КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (17), 2022
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2022.17.620
УДК 004.056:519.856

Лахно Валерій Анатолійович
д.т.н., професор, завідувач кафедри комп'ютерних систем, мереж та кібербезпеки НУБіП України
Національний університет біоресурсів і природокористування України, Київ, Україна
ORCID ID 0000-0001-9695-4543
valss21@ukr.net

Малюков Володимир Павлович
д.ф.-м.н., професор, професор кафедри комп'ютерних систем, мереж та кібербезпеки НУБіП України
Національний університет біоресурсів і природокористування України, Київ, Україна
ORCID ID 0000-0002-7533-1555
volod.malyukov@gmail.com

Комарова Лариса Олексіївна,
д.т.н., проф. Лауреат державної премії України в галузі науки і техніки, директор ННІ ІБ СК НА СБУ України, Київ, Україна
ORCID ID 0000-0002-9776-0879
lacosta_k@ukr.net.

Касаткін Дмитро Юрійович
к.пед.н., доцент, доцент кафедри комп'ютерних систем, мереж та кібербезпеки НУБіП України
Національний університет біоресурсів і природокористування України, Київ, Україна
ORCID ID 0000-0002-2642-8908
d.kasatkin@nubip.edu.ua

Осипова Тетяна Юріївна
к.пед.н., доцент кафедри комп'ютерних систем, мереж та кібербезпеки НУБіП України
Національний університет біоресурсів і природокористування України, Київ, Україна
ORCID ID 0000-0002-9199-3436
t_osipova@nubip.edu.ua

Часновський Єгор Анатолійович
аспірант кафедри комп'ютерних систем, мереж та кібербезпеки НУБіП України
Національний університет біоресурсів і природокористування України, Київ, Україна
ORCID ID 0000-0002-1848-4221
egor.chasnovskii@gmail.com

ОПТИМІЗАЦІЯ РОЗМІЩЕННЯ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ ЗАСТОСУВАННЯ ГЕНЕТИЧНОГО АЛГОРИТМУ

Анотація. У статті розглянуто можливості модифікації генетичного алгоритму (ГА) для розв'язання задачі щодо підбору та оптимізації конфігурацій засобів захисту інформації (ЗЗІ) для контурів безпеки інформаційно-комунікаційних систем (ІКС). Наукова новизна роботи полягає в тому, що в ГА в якості критеріїв для оптимізації складу ЗЗІ запропоновано використовувати сумарну величину ризиків від втрати інформації, а також інтегральний показник ЗЗІ та вартісні показники для кожного класу ЗЗІ. Генетичний алгоритм у задачі оптимізації вибору складу ЗЗІ для ІКС розглянутий як варіація задачі, пов'язаної з мультивибором. У такій постановці оптимізація розміщення ЗЗІ по контурам захисту ІКС розглянута як модифікація комбінаторної задачі про рюкзак. Застосований в обчислювальному ядрі системи підтримки прийняття рішень (СППР) ГА відрізняється від стандартного ГА. У рамках модифікації ГА хромосоми представлені у вигляді матриць, елементи яких є числами, що відповідають номерам ЗЗІ у вузлах ІКС. У процесі модифікації ГА був застосований k-точковий кросинговер. Фітнес-функція представлена як сума коефіцієнтів ефективності. При цьому крім традиційних абсолютних показників ефективності ЗЗІ враховуються сумарна величина ризиків від втрати інформації, а також вартісні показники для кожного класу ЗЗІ. Практична цінність дослідження полягає у

реалізації СППР на основі запропонованої модифікації ГА. Виконані обчислювальні експерименти щодо вибору раціонального програмного алгоритму реалізації моделі. Показано, що реалізація ГА у СППР дозволяє прискорити пошук оптимальних варіантів розміщення засобів кібербезпеки (КрБ) для ІКС більш ніж у 25 разів. Ця перевага дозволяє не тільки виконати швидкий перебір різних варіантів апаратно-програмних ЗЗІ та їх комбінацій для ІКС, але й у подальшому об'єднати запропонований алгоритм із наявними моделями та алгоритмами оптимізації складу контурів кібербезпеки ІКС. Потенційно таке об'єднання моделей та алгоритмів надасть можливість швидко перебудовувати захист ІКС, коригуючи його профілі відповідно до нових загроз та класів кібератак.

Ключові слова: система підтримки прийняття рішень, засоби захисту інформації, багатокритеріальна оптимізація, задача про рюкзак, генетичний алгоритм

ВСТУП

У міру зростання кількості та складності успішно реалізованих кібератак на різні інформаційно-комунікаційні системи (ІКС) [1, 2] зростає потреба в якісно нових процедурах формування складу комплексів захисту інформації (ЗІ) та кібербезпеки (КрБ) на всіх контурах захисту ІКС. Зауважимо, що перманентне завдання щодо формування ефективних контурів кібербезпеки ІКС викликало безліч досліджень, присвячених питанням оптимізації складу засобів захисту інформації (ЗЗІ) та КрБ. Ці дослідження, перш за все, мають на меті відповісти на питання, пов'язані з вирішенням багатокритеріальних оптимізаційних завдань, яким властиві такі особливості як: складна конфігурація допустимої сфери застосування окремих ЗЗІ; багатоекстремальність функцій, що розглядаються; алгоритмічне завдання функцій тощо. Окрім того, у реальних завданнях побудови ефективних багатоконтурних систем КрБ [3, 4] розв’язання нечасто прийнято оцінювати за єдиним критерієм. Тому, в подібних задачах, важливо не тільки знаходити допустимі парето-оптимальні рішення, а й апроксимувати безліч отриманих варіантів, щоб запропонувати людині, яка приймає рішення (ЛПР) об'єктивний вибір ЗЗІ за відповідними контурами КрБ ІКС. Вирішення вищезазначених завдань побудови багатоконтурних систем захисту в умовах зростання кількості спроб деструктивних впливів на ІКС вимагає застосування не тільки класичних процедур оптимізації, але й більш універсальних методів, наприклад, генетичних алгоритмів (ГА), які довели свою ефективність під час розв’язання багатьох складних завдань [5, 6].

