DOI: 10.25140/2411-5363-2021-3(25)-138-149
УДК 004.056.57-048.34

Валерій Лахно[1], Дмитро Касаткін[2], Андрій Блозва[3], Борис Гусєв[4], Тетяна Осипова[5], Юрій Матус[6]

[1]доктор технічних наук, професор, завідувач кафедри комп'ютерних систем, мереж та кібербезпеки
Національний університет біоресурсів та природокористування України (Київ, Україна)
E-mail: valss21@ukr.net. **ORCID:** http://orcid.org/0000-0001-9695-4543

[2]кандидат педагогічних наук, доцент, доцент кафедри комп'ютерних систем, мереж та кібербезпеки
Національний університет біоресурсів та природокористування України (Київ, Україна)
E-mail: d.kasatkin@nubip.edu.ua. **ORCID:** http://orcid.org/0000-0002-2642-8908

[3]кандидат педагогічних наук, доцент кафедри комп'ютерних систем, мереж та кібербезпеки
Національний університет біоресурсів та природокористування України (Київ, Україна)
E-mail: andriy.blozva@nubip.edu.ua. **ORCID:** http://orcid.org/0000-0002-4377-0916

[4]кандидат технічних наук, доцент, доцент кафедри комп'ютерних систем, мереж та кібербезпеки
Національний університет біоресурсів та природокористування України (Київ, Україна)
E-mail: gusevbs@nubip.edu.ua. **ORCID:** http://orcid.org/0000-0003-1658-7822

[5]кандидат педагогічних наук, доцент кафедри комп'ютерних систем, мереж та кібербезпеки
Національний університет біоресурсів та природокористування України (Київ, Україна)
E-mail: t_osipova@nubip.edu.ua. **ORCID:** http://orcid.org/0000-0002-9199-3436

[6]старший викладач кафедри комп'ютерних систем, мереж та кібербезпеки
Національний університет біоресурсів та природокористування України (Київ, Україна)
E-mail: umatus@nubip.edu.ua. **ORCID:** http://orcid.org/0000-0003-0974-4789

ОПТИМІЗАЦІЯ ВИБОРУ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ ЗА ДОПОМОГОЮ ГЕНЕТИЧНОГО АЛГОРИТМУ

У статті запропоновано переглянути завдання визначення оптимального складу комплексів засобів захисту інформації (ЗЗІ) для узгоджено розподіленої обчислювальної системи (РОС) за допомогою модифікованого генетичного алгоритму (МГА). Як цільову функцію запропоновано критерій максимуму ймовірності успішної протидії ЗЗІ реалізації всіх цілей порушником. На відміну від існуючих підходів, запропонований у роботі МГА і відповідна цільова функція, реалізують кросинговер для випадків, коли пари батьків підбираються виходячи із принципу «елітарності» однієї особини та «випадковості» другої. Показано, що реалізація МГА дозволила прискорити пошук оптимальних варіантів розміщення ЗЗІ по вузлах РОС у 7–15 разів.

Ключові слова: *оптимізація; модифікований генетичний алгоритм; засоби захисту інформації; об'єкт інформатизації; розподілена обчислювальна система.*
Рис.: 4. Бібл.: 25.

Актуальність теми дослідження. При проєктуванні та реалізації комплексних систем захисту інформації (КСЗІ) для розподілених обчислювальних систем (РОС) різних об'єктів інформатизації (ОБІ) величезне значення мають методи автоматизованого проєктування. Особливо ці методи важливі для проектування контурів інформаційної безпеки (ІБ) критично важливих комп'ютерних систем (КВКС), оскільки саме автоматизація та оптимізація розмірів різних засобів захисту інформації (ЗЗІ) за допомогою КВКС дозволяє створювати високоефективні системи ІБ у короткі терміни та за порівняно низьких витрат.

Тенденція зростання складності сценаріїв проведення успішних кібернетичних атак, спрямованих проти різних ОБІ, у тому числі КВКС, а також динамічна зміна ландшафту кібернетичних загроз, призводить до того, що необхідно постійно вдосконалювати КСЗІ [1; 2]. У свою чергу, це збільшує трудомісткість проєктування як усієї КСЗІ загалом, так і окремих її складових. Фактично сторона захисту зіткнулася з ситуацією постійного зростання розмірності, що вирішується під час проєктування КСЗІ задачі.

Таким чином, задача автоматизації проєктування КСЗІ для РОС не втрачає своєї актуальності, а пошук методів, здатних скоротити кількість ітерацій у циклі проєктування КСЗІ, продовжується.

Постановка проблеми. Актуальною науково-практичною проблемою в процесі проектування КСЗІ для РОМ залишається автоматизація вибору складу апаратно-технічних засобів для різних контурів інформаційної безпеки. Для вирішення цієї проблеми необхідно продовжити пошук алгоритмів визначення оптимального складу комплексів засобів захисту інформації (ЗЗІ), наприклад, шляхом удосконалення генетичного алгоритму.

