó, T., McNeil, M., & Noteboom, C. (2019). Multi-Criteria Selection of Capability-Based Cybersecurity Solutions. In Proceedings of the 52nd Hawaii International Conference on System Sciences, pp. 7322–7330.
19 Kong, T., Wang, L., Ma, D., Xu, Z., Yang, Q., & Chen, K. (2019). A Secure Container Deployment Strategy by Genetic Algorithm to Defend against Co-Resident Attacks in Cloud Computing. In 2019 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS) (pp. 1825–1832). IEEE.
20 Lakshmanaprabu, S. K., Mohanty, S. N., Krishnamoorthy, S., Uthayakumar, J., & Shankar, K. (2019). Online clinical decision support system using optimal deep neural networks. Applied Soft Computing, 81, 105487.
21 Lakhno, V., Akhmetov, B., Adilzhanova, S., Blozva, A., Svitlana, R., Dmytro, R. The use of a genetic algorithm in the problem of distribution of information security organizational and financial resources (2020) ATIT 2020 - Proceedings: 2020 2nd IEEE International Conference on Advanced Trends in Information Theory, № 9349310, pp. 251-254.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (13), 2021
ISSN 2663 - 4023

Vitaliy Chubaievskyi
Candidate of Political Sciences, Associate Professor of Department of Software Engineering and Cyber Security
Kyiv National University of Trade and Economics, Kyiv, Ukraine
ORCID ID: 0000-0001-8078-2652
chubaievskyi_vi@knute.edu.ua

Valery Lakhno
Doctor of Technical Sciences, Professor of Department of Computer Systems and Networks
National University of Life and Environmental Sciences of Ukraine Kyiv, Ukraine
ORCID ID: 0000-0001-9695-4543
lva964@gmail.com

Olena Kryvoruchko
Doctor of Engineering Sciences, Professor, Head of Department of Software Engineering and Cyber Security
Kyiv National University of Trade and Economics, Kyiv, Ukraine
ORCID ID: 0000-0002-7661-9227
kryvoruchko_ev@knute.edu.ua

Dmytro Kasatkin
Candidate of Pedagogical Sciences, Associate Professor, Associate Professor of Department of Computer Systems and Networks
National University of Life and Environmental Sciences of Ukraine Kyiv, Ukraine
ORCID ID: 0000-0002-2642-8908
dm_kasat@ukr.net

Alona Desiatko
PhD in Computer Sciences, Associate Professor of Department of Software Engineering and Cyber Security
Kyiv National University of Trade and Economics, Kyiv, Ukraine
ORCID ID: 0000-0003-2860-2188
desyatko@knute.edu.ua

Andrii Blozva
Candidate of Pedagogical Sciences, Associate Professor, Associate Professor of Department of Computer Systems and Networks
National University of Life and Environmental Sciences of Ukraine Kyiv, Ukraine
ORCID ID: 0000-0002-4377-0916
andriy.blozva@nubip.edu.ua

Boris Gusev
Candidate of Pedagogical Sciences, Associate Professor, Associate Professor of Department of Computer Systems and Networks
National University of Life and Environmental Sciences of Ukraine Kyiv, Ukraine
ORCID ID: 0000-0003-1658-7822
gusevbs@gmail.com

EFFICIENCY OF THE INDICATORS INVESTMENT CALCULATION METHOD IN THE INFORMATION SECURITY SYSTEM OF INFORMATION OBJECTS

Abstract. The article describes the methodology of multi-criteria optimization of costs for the information protection system of the object of informatization. The technique is based on the use of a modified VEGA genetic algorithm. A modified algorithm for solving the MCO problem of parameters of a multi-circuit information protection system of an informatization object is proposed, which makes it possible to substantiate the rational characteristics of the ISS components, taking into account the priority metrics of OBI cybersecurity selected by the expert. In contrast to the existing classical VEGA algorithm, the modified algorithm additionally applies the Pareto principle, as well as a new mechanism for the selection of population specimens.
The Pareto principle applies to the best point. At this point, the solution, interpreted as the best, if there is an improvement in one of the cybersecurity metrics, and strictly no worse in another metric (or metrics). The new selection mechanism, in contrast to the traditional one, involves the creation

of an intermediate population. The formation of an intermediate population occurs in several stages. At the first stage, the first half of the population is formed based on the metric - the proportion of vulnerabilities of the object of informatization that are eliminated in a timely manner. At the second stage, the second half of the intermediate population is formed based on the metric - the proportion of risks that are unacceptable for the information assets of the informatization object. Further, these parts of the intermediate population are mixed. After mixing, an array of numbers is formed and mixed. At the final stage of selection for crossing, specimens (individuals) will be taken by the number from this array. The numbers are chosen randomly. The effectiveness of this technique has been confirmed by practical results

Keywords: information security, cybersecurity, protection circuits, multi-criteria optimization, genetic algorithm

REFERENCES (TRANSLATED AND TRANSLITERATED)