Ефективність ГА визначається ретельним налаштуванням та контролем їх параметрів. Це ускладнює застосування ГА у звичайних інженерних розрахунках ефективності ЗЗІ за контурами ІКС. Однак, застосування ГА стає цілком виправданим, якщо, крім традиційної багатокритеріальної оптимізаційної задачі щодо вибору складу ЗЗІ для ІКС, розглядати і величину ризиків, а також вартісні показники відібраних ЗЗІ для конкретних активів (бази даних, бази знань, пошта, сайт та ін.). Процедура пошуку рішення може бути більш ефективною, якщо задіяти потенціал інтелектуальних систем підтримки прийняття рішень (СППР), обчислювальне ядро яких власне і базується на застосуванні ГА.

Постановка проблеми.

Вище наведені міркування визначили актуальність досліджень, спрямованих на вдосконалення еволюційних алгоритмів та моделей для обчислювального ядра СППР у процесі багатокритеріальної оптимізації складу ЗЗІ за контурами КрБ ІКС.

Аналіз останніх досліджень і публікацій. Генетичні алгоритми, що застосовуються під час вирішення багатокритеріальних оптимізаційних завдань, є

варіантами еволюційних методів пошуку [7]. Дослідженням у цій галузі за останні кілька років присвячена досить велика кількість робіт. Так, наприклад, в [8] зображено модель, відповідно до якої створюється популяція елементів ЗЗІ (особин), де в задачі оптимізації кожна особина відповідає одному з можливих рішень. Для пошуку найкращого рішення автори використовували власну цільову функцію. У дослідженні не зазначено яким чином і де конкретно були використані запропоновані рішення на практиці.

У роботах [9, 10] були досліджені ГА, які можна віднести до двох груп. У першій групі досліджувалися ГА із бінарним кодуванням [10, 11]. У другій групі, відповідно, ГА із дійсним кодуванням [12, 13]. У роботі [12] показано, що в першій групі можна досягти більш високої ефективності пошуку екстремального значення на множині допустимих рішень.

У роботах [12, 14] показано, що постійна мутація об'єктів використовується у більшості реалізацій ГА. Змінні у цьому випадку є більш гнучкими, що дозволяє шукати початкові рішення вже на досить ранніх стадіях роботи ГА. Програмну реалізацію алгоритму в дослідженнях не представлено.

У працях [15, 16] висвітлено, що враховуючи велику залежність успішної роботи алгоритму від мутації, викликаної особливостями завдання формування контурів КрБ ІКС, змінна мутація є кращою з точки зору пошуку глобального оптимуму. Це пояснюється тим, що на ранніх стадіях роботи ГА діятиме великий елемент випадковості.

У роботах [17, 18] розглядалися особливості застосування модифікованого ГА у подібних багатокритеріальних оптимізаційних задачах. Відмінність ГА з відносною фітнес-функцією від стандартного ГА полягає в тому, що тут під час роботи алгоритму в якості фітнес-функції застосовувалася не сума ефективностей ЗЗІ, які власне, складали хромосому, а використовувалася сума відношень ефективностей до обмежуючих характеристик ЗЗІ, або так званий – коефіцієнт ефективності. Подібна модифікація ГА по суті є диз'юнкцією стандартного ГА і жадібного алгоритму.

У роботах [19, 20] досліджувалися можливості щодо зменшення кількості параметрів ГА що налаштовуються. На відміну від стандартного, запропоновані авторами рішення не містили оператора схрещування. По суті, рішення виходило на основі статистичної інформації про пошуковий простір. Таким чином, накопичуючи та використовуючи цю інформацію, дані алгоритми самостійно можуть адаптуватися до розв'язуваної задачі.

Завдання оптимізації вибору складу ЗЗІ для ІКС можна розглядати як варіацію завдань пов’язаних з мультивибором [21, 22]. У зазначених роботах оптимізація розміщення компонентів контурів КрБ розглянута як деяка модифікація комбінаторної задачі про рюкзак. Цей підхід відрізняється досить простими формалізацією постановки та інтерпретації рішення. Однак автори не навели повного рішення та порівняння алгоритмів розв’язання, наприклад, генетичного, простого перебору, динамічного програмування та ін.

Слід зазначити, що завдання про мультиплікативний рюкзак не відображає всіх можливостей, пов'язаних із заміщенням предметів з одного класу ЗЗІ предметами з інших класів. Однак, предмети, що заміщуються виконують еквівалентні функції. Отже, замість загальної цінності предметів необхідно запровадити функцію, що відображає безліч цілей. Це робиться для того, щоб відобразити взаємозамінність чи еквівалентність предметів у «рюкзаку» [24, 25].

У дослідженнях [17, 20] показано, що стандартні та модифіковані ГА досить ефективні для вирішення більшості складних оптимізаційних завдань [23] та є перспективними для подальшого вивчення та вдосконалення.

Все вище зазначене визначило релевантність дослідження, спрямованого на розвиток ГА для обчислювального ядра СППР у задачах оптимізації вибору ЗЗІ та КрБ для ІКС різних об'єктів інформатизації.

Мета статті. Метою статті є розвиток генетичного алгоритму для обчислювального ядра системи підтримки прийняття рішень у процесі добору та оптимізації складу засобів захисту інформації.

Для досягнення поставленої мети дослідження необхідно вирішити такі завдання:

- Розробити уточнення для ГА з урахуванням сумарної величини ризику та вартості системи КрБ;
- Розробити та реалізувати СППР на базі обчислювального ядра ГА для підбору та оптимізації складу ЗЗІ;
- Провести обчислювальні експерименти з перевірки працездатності модифікованого ГА та запропонованої СППР.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

За замовчуванням у вузлах ІКС встановлено стандартні ЗЗІ [23]: антивіруси; брандмауер; засоби: 1) виявлення вторгнень; 2) криптографічного ЗІ; 3) розмежування доступу; 4) контролю цілісності; 5) автентифікації та ін.