Аналіз останніх досліджень і публікацій. Особливу роль на етапах конструкторського проектування КСЗІ для РОС займають завдання оптимізації розміщення окремих ЗЗІ (а також методів захисту) по вузлах РОС [3; 4]. На різних етапах проєктування КСЗІ для РОС традиційно подібні багатокритеріальні оптимізаційні задачі розв'язуються різними точними методами, наприклад, гілок та меж, лінійного програмування та ін. Застосування точних методів вирішення подібних завдань, частіше всього призводить до зростання витрат як тимчасових, так і обчислювальних.

У роботі [5] представлені різні формулювання завдань оптимального розподілу ресурсів між функціями управління механізмами ІБ ОБІ. Було запропоновано кілька постановок завдань розподілу ресурсів сторін захисту ОБІ. Відповідні засоби призначені для застосування як на стадії проектування КСЗІ для ОБІ, так і на стадії удосконалення та розвитку його контурів ІБ.

Автори [6] виділяють сім основних функцій забезпечення ІБ ОБІ. Відповідно, було запропоновано два підходи до деталізації та формалізації розподілу ресурсів між різними функціями ЗЗІ. Перший підхід базується на необхідності обліку складу та кількості ЗЗІ. Другий підхід – аналіз узагальнених закономірностей і зв'язків між вкладеними в ЗЗІ та ефективністю їх застосування для ОБІ. Автори робіт [5; 6] не наводять конкретні приклади застосування запропонованих оптимізаційних моделей.

У роботах [7; 8] розглянуті моделі, у яких розподіл ресурсів між об'єктами захисту для ОБІ виконано на основі ігрової моделі та принципу рівної захищеності об'єктів. Рішення достатньо трудомістке, оскільки для кожного ігрового персоналу необхідно розв'язувати задачу лінійного програмування за умови фіксованого рішення іншого гравця.

У [9; 10] показано, що ускладнення сценаріїв протистояння сторони захисту ОБІ та атакуючих, відбивається на структурі математичних моделей, які повинні відображати нові умови та ситуації що виникають.

Одним із напрямів досліджень за цією проблемою, пов'язаною з підвищенням ефективності вирішення оптимізаційної задачі, є еволюційні та генетичні алгоритми (ГА) [11].

У роботах [11; 12] показано, що ГА досить успішно можуть застосовуватися для вирішення задач структурної та параметричної оптимізації контурів ІБ для ОБІ.

У роботі [13] наведено розв'язання оптимізаційної задачі побудови ефективної системи захисту інформації за допомогою ГА. Однак не описано, як саме обиралася цільова функція.

У роботі [14] розглядається можливість застосування систем підтримки прийняття рішень для завдання розміщення засобів технічного виявлення для захисту інформації на основі ГА. Проте, докладного рішення автори не наводять.

У роботі [15] вивчається можливість застосування модифікованого генетичного алгоритму для вирішення завдання раціонального вибору апаратно-програмних засобів захисту інформації (ЗЗІ) і динамічного керування конфігураціями засобів на різних рівнях безпеки радіотехнічних систем, а також інформаційних систем. Але, як і в роботі [15], обґрунтованого розв'язання завдання авторами не наведено.

Новим етапом розвитку теорій ГА стали гібридні системи [16; 17]. Такі системи базуються на поєднанні різних наукових напрямів. Існує декілька способів гібридизації. Один з таких способів – поєднання нечітких і ГА. Тобто при такому підході методи нечіткої логіки застосовують для налаштування параметрів ГА.

Виділення недосліджених частин загальної проблеми. На основі вищезазначеного можна констатувати, що до сьогодні залишається актуальним завдання розробки інтегрованих методів вирішення завдань, пов'язаних із розміщенням ЗЗІ по контурам РОС та

оптимізацією ресурсів сторони захисту (точніше коаліції захисників). Це дозволяє паралельно шукати рішення оптимізаційної задачі з розміщення окремих ЗЗІ по контурах РОС, враховуючи обмеження.

Метою статті є проведення досліджень модифікованого ГА для автоматизації підбору ЗЗІ на вузлах РОС шляхом максимізації ймовірності успішної протидії ЗЗІ на вузлах РОС реалізації всіх задач атакуючої сторони.

Для досягнення мети дослідження необхідно вирішити такі завдання:

- розробити модифікований ГА (МГА) для вирішення завдань максимізації ймовірності успішної протидії ЗЗІ на вузлах РОС реалізації всіх задач атакуючої сторони та оптимізації розміщення ЗЗІ на вузлах РОС;

- розробити та протестувати прикладне програмне забезпечення на базі модифікованого ГА (далі МГА) для вирішення оптимізаційної задачі щодо розміщення окремих ЗЗІ по контурам РОС, враховуючи обмеження.