1 Okutan, A., Yang, S. J., McConky, K., & Werner, G. (2019). CAPTURE: Cyberattack Forecasting Using Non-Stationary Features with Time Lags. In 2019 IEEE Conference on Communications and Network Security (CNS) (pp. 205–213). IEEE.
2 Barreto, C., & Koutsoukos, X. (2019, October). Design of Load Forecast Systems Resilient Against Cyber-Attacks. In International Conference on Decision and Game Theory for Security (pp. 1–20). Springer, Cham.
3 Chandra, Y., & Mishra, P. K. (2019). Design of cyber warfare testbed. In Software Engineering (pp. 249–256). Springer, Singapore.
4 Sándor, H., Genge, B., Szántó, Z., Márton, L., & Haller, P. (2019). Cyber attack detection and mitigation: Software Defined Survivable Industrial Control Systems. International Journal of Critical Infrastructure Protection, 25, pp. 152–168.
5 Chiba, Z., Abghour, N., Moussaid, K., El Omri, A., & Rida, M. (2019). New Anomaly Network Intrusion Detection System in Cloud Environment Based on Optimized Back Propagation Neural Network Using Improved Genetic Algorithm. International Journal of Communication Networks and Information Security, 11(1), 61–84.
6 Nozaki, Y., & Yoshikawa, M. (2019). Security evaluation of ring oscillator puf against genetic algorithm based modeling attack. In International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (pp. 338–347). Springer, Cham.
7 Dwivedi, S., Vardhan, M., & Tripathi, S. (2020). Incorporating evolutionary computation for securing wireless network against cyberthreats. The Journal of Supercomputing, 1–38.
8 Zhang, F., Kodituwakku, H. A. D. E., Hines, J. W., & Coble, J. (2019). Multilayer Data-Driven Cyber-Attack Detection System for Industrial Control Systems Based on Network, System, and Process Data. IEEE Transactions on Industrial Informatics, 15(7), 4362–4369.
9 Sureshkumar, T., Anand, B., & Premkumar, T. (2019). Efficient Non-Dominated Multi-Objective Genetic Algorithm (NDMGA) and network security policy enforcement for Policy Space Analysis (PSA). Computer Communications, 138, 90–97.
10 Shang, Q., Chen, L., Wang, D., Tong, R., & Peng, P. (2019). Evolvable Hardware Design of Digital Circuits Based on Adaptive Genetic Algorithm. In International Conference on Applications and Techniques in Cyber Security and Intelligence (pp. 791–800). Springer, Cham.
11 Yang, Y. (2019). Research on Hybrid Quantum Genetic Algorithm Based on Cross-Docking Delivery Vehicle Scheduling. In The International Conference on Cyber Security Intelligence and Analytics (pp. 893–900). Springer, Cham.
12 Saenko, I., & Kotenko, I. (2019). A role-base approach and a genetic algorithm for VLAN design in large critical infrastructures. In Proceedings of the Genetic and Evolutionary Computation Conference Companion (pp. 1643–1650).
13 Aleksieva, Y., Valchanov, H., & Aleksieva, V. (2019). An approach for host based botnet detection system. In 2019 16th Conference on Electrical Machines, Drives and Power Systems (ELMA) (pp. 1–4). IEEE.
14 Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., Al-Nemrat, A., & Venkatraman, S. (2019). Deep learning approach for intelligent intrusion detection system. IEEE Access, 7, 41525–41550.
15 Malarvizhi, N., Selvarani, P., & Raj, P. (2019). Adaptive fuzzy genetic algorithm for multi biometric authentication. Multimedia Tools and Applications, 1–14.

16 Alhijawi, B., Kilani, Y., & Alsarhan, A. (2020). Improving recommendation quality and performance of genetic-based recommender system. International Journal of Advanced Intelligence Paradigms, 15(1), 77–88.

17 Baroudi, U., Bin-Yahya, M., Alshammari, M., & Yaqoub, U. (2019). Ticket-based QoS routing optimization using genetic algorithm for WSN applications in smart grid. Journal of Ambient Intelligence and Humanized Computing, 10(4), 1325–1338.

18 Llansó, T., McNeil, M., & Noteboom, C. (2019). Multi-Criteria Selection of Capability-Based Cybersecurity Solutions. In Proceedings of the 52nd Hawaii International Conference on System Sciences, pp. 7322–7330.

19 Kong, T., Wang, L., Ma, D., Xu, Z., Yang, Q., & Chen, K. (2019). A Secure Container Deployment Strategy by Genetic Algorithm to Defend against Co-Resident Attacks in Cloud Computing. In 2019 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS) (pp. 1825–1832). IEEE.

20 Lakshmanaprabu, S. K., Mohanty, S. N., Krishnamoorthy, S., Uthayakumar, J., & Shankar, K. (2019). Online clinical decision support system using optimal deep neural networks. Applied Soft Computing, 81, 105487.

21 Lakhno, V., Akhmetov, B., Adilzhanova, S., Blozva, A., Svitlana, R., Dmytro, R. The use of a genetic algorithm in the problem of distribution of information security organizational and financial resources (2020) ATIT 2020 - Proceedings: 2020 2nd IEEE International Conference on Advanced Trends in Information Theory, № 9349310, pp. 251-254.