Вочевидь, для конкретної ІКС перелік може бути доповнений у зв’язку з недостатністю чи скорочений через надмірність.

У рекомендаціях NIST докладно описано архітектуру, основні вразливості та особливості забезпечення КрБ та ЗІ в ІКС. Зауважимо, однак, що на сьогодні відсутній універсальний підхід, який здатний дати однозначне рішення в процесі пошуку оптимального варіанта розміщення ЗЗІ та КрБ по вузлах ІКС з урахуванням усіх особливостей конкретної ІКС, аналізу механізмів забезпечення КрБ та ефективності ЗЗІ щодо наявного спектра загроз. Як наслідок постає питання про створення такого підходу. При цьому отримане рішення має відрізнятися такими можливостями:

1. по проектуванню різних варіантів контурів інформаційної та КрБ, виходячи з структури конкретної ІКС.

2. щодо вибору ЗЗІ виходячи з потреб протидії конкретним загрозам різних класів.

3. адаптивно (еволюційно) змінювати алгоритм відбору та оптимізації наборів ЗЗІ та КрБ, виходячи з еволюціонування механізмів атак. А це, у свою чергу, унеможливлює застосування лише точних методів відбору ЗЗІ для вузлів ІКС.

Виходячи з вищенаведеного, розглянемо можливість застосування ГА для вирішення задачі про мультивибір у процесі підбору оптимальної конфігурації (далі - набір) ЗЗІ (наприклад, антивіруси, мережеві екрани, засоби виявлення вторгнень та ін.) для ІКС.

Формалізація завдання у термінах ГА.

Вважаємо, що хромосома – це набір захисних заходів (наприклад, правила щодо дотримання політики інформаційної безпеки на об'єкті захисту), у тому числі ЗЗІ. Набір закодований у вигляді двійкового числа [8, 9]. Якщо двійковий розряд числа дорівнює одиниці (1), то відповідний ЗЗІ або міра захисту інформації з відповідним номером,

ISSN 2663 - 4023

долучається до набору. Тоді діапазон зміни коду можна представити так:

$$G = (d_0 d_1 ... d_{NC})_2 = (0...2NC)_{10}, \quad (1)$$

де NC – кількість наявних ЗЗІ та захисних заходів, які потенційно розглядаються для включення до оптимального набору;

d_i – включення ЗЗІ і/або захисної міри в набір.

У термінах ГА популяція буде складатись з екземплярів із різними хромосомами. Розмір популяції обмежений максимальною кількістю екземплярів у ній. Кожен екземпляр популяції можна описати так:

$$Ch = \{G, C, R\}, \quad (2)$$

де G – генетичний код екземпляра у популяції;

C – вартість ЗЗІ та/або відповідних захисних заходів;

R – сумарний ризик втрати інформації (або її конфіденційності, цілісності) з урахуванням обраних ЗЗІ та/або відповідних захисних заходів (далі прийнято ЗЗІ).

У процесі модифікації алгоритму з метою визначення ризику, використовується наступне припущення. Абсолютна величина втрат у грошовому еквіваленті для конкретної ІКС залежить від ланцюжка елементів – загрози, уразливості, ЗЗІ [2, 3]. Отже, кількість ризиків – це кількість комбінацій загроз та активів:

$$R = TH \cdot M, \quad (3)$$

де TH – кількість загроз, M – кількість активів.

У формулі (3) не враховано поєднання кількох загроз, а також внутрішній вплив між ЗЗІ. Тому найбільш адекватним способом визначити ризики для ІКС є метод, який заснований на складанні профілів атак [3, 4]. При такому методі профілі атак розглядаються як послідовності атак, які складаються із поєднання різних загроз [1, 4]. Тоді кількість ризиків можна описати такою залежністю:

$$R = \left(2^{TH}\right)^{TA}, \quad (4)$$

де TA – кількість атак.

Отже, величиною ризику для заданого профілю атак можна вважати величину сумарного збитку від успішних атак.

Якщо відсутня ланцюгова реакція в ході атаки, то величину сумарного ризику можна представити як математичне очікування шкоди для кожного активу ІКС:

$$r = \sum P_{i,j} \cdot D_{i,j}, \quad i = \overline{1, TH}, \; j = \overline{1, M}, \quad (5)$$

де $P_{i,j}$ – ймовірність виникнення інциденту інформаційної безпеки ІКС, спричиненого загрозою (i) активу (j); $D_{i,j}$ – розмір збитків, пов'язаних з інцидентом (прийнятий у грошовому еквіваленті).

Хромосому (Ch) можна подати у вигляді матриці. Тоді, рядки матриці являтимуть собою точки розміщення, відповідно, стовпці - класи засобів, які включають конкретні ЗЗІ (наприклад, до класу засобів антивірусне ПЗ можна віднести всі варіанти аналізованих антивірусних програм - Avast, Avira, AVG, Bitdefender тощо). Елемент матриці g_{ij} показує номер засобу захисту інформації з класу j, що розміщується на вузлі i. Якщо $g_{ij} = 0$, то вважаємо, що з класу j на вузлі i не використовується жодний засіб, наприклад, антивірусне програмне забезпечення не використовується на міжмережевому екрані. Схема формування хромосоми (Ch) ГА представлена у таблиці 1.

Таблиця 1

Схема формування хромосоми

Класи контрзаходів / Вузли мережі	N_1	N_2	...	N_{NC}
K_1	g_{11}	g_{12}	...	g_{1NC}
K_2	g_{21}	g_{22}	...	g_{2NC}
...	...	...	...	...
K_{KC}	g_{KC1}	g_{KC2}	...	$g_{KC,NC}$

У такому форматі подання хромосоми і у контексті розв'язуваної задачі вважаємо, що K_{KC} та N_{NC} – відповідно, кількість вузлів ІКС та ЗЗІ на вузлі.