Виклад основного матеріалу. Трудність постановки задачі насамперед пов'язана з вибором цільової функції (ЦФ – *W*). Це спричинене тим, що однією з головних цілей розміщення ЗЗІ по вузлах РОС для конкретного ОБІ, є підвищення його метрик інформаційної безпеки.

Згідно з метою дослідження як ЦФ прийнято значення ймовірності успішної протидії ЗЗІ на вузлах РОС реалізації всіх завдань атакуючої сторони (наприклад, у грошовому еквіваленті). Для цього необхідно визначити величину:

$$W = P^{з}(X) = \max_{X} \prod_{p_a=1}^{PA} \left(1 - \sum_{j \in G^{p_a}_{I^{p_a}-1}} P_j^{p_a} p_{jn_{p_a}} \right), \qquad (1)$$

при обмеженнях: $C^{з} \le C^{з}_{доп}$,

$$\sum_{j \in G^{p_a}_{I^{p_a}-1}} P_j^{p_a} p_{jn_{p_a}} \le P^{p}_{p_a доп} \;\; p_a = 1,2,...,PA$$

$$x_{jm} = \{0,1\}, (j \in B_{p_a}, j \ne 0; m \in N_j^{p_a};\;\; p_a = 1,2,...,PA)$$

де $C^{з}, C^{з}_{доп}$ – відповідно, базова вартість і максимально допустима вартість ЗЗІ для вузла РОС; p_a – ціль кібернетичної атаки на вузол РОС; B_{p_a} – множина номерів кібернетичних загроз для вузла РОС; $P_j^{p_a}$ – ймовірність реалізації тими, хто атакує p_a – цілі; $P^{p}_{p_a доп}$ - допустиме значення ймовірності реалізації атакуючими p_a – цілі; $p_{jn_{p_a}} = \rho_l^{p_a} \cdot g_l^{p_a}$; $g_j^{p_a}$ – ймовірність подолання *j - го* ЗЗІ при спробі атакуючих досягнути p_a – цілі; $\rho_l^{p_a}$ – ймовірність переходу атакуючих на більш високий рівень (l) у станах вузла РОС; $G_i^{p_a}$ - множина станів вузла РОС при спробах атакуючих досягнути p_a – цілі атаки; I^{p_a} – кількість рівнів графа станів вузла РОС, що описує дії атакуючих при спробі досягнути p_a – й цілі атаки; $N_j^{p_a}$ - множина номерів ЗЗІ, які можуть бути застосовані для протидії цілі p_a на j контурі захисту РОС; m – засоби або міра захисту інформації для j – го контуру ІБ ОБІ.

Припустимо, що *PO* – деяка популяція на етапі *t* рішення описаної виразом (1) оптимізаційної задачі. Тобто $PO_t = \{ch_1, ch_2, ..., ch_z\}$, де ch_z – хромосома популяції, що аналізується; $t = [1, N]$; $z = [1, M]$ – відповідно, *N, M* - кількість популяцій і кількість хромосом (ch) в популяції.

Отже, множина рішень ГА для цієї задачі може бути описана так:

$$Ch = \{ch_{zt}; t = 1, 2, ..., N; \quad z = 1, 2, ..., M\}. \tag{2}$$

Цільову функцію (*W*) представимо як нормований адитивний критерій. Цей адитивний критерій повинен включати в себе оцінки кількості вузлів РОС, що аналізує ОБІ з найменшими показниками метрик ІБ та сумарною вартістю всіх ЗЗІ, які необхідно використовувати:

$$W = k_1 \cdot W_1 + k_2 \cdot W_2, \tag{3}$$

де k_1, k_2 – вагові коефіцієнти для локальних критеріїв.

За допомогою вагового коефіцієнта k_1 враховуємо важливість впливу на загальні показники захищеності ОБІ числа критично важливих вузлів РОС. А з допомогою k_2 - вплив вартості окремого ЗЗІ на вузлі.

Крім того, W_1 – критерій для оцінювання кількості вузлів РОС, на яких метрики ІБ низькі або відсутні, W_2 – критерій оцінювання сумарної вартості усіх ЗЗІ для РОС або, іншими словами, це ресурси, необхідні коаліції сторони захисту для досягнення своїх цілей.

Для вирішення задачі необхідно максимізувати значення ЦФ – *W*, тобто

$$W(Ch) \to \max W(ch_{opt}) = \max W(ch_{ij}), \quad ch_{ij} \subset Z. \tag{4}$$

З урахуванням робіт [11; 18–20] пропонується така процедура вирішення цих задач розміщення ЗЗІ по вузлах РОС для ОБІ.