Для розрахунку ризику (R) скористаємося наступною моделлю.

Підберемо за генетичним кодом для кожного носія відповідні ЗЗІ.

Введемо в ГА функцію корисності - U. Дана функція необхідна для оцінки ефективності ЗЗІ, що відбираються в набір. Зауважимо, що ЗЗІ, що відбираються, повинні відповідати профілю атаки. Адже цілком зрозуміло, що, наприклад, безкоштовне антивірусне програмне забезпечення з обмеженим функціоналом абсолютно не придатне для боротьби з DoD / DDoS атаками, а інструкції з дотримання політики безпеки для ІКС самі по собі не захистять від інсайдера.

Тоді функцію корисності (U) можна подати так:

$$U(Ch) = R_0 - Ch.R, \tag{6}$$

де Ch – екземпляр набору ЗЗІ;

R_0 – величина ризиків, пов'язаних із втратою інформації, якщо не застосовувати відповідний набір ЗЗІ;

$Ch.R$ – величина ризиків з урахуванням застосування відповідного набору ЗЗІ (екземпляру) $Ch.G$.

Однак, досягнута результативність захисту ІКС від атак, відповідно, вимагає додаткових витрат на ЗЗІ. Врахуємо вплив витрат на ЗЗІ, застосовуючи наступне відношення:

$$U(Ch) = (R_0 - Ch.R) / Ch.C, \tag{7}$$

де $Ch.C$ – вартість набору ЗЗІ

Залежність (7) показує, як можна зменшити (або збільшити) ризик втрати інформації на кожну вкладену одиницю вартості.

Далі розглянемо, як отримані вирази можна застосувати до ГА. У синтаксисі мов програмування високого рівня функції кросинговеру, мутації, селекції виглядатимуть наступним чином.

Функція кросовера – породження нових носіїв. У процесі програмної реалізації СППР на базі ГА було розглянуто два види кросинговеру. Аналізувалися можливості застосування одноточкового та *n*-точкового кросинговера. Вибір цих двох видів зумовлений такими міркуваннями. Стандартний підхід, заснований на одноточковому кросинговері, підходить до більшості завдань, в яких доцільний пошук рішення за допомогою ГА. Зауважимо, однак, що для задач мультивибору ЗЗІ для вузлів ІКС

стандартний ГА виявиться неточним. Це зумовлено тим, що хромосома буде не єдиною неподільною структурою. У постановці цієї задачі хромосому можна інтерпретувати як систему, яка потребує процедури декомпозиції. Декомпозиція дозволить розбити хромосому на ділянки, причому кожній ділянці буде відповідати свій клас вузлів ІКС.

Створимо для кожної пари новий екземпляр, який успадкує риси батьків (PA).

$$\begin{aligned} &func\ K(PA) := \ foreach\ Ch(X)\ from\ PA\ and \\ &foreach\ Ch(Y)\ from\ PA\ where\ Ch(X) != \\ &Ch(Y)\ do\ R.add(\{G : xor(Ch(Xi).G, Ch(Xj).G), C :, R :\}) \\ &return\ R.add(PA) \end{aligned} \tag{8}$$

Далі розглянемо функцію мутації, тобто варіювання генетичного коду. Було розглянуто два види мутації. Це зумовлено такими припущеннями: 1) постійна мутація використовується у більшості програмних реалізацій ГА; 2) змінні нашого завдання вимагають більшої гнучкості, і для нашої задачі залежність успішної роботи ГА від мутації більше ніж від кросинговера; 3) припущення 2 пов'язане з тим, що існують об'єктивні особливості вирішення завдань, пов'язаних із формуванням контурів КрБ ІКС. Це зумовило великі розміри хромосом, і навіть наявність обмежень.

Отже, змінна мутація, для якої характерні елементи випадковості на ранніх стадіях роботи алгоритму, буде кращою з погляду пошуку оптимального складу рюкзака.

У процесі обчислювальних експериментів розглядалися два види мутацій. Перший вид – постійна мутація. У цьому випадку кожна позиція в хромосомі з ймовірністю 1% буде інвертуватися. Другий – змінна мутація. І тут ймовірність мутації буде залежати від поточних потреб ГА. Коефіцієнт мутації варіюватиметься в діапазоні 1-6%.

У розглянутому ГА з відносною фітнес-функцією у якості фітнес-функції використовувалася не сума ефективностей ЗЗІ, які, власне, і становили хромосому, а застосовувалася сума відношень ефективностей або інтегральних показників ЗЗІ, що входять до класу.

Для цього випадковим чином інвертуватимемо два двійкових розряди у хромосомі:

$$\begin{aligned} &func\ M(PA) := \ foreach\ Ch(X)\ from\ PA\ do\ Ch(X).G = \\ &= xor(Ch(X).G, 1 << rand(0, NC)). \end{aligned} \tag{9}$$

Тоді функцію селекції, тобто відбору найкращих носіїв можна подати так:

$$func\ S(PA) := return\ PA.sort(\ ).slice(1, K). \tag{10}$$

Зауважимо, що для скорочення запису та зменшення популяції залишаємо лише K носіїв, які дають найбільший результат щодо функції корисності (U).

Перед застосуванням селекції попередньо обчислюємо $Ch(X).C$ та $Ch(X).R$ для популяції. Відповідно до [5,7] прийнято, що початкова популяція як мінімум включає два екземпляри. Тоді кожна епоха в ГА [6,7] буде складатись з послідовного застосування основних функцій, розглянутих вище. Відповідно отримаємо:

$$func\ E(\ ) := ((PA = K(PA), M(PA)), (P = S(PA))). \tag{11}$$

В результаті роботи СППР визначається оптимальний набір ЗЗІ для вузла ІКС, виходячи з інтегрального показника кожного ЗЗІ з відповідного класу та вартості цього ЗЗІ. В якості інтегрального показника (ІнП) ЗЗІ прийнято так званий індекс якості або ступінь досяжності бажаних цілей для конкретного ЗЗІ [23]. Також ІнП можна трактувати як узагальнений показник якості найважливіших характеристик конкретного ЗЗІ. При цьому вважаємо, що ІнП обчислено як ступінь близькості параметрів ЗЗІ до ідеальних характеристик простору виділених часткових показників [23]. Для розрахунку

ISSN 2663 - 4023

ІнП ЗЗІ використовувалася наступна залежність:

$$IND_j = \sum_{i=1}^{k} \beta_i \cdot a_{ij}, \quad (12)$$

де β_i – вага критерію, що використовується для оцінки i -го ЗЗІ (наприклад для фаєрволів можливо використовувати такі критерії: тест фаєрволів на захист від внутрішніх атак; тест фаєрволів на захист від зовнішніх атак; тест персональних IDS/IPS на захист від атак на вразливі застосунки; наявність документації та ін);

a_{ij} – ступінь досягнення заданого рівня захисту вузла для j -ого класу атак;

k – кількість класів ЗЗІ для конкретного типу вузла ІКС.

На основі аналізу та розрахунку ІнП для класів ЗЗІ можна скласти уявлення про максимальне значення ІнП на основі вагових коефіцієнтів для класів ЗЗІ без застосування експертного методу їх формування.

МЕТОДИКА ДОСЛІДЖЕННЯ

Програмна реалізація обчислювального ядра СППР, моделей, описаних вище, а також алгоритму, що реалізує задачу пошуку оптимальної стратегії формування наборів ЗЗІ для контурів КрБ ІКС, виконана мовою C# в середовищі Microsoft Visual Studio 2019. Концепція СППР полягає в тому, що на основі наявних архітектури ІКС, сукупності класів та ЗЗІ, а також застосовуючи на першому етапі метод аналізу ієрархій (метод Т. Сааті) за допомогою ГА вирішується завдання щодо формування оптимального варіанту розміщення ЗЗІ у кожному з ключових вузлів ІКС.

Після введення всіх даних, що стосуються загального набору предметів для забезпечення КрБ і ЗІ (тобто хромосом), які потенційно можуть бути застосовані на вузлі ІКС для забезпечення необхідного рівня кібернетичної безпеки та налаштування параметрів розрахунку починає роботу безпосередньо ГА. Він формує популяцію, що складається з 25 хромосом. Далі обчислюється фітнес-функція (ефективність) кожної хромосоми. У ГА застосований k -точковий кросинговер, де k – кількість класів точок розміщення ЗЗІ для ІКС.

Фактично вирішується задача про формування мультирюкзака. СППР розроблено з використанням об'єктно-орієнтованого підходу.

Застосований у обчислювальному ядрі СППР ГА відрізняється від стандартного ГА наступними ознаками: хромосоми представлені у вигляді матриць, елементи яких є числами, які відповідають номерам ЗЗІ у вузлах ІКС; застосований k -точковий кросинговер. Використовувалася змінна мутація, тобто ймовірність мутації може адаптивно змінюватися під час роботи ГА залежно від потреб. Фітнес-функція представлена як сума коефіцієнтів ефективності. При цьому, окрім традиційних абсолютних показників ефективності ЗЗІ (які інтегровані в інтегральному показнику) враховуються сумарна величина ризиків від втрати інформації та вартісні показники для кожного класу ЗЗІ.

ISSN 2663 - 4023

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Для перевірки адекватності алгоритму та СППР щодо багатокритеріальної оптимізації розміщення ЗЗІ по вузлах ІКС були проведені відповідні обчислювальні експерименти, див. рис. 1-4.

Обчислювальні експерименти проводилися для випадково згенерованих наборів ЗЗІ. Порівнювалась ефективність роботи модифікованого ГА, методу гілок та меж, жадібного алгоритму.

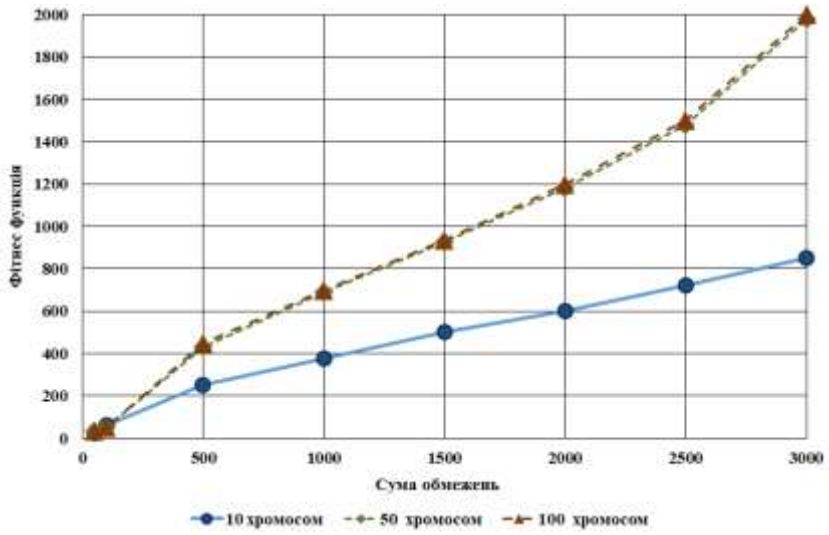

Рис. 1. Порівняння ефективності алгоритму для різної кількості хромосом у популяції