Ця методика застосування алгоритму описується так.

1. Введення початкових даних (кількість вузлів РОС, кількість ЗЗІ для кожного вузла, інтегральний показник [21] ефективності ЗЗІ та ін.).

2. Задаємо варіант початкового розміщення ЗЗІ для вузла РОС.

3. Формуємо початкову популяцію (побудова початкової множини рішень).

4. Задаємо початкові значення керуючих параметрів для ГА.

5. За рахунок застосування нечітких генетичних операторів, реалізуємо процедуру покращення якості розміщення ЗЗІ по вузлах РОС. Для цього застосовуємо такі оператори:

а) для вибору рішень;

б) для вибору стратегії інвестування в захист вузла і РОС в цілому (на основі робіт [11; 22]);

в) застосування класичних операторів ГА;

d) для відбору кращих рішень;

д) для формування нових множин розв’язків.

6. Реалізуємо заданий ГА за попереднім відбором ЗЗІ для вузла РОС.

7. Розрахунок одержаного значення цільової функції.

8. Перевіряємо виконання критерію зупинки роботи ГА.

9. Відслідковуємо роботу нечіткого логічного контролера.

10. Якщо необхідно, то виконуємо повернення до етапу 5.

Одержане значення ЦФ (*W*) перевіряється на можливе покращення рішення. Крім того, додаткова перевірка виконується за показниками кількості заданих ітерацій.

Як початкові дані прийняті: кількість вузлів РОС; кількість ЗЗІ для кожного вузла; інтегральний показник ефективності ЗЗІ; ступінь критичності вузла РОС для бізнес-процесів ОБІ.

Після введення початкових даних та їх кодування, наприклад, у бінарному вигляді, отримуємо початкову популяцію ГА. В якості механізму отримання нових рішень застосовується операція кросинговеру. Розраховується значення ЦФ (*W*). Значення проходить перевірку. Якщо ЦФ пройшла перевірку (за інтегральними метриками безпеки, наприклад, ймовірність успішної протидії ЗЗІ на вузлах РОС реалізації всіх завдань атакуючої сторони не повинна бути менше 0,95), то алгоритм завершує свою роботу.

З метою покращення якості розміщення ЗЗІ по вузлам РОС задіяний нечіткий ГА. В ньому у відповідності з роботою [23] застосовується кодування розв'язків за допомогою дійсних чисел. У такому випадку хромосома (ch_{ij}) – вектор дійсних чисел. Довжина (ch_{ij}) еквівалентна довжині вектору розв'язку задачі, що розглядається щодо багатокритеріальної оптимізації КСЗІ для ОБІ.

При реалізації кросинговера пари батьків підбираються за принципом «елітарності» однієї особини та «випадковості» другої. Розв'язки, які були отримані в результаті кросинговера, а також вихідні рішення, сформують так звану підпопуляцію. Потім з підпопуляції відберемо найкращі особини.

Для реалізації оператора кросинговера прийняті наступні припущення.

Нехай $Ch=(ch_1,...,ch_n)$ і $ChY=(chy_1,...,chy_n)$ – хромосоми для яких використовується кодування за допомогою дійсних чисел. Ці хромосоми обрані на основі визначеної стратегії. Стратегія відповідає за результат кросинговеру. У результаті кросинговеру будуть отримані нащадки:

$$De_1 = \left(de_1^1,..., de_n^1\right) \text{ або } De_2 = \left(de_1^2,..., de_n^2\right), \quad (5)$$

де de_i^1 – випадково відібране число на інтервалі $\left[x_i^1, z_i^1\right]$.

При цьому $x_i^1 = \max\{a_i, ch_i - H\cdot\alpha\}$ і $z_i^1 = \min\{b_i, ch_i + H\cdot\alpha\}$,

відповідно, de_i^2 – випадково відібране число на інтервалі $\left[x_i^2, z_i^2\right]$,

a, b – межі арифметичного оператора кросинговеру,

При цьому $x_i^2 = \max\{a_i, chy_i - H\cdot\alpha\}$ і $x_i^2 = \max\{a_i, chy_i - H\cdot\alpha\}$ $z_i^2 = \min\{b_i, chy_i + H\cdot\alpha\}$, де $H = \left[ch_i - chy_i\right]$, α - коефіцієнт налаштування арифметичного оператора кросинговеру.

Перевагою такого варіанту реалізації кросинговеру є те, що враховується різноманітність популяцій рішень. Крім того, враховується ступінь «близькості» нових рішень до батьківських.

На рис. 1 c_{ch}^1 та c_{ch}^2 – хромосоми, які відібрані для реалізації генетичного оператора.

Після того, як були задіяні генетичні оператори, зокрема, арифметичний оператор кросинговера [24], виконано підсумковий розрахунок значень ЦФ - *W*. Модифікація розмірів ЗЗІ по вузлам РОС виконується до тих пір, поки не будуть досягнуті необхідні показники за метриками ІБ для ОБІ. Процес пошуку оптимального рішення можна прискорити, якщо додатково задіяти так званий нечіткий логічний контролер (НЛК).

Запропоновані алгоритми були реалізовані в програмному комплексі для інженерного рішення оптимізаційної задачі, пов'язаної з підбором ЗЗІ по вузлам РОС. Такий підбір дозволяє здійснювати різні підходи до створення КСЗІ. Наприклад, можна збільшити розміри ресурсів (фінансових, організаційних, матеріальних), які спрямовані на захист найбільш критичних вузлів РОС, на яких зберігаються найбільш цінні інформаційні масиви компанії.

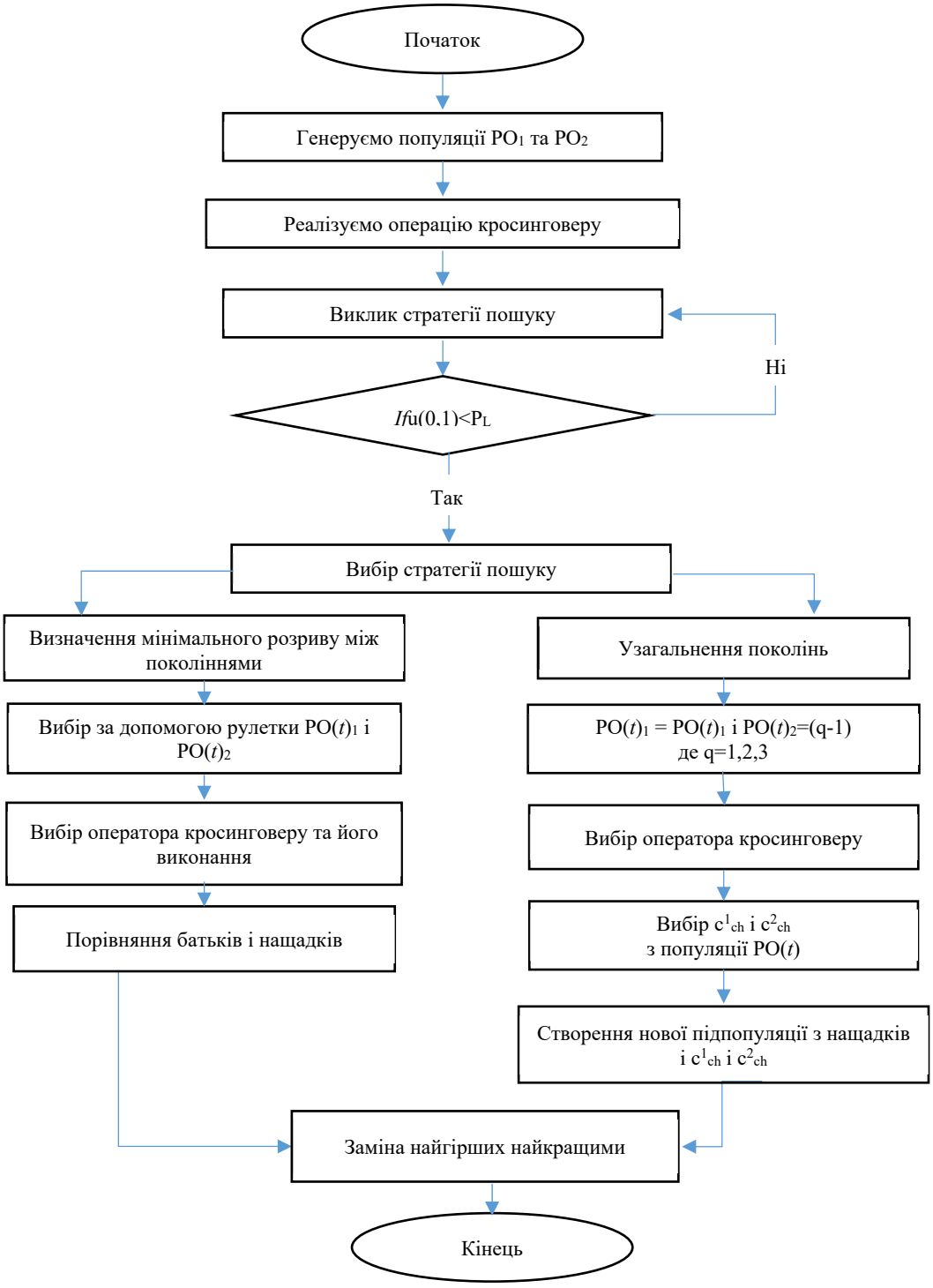

Рис. 1. Концептуальна блок-схема формування нової популяції ЗЗІ

Наведений алгоритм було реалізовано у програмному застосунку. Загальний вигляд інтерфейсу програми, показаний на рисунку 2.

МГА дозволяє дослідити цільову функцію (вираз (1)), яка описує ймовірність успішної протидії ЗЗІ на вузлах РОС реалізації всіх задач атакуючої сторони. Це, у свою чергу, дозволяє виконати швидкий перебір різних варіантів ЗЗІ та їх комбінацію для отримання результатів РОС, виходячи з критерію максимуму ймовірності успішної протидії ЗЗІ реалізації всіх цілей порушниками.

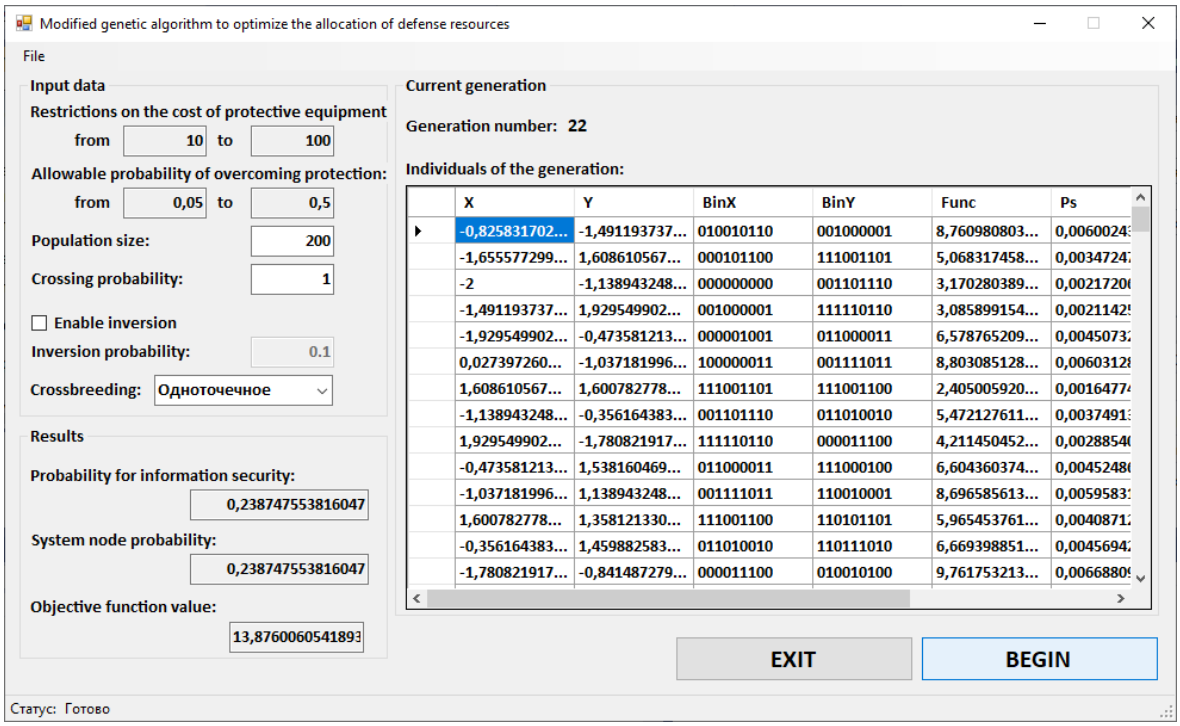

Рис. 2. Загальний вигляд додатків для визначення ймовірності успішної протидії ЗЗІ на вузлах РОС реалізації всіх завдань атакуючої сторони (на основі МГА)

Також було виконано порівняння продуктивності запропонованого МГА з рішенням на основі класичного оптимізаційного методу гілок та меж [25]. Результати показані на гістограмах рисунків 3 і 4.

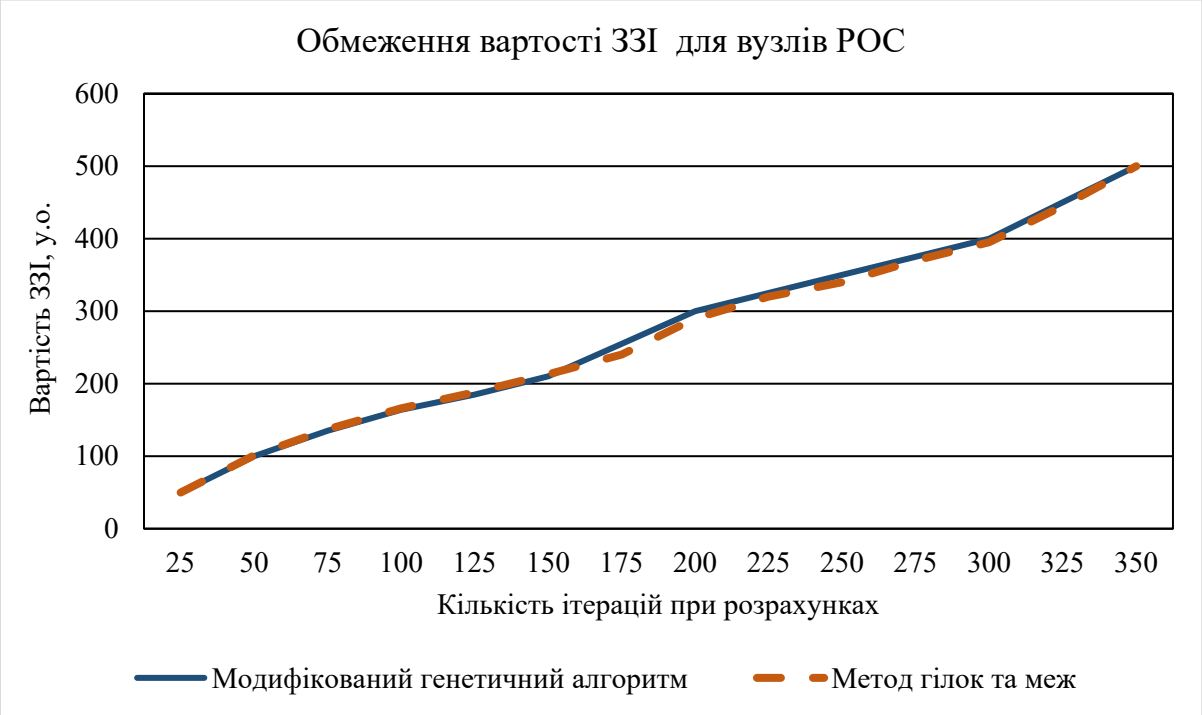

Рис. 3. Результати обчислювальних експериментів для різних варіантів обмежень за вартістю ЗЗІ для вузлів РОС

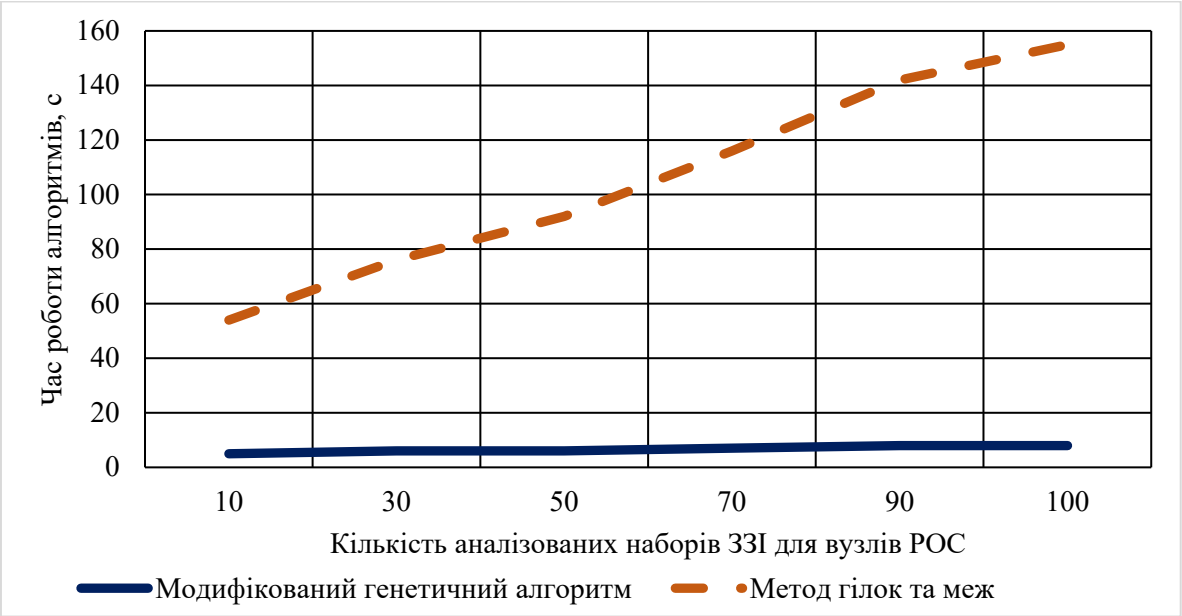

Рис. 4. Результати обчислювальних експериментів відповідно до часу роботи МГА і методу гілок і меж

На рис. 3 показані порівняльні результати вибіркових експериментів для різних варіантів обмежень за даними ЗЗІ для вузлів РОС. Як видно на графіку метод гілок та меж і МГА демонструють приблизно однакову ефективність у ході вирішення розглянутої задачі. Максимальна похибка склала 3,1-3,5 %.

На рисунку 4 показані порівняльні результати обчислювальних експериментів за умови порівняння часу роботи МГА та методу гілок та меж. За графіками, очевидно, що програмна реалізація МГА дозволила прискорити пошук оптимальних варіантів розміщення ЗЗІ за вузлами РОС у 7–15 раз.

До недоліків застосування МГА на теперішньому етапі проведення наших досліджень, може бути віднесений той факт, що були проаналізовані не всі можливі алгоритми вирішення поставлених завдань з метою оптимізації задач. Наприклад, не розглядались варіанти вирішення шляхом залучення інших еволюційних алгоритмів.

Висновки. Таким чином, у статті отримані наведені нижче основні результати.

Запропоновано розв’язувати завдання визначення оптимального складу комплексу ЗЗІ для вузлів розподіленої обчислювальної системи (РОС) з допомогою модифікованого ГА (МГА). Наукова новизна полягає в тому, що в якості цільової функції обраний критерій максимальної ймовірності успішної протидії ЗЗІ реалізації всіх цілей порушником. На відміну від існуючих підходів, запропонований у роботі МГА та відповідна цільова функція, передбачають реалізацію кросинговеру у випадку, коли пари батьків підібрані виходячи з принципу «елітарності» однієї особини та «випадковості» другої. Запис хромосом здійснюється за допомогою кодування дійсними числами, а хромосоми відображаються на основі конкретної стратегії, яка відповідає за результат кросинговеру. Модифікація розмірів ЗЗІ за вузлами РОС виконується доти, поки не будуть досягнуті необхідні показники для метрики ІБ для ОБІ. Процес пошуку оптимального рішення може бути прискорено, якщо в структурі МГА додатково задіяно нечіткий логічний контролер.

Практична цінність дослідження полягає в програмній реалізації запропонованого МГА. Це дозволило автоматизувати процедуру аналізу варіантів розміщення різних ЗЗІ за вузлами РОС. Відповідно, можна проектувати високонадійні системи ІБ (або КСЗІ) для РОС у короткі терміни та за порівняно низьких обчислювальних витрат.

За допомогою розробленого програмного продукту виконані обчислювальні експерименти для перевірки працездатності МГА в процесі визначення ймовірності успішної протидії ЗЗІ на вузлах РОС реалізації всіх задач атакуючої сторони. Показано, що реалізація МГА дозволила прискорити пошук оптимальних варіантів розміщення ЗЗІ по вузлам РОС у 7–15 раз. Зазначена перевага дозволяє виконувати швидкі перебори різних варіантів ЗЗІ та їх комбінацій для вузлів РОС, виходячи з критерію максимуму ймовірності успішної протидії ЗЗІ реалізації всіх цілей порушниками.

Результати, включені до статті, отримані на підставі досліджень, проведених із застосуванням сучасного обладнання. Наукові висновки, сформульовані у статті, обґрунтовані теоретично та підтверджені в процесі обчислювальних експериментів, добре узгоджуються з іншими роботами в цьому напрямку.

Список використаних джерел

1. Годовой отчет компаний Cisco по информационной безопасности [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/dam/global/ru_ru/assets/offers/assets/cisco_2018_acr_ru.pdf.

2. Отчет «Понимание кибер-угроз 2020» [Електронний ресурс]. – Режим доступу: https://www.cloudav.ru/upload/iblock/b58/PandaLabs%20-%20Threat-Insights-2020.pdf.

3. Optimization Model of Adaptive Decision Taking Support System for Distributed Systems Cyber Security Facilities Placement / Kalizhanova, Aliya, et al. // International Journal of Electronics and Telecommunications. – 2020. – Pp. 493-498.

4. Optimization of NIDS placement for protection of intercommunicating critical infrastructures / R. Puzis, M. D. Klippel, Y. Elovici, S. Dolev // European Conference on Intelligence and Security Informatics. – Springer, Berlin, Heidelberg, December 2008. – Pp. 191-203.

5. Белов С. В. Формализация задачи распределения ресурсов между различными функциями обеспечения защиты информации / С. В. Белов, Е. А. Попова, М. В. Кальнов // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. – 2012. – № 1. – С. 112–116.

6. Быков А. Ю. Алгоритмы распределения ресурсов для защиты информации между объектами информационной системы на основе игровой модели и принципа равной защищенности объектов / А. Ю. Быков, Е. С. Шматова // Машиностроение и компьютерные технологии. – 2015. – Вып. 9. – С. 160–187.

7. Oh S. J. Adversarial image perturbation for privacy protection a game theory perspective / S. J. Oh, M. Fritz, B. Schiele // 2017 IEEE International Conference on Computer Vision (ICCV). – IEEE. – October 2017. – Pp. 1491-1500.

8. Zhu Q. Game