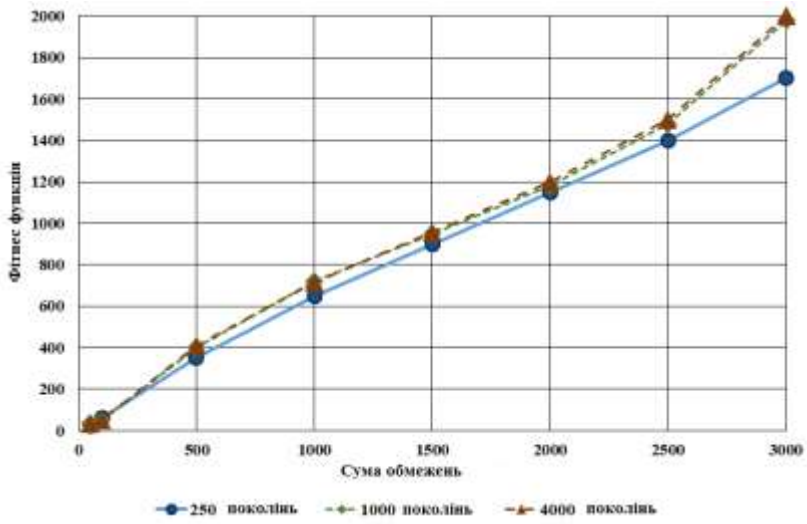

Рис. 2. Порівняння ефективності алгоритму для різної кількості поколінь

ISSN 2663 - 4023

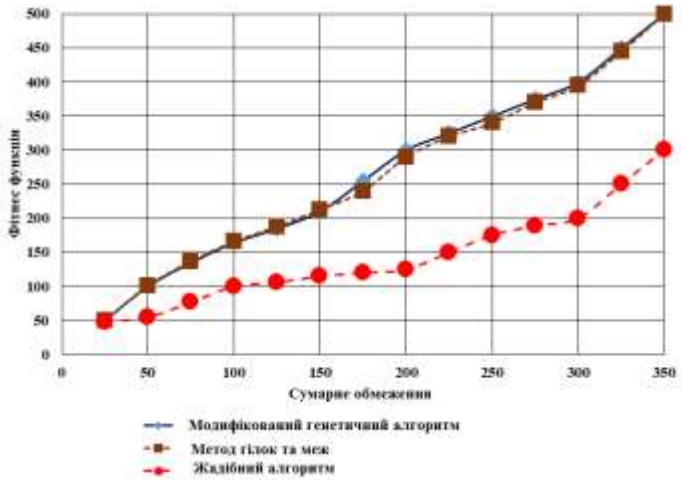

Рис. 3. Результати обчислювальних експериментів у порівнянні ефективності алгоритмів, що використовуються в СППР

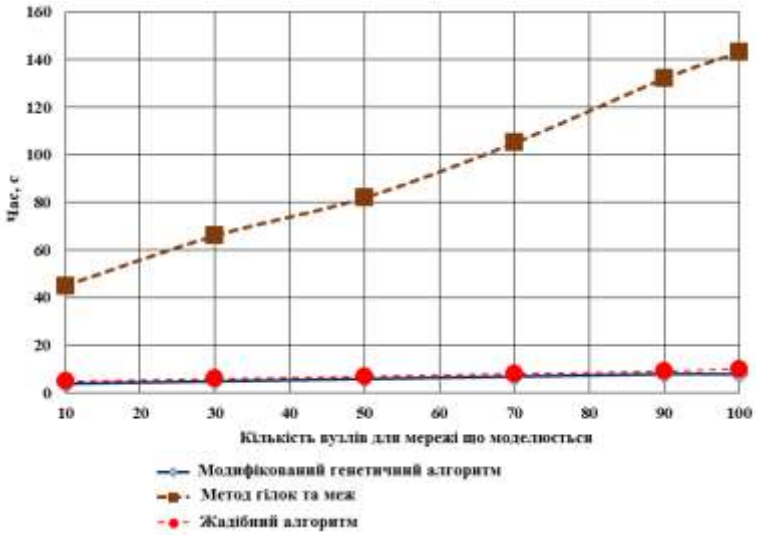

Рис. 4. Результати обчислювальних експериментів у порівнянні з часом роботи алгоритмів

На графіках рис. 1 показані результати досліджень ГА в ході пошуку оптимальної кількості хромосом у популяції для вирішення поставленої задачі з пошуку оптимальних наборів засобів захисту інформації для ІКС.

Як показали обчислювальні експерименти, оптимального результату не вдається досягти, якщо кількість хромосом невелика (менше 20). Однак, при збільшенні їх кількості до понад 22–25, ефективність роботи алгоритму не підвищилась. На основі серії більш ніж із 500 обчислювальних експериментів було встановлено, що для остаточної версії алгоритму та його програмної реалізації в СППР достатньо брати 25 хромосом у популяції.

Були також проведені серії обчислювальних експериментів у ході пошуку оптимальної кількості поколінь для ГА, що розглядається (див. рис 2). В процесі

перевірки встановлено, що ефективність ГА не збільшується після подолання межі в 450–500 поколінь. Ця обставина дає підстави обмежити кількість поколінь у ГА для нашої СППР числом 500 поколінь.

У ході обчислювальних експериментів встановлено, що ГА відрізняється досить високою ефективністю, а також швидкодією (див. рис. 3, 4).

Встановлено, що час, витрачений на розв'язання задачі з використанням ГА, приблизно у 16–25 разів менший у порівнянні з показниками методу гілок та меж. Жадібний алгоритм істотно поступається як ГА так і методу гілок та меж з точки зору пристосованості до вирішення багатокритеріальної оптимізаційної задачі з урахуванням обмежень, що накладаються, і кількості змінних.

Таким чином, проведений аналіз показує, що розроблені моделі та алгоритм є достовірними, а результати обчислювальних експериментів багаторазово підтверджені серіями практичних реалізацій.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Таким чином, у статті викладено такі результати:

1. Розглянуто можливість модифікації генетичного алгоритму (ГА) на вирішення завдання пов’язаного з підбором і оптимізацією варіантів конфігурацій засобів захисту (ЗЗІ) для контурів безпеки інформаційно-комунікаційних систем. Наукова новизна роботи полягає в тому, що в ГА як критерії для оптимізації складу ЗЗІ, запропоновано використовувати сумарну величину ризиків від втрати інформації, інтегральні показники ЗЗІ, а також вартісні показники для кожного класу ЗЗІ. Генетичний алгоритм у задачі оптимізації вибору складу ЗЗІ для ІКС розглянутий як варіація задачі, пов'язаної з мультивибором. У такій постановці оптимізація розміщення ЗЗІ за контурами захисту ІКС розглянута як модифікація комбінаторного завдання про рюкзак. Практична цінність дослідження полягає у реалізації системи підтримки прийняття рішення на основі запропонованої модифікації ГА.

2. Виконані обчислювальні експерименти щодо вибору раціонального програмного алгоритму реалізації моделі. Як раціональний варіант запропоновано використовувати модифікацію ГА. Показано, що реалізація ГА у СППР дозволяє прискорити пошук оптимальних варіантів розміщення засобів КрБ для ІКС.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Okutan, A., Yang, S. J., McConky, K., Werner, G. (2019). CAPTURE: Cyberattack Forecasting Using Non-Stationary Features with Time Lags. У 2019 IEEE Conference on Communications and Network Security (CNS). IEEE. https://doi.org/10.1109/cns.2019.8802639.

2 Barreto, C., Koutsoukos, X. (2019). Design of Load Forecast Systems Resilient Against Cyber-Attacks. У *Lecture Notes in Computer Science* (с. 1–20). Springer International Publishing. https://doi.org/10.1007/978-3-030-32430-8_1

3 Chandra, Y., Mishra, P. K. (2018). Design of Cyber Warfare Testbed. У Advances in Intelligent Systems and Computing (с. 249–256). Springer Singapore. https://doi.org/10.1007/978-981-10-8848-3_24.

4 Sándor, H., Genge, B., Szántó, Z., Marton, L., Haller, P. (2019). Cyber attack detection and mitigation: Software Defined Survivable Industrial Control Systems. *International Journal of Critical Infrastructure Protection, 25*, 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* (c. 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. https://doi.org/10.1109/tii.2019.2891261.

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. https://doi.org/10.1016/j.comcom.2019.03.008.

10 Shang, Q., Chen, L., Wang, D., Tong, R., Peng, P. (2019). Evolvable Hardware Design of Digital Circuits Based on Adaptive Genetic Algorithm. У Advances in Intelligent Systems and Computing (c. 791–800). Springer International Publishing. https://doi.org/10.1007/978-3-030-25128-4_97.

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* (c. 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 GECCO '19: Genetic and Evolutionary Computation Conference. ACM. https://doi.org/10.1145/3319619.3326853.

13 Aleksieva, Y., Valchanov, H., Aleksieva, V. (2019). A volumetric system is based on the example for the client detection. 2019 16th Conference on Electrical Machines, Drives and Power Systems (ELMA) (c. 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 algoritm 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. (2018). 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. https://doi.org/10.1007/s12652-018-0906-0.

18 Llanso, T., McNeil, M., Noteboom, C. (2019). Multi-Criteria Selection of Capability-Based Cybersecurity Solutions. In *Hawaii International Conference on System Sciences.* https://doi.org/10.24251/hicss.2019.879.

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).* IEEE. https://doi.org/10.1109/hpcc/smartcity/dss.2019.00251.

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

21 Yan, D., Liu, F., Zhang, Y., Jia, K., Zhang, Y. (2018). Characterizing the Optimal Attack Strategy Decision in Cyber Epidemic Attacks with Limited Resources. In *International Conference on Science of Cyber Security* (pp. 65-80). Springer, Cham.

22 Lee, Y., Choi, T. J, Ahn, CW (2019). Multi-objective evolutionary approach до selective security solutions. *CAAI Transactions on Intelligence Technology*, *2*(2), 64-67.

23 Akhmetov, B., Lakhno, V., Akhmetov, B., & Alimseitova, Z. (2018). Development of Sectoral Intellectualized Expert Systems and Decision Making Support Systems in Cybersecurity. У *Intelligent Systems in Cybernetics and Automation Control Theory* (c. 162–171). Springer International Publishing. https://doi.org/10.1007/978-3-030-00184-1_15.

24 Dewri, R., Poolsappasit, N., Ray, I., Whitley, D. (2007). Optimal security hardening using multi-objective optimization on attack tree models of networks. У *the 14th ACM conference*. ACM Press. https://doi.org/10.1145/1315245.1315272.

25 Saurabh, P., Verma, B., Sharma, S. (2012). Biologically Inspired Computer Security System: The Way Ahead. У Communications in Computer and Information Science (c. 474–484). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-34135-9_46.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (17), 2022
ISSN 2663 - 4023

Valerii A. Lakhno
Dr. Tech. Sc., Professor, Head of the Department of Computer System, Networks and Cybersecurity
National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine
ORCID ID 0000-0001-9695-4543
valss21@ukr.net

Volodimir P. Maliukov
Dr. Phys.-Math. Sc., Professor, Professor of the Department of Computer System, Networks and Cybersecurity
National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine
ORCID ID 0000-0002-7533-1555
volod.malyukov@gmail.com

Larysa Komarova
Dr. Tech. Sc., Professor, director of the Educational Scientific Institute of Information Security and Strategic Communications of the National Academy of the Security Service of Ukraine, Kyiv, Ukraine
ORCID ID 0000-0002-9776-0879
lacosta_k@ukr.net.

Dmytro Y. Kasatkin
Cand. Pedag. Sc. (Ph.D.), Docent, Associate Professor at the Department of Computer System, Networks and Cybersecurity
National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine
ORCID ID 0000-0002-2642-8908
d.kasatkin@nubip.edu.ua

Tetiana Y. Osypova
Cand. Pedag. Sc. (Ph.D), Associate Professor of the Department of Computer System, Networks and Cybersecurity
National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine
ORCID ID 0000-0002-9199-3436
t_osipova@nubip.edu.ua

Yehor Chasnovskyi
Postgraduate Student of the Department of Computer System, Networks and Cybersecurity
National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine
ORCID ID 0000-0002-1848-4221
egor.chasnovskii@gmail.com

OPTIMIZATION OF PLACEMENT OF INFORMATION PROTECTION MEANS BASED ON THE APPLICATION OF A GENETIC ALGORITHM

Abstract. The article considers the possibilities of modifying the genetic algorithm (GA) for solving the problem of selecting and optimizing the configurations of information protection means (IPR) for security circuits of information and communication systems (ICS). The scientific novelty of the work lies in the fact that in GA, as criteria for optimizing the composition of IPR, it is proposed to use the total value of risks from loss of information, as well as the integral indicator of IPR and cost indicators for each class of IPR. The genetic algorithm in the task of optimizing the selection of the composition of the IPR for ICS is considered as a variation of the problem associated with multiple selection. In such a statement, the optimization of the placement of IPR along the contours of ICS protection is considered as a modification of the combinatorial problem about the backpack. The GA used in the computing core of the decision support system (DSS) differs from the standard GA. As part of the GA modification, chromosomes are presented in the form of matrices, the elements of which are numbers that correspond to the numbers of the IPR in the ICS nodes. In the process of GA modification, k-point crossover was applied. The fitness function is represented as the sum of efficiency coefficients. At the same time, in addition to the traditional absolute indicators of the effectiveness of IPR, the total value of risks from loss of information, as well as cost indicators for each class of IPR are taken into account. The practical value of the research lies in the implementation of the DSS based on the proposed modification of the GA. Computational

experiments on the selection of a rational software algorithm for the implementation of the model were performed. It is shown that the implementation of GA in DSS allows to speed up the search for optimal options for the placement of cyber security means (CS) for ICS by more than 25 times. This advantage allows not only to perform a quick review of various options of hardware and software IPR and their combinations for ICS, but also to further combine the proposed algorithm with existing models and algorithms for optimizing the composition of ICS cyber security circuits. Potentially, such a combination of models and algorithms will provide an opportunity to quickly rebuild ICS protection, adjusting its profiles in accordance with new threats and classes of cyberattacks.

Keywords: decision support system, information protection tools, multi-criteria optimization, knapsack problem, genetic algorithm.

REFERENCES

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). IEEE. https://doi.org/10.1109/cns.2019.8802639.

2 Barreto, C., Koutsoukos, X. (2019). Design of Load Forecast Systems Resilient Against Cyber-Attacks. In *Lecture Notes in Computer Science* (pp. 1–20). Springer International Publishing. https://doi.org/10.1007/978-3-030-32430-8_1

3 Chandra, Y., Mishra, P. K. (2018). Design of Cyber Warfare Testbed. In Advances in Intelligent Systems and Computing (pp. 249–256). Springer Singapore. https://doi.org/10.1007/978-981-10-8848-3_24.

4 Sándor, H., Genge, B., Szántó, Z., Marton, L., Haller, P. (2019). Cyber attack detection and mitigation: Software Defined Survivable Industrial Control Systems. *International Journal of Critical Infrastructure Protection*, *25*, 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. https://doi.org/10.1109/tii.2019.2891261.

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. https://doi.org/10.1016/j.comcom.2019.03.008.

10 Shang, Q., Chen, L., Wang, D., Tong, R., Peng, P. (2019). Evolvable Hardware Design of Digital Circuits Based on Adaptive Genetic Algorithm. In Advances in Intelligent Systems and Computing (pp. 791–800). Springer International Publishing. https://doi.org/10.1007/978-3-030-25128-4_97.

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 GECCO '19: Genetic and Evolutionary Computation Conference. ACM. https://doi.org/10.1145/3319619.3326853.

13 Aleksieva, Y., Valchanov, H., Aleksieva, V. (2019). A volumetric system is based on the example for the client detection. 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 algoritm 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. (2018). 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. https://doi.org/10.1007/s12652-018-0906-0.

18 Llanso, T., McNeil, M., Noteboom, C. (2019). Multi-Criteria Selection of Capability-Based Cybersecurity Solutions. In *Hawaii International Conference on System Sciences.* https://doi.org/10.24251/hicss.2019.879.

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).* IEEE. https://doi.org/10.1109/hpcc/smartcity/dss.2019.00251.

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

21 Yan, D., Liu, F., Zhang, Y., Jia, K., Zhang, Y. (2018). Characterizing the Optimal Attack Strategy Decision in Cyber Epidemic Attacks with Limited Resources. In *International Conference on Science of Cyber Security* (pp. 65-80). Springer, Cham.

22 Lee, Y., Choi, T. J, Ahn, CW (2019). Multi-objective evolutionary approach до selective security solutions. *CAAI Transactions on Intelligence Technology*, *2*(2), 64-67.

23 Akhmetov, B., Lakhno, V., Akhmetov, B., & Alimseitova, Z. (2018). Development of Sectoral Intellectualized Expert Systems and Decision Making Support Systems in Cybersecurity. In *Intelligent Systems in Cybernetics and Automation Control Theory* (pp. 162–171). Springer International Publishing. https://doi.org/10.1007/978-3-030-00184-1_15.

24 Dewri, R., Poolsappasit, N., Ray, I., Whitley, D. (2007). Optimal security hardening using multi-objective optimization on attack tree models of networks. In *the 14th ACM conference.* ACM Press. https://doi.org/10.1145/1315245.1315272.

25 Saurabh, P., Verma, B., Sharma, S. (2012). Biologically Inspired Computer Security System: The Way Ahead. In Communications in Computer and Information Science (pp. 474–484). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-34135-9_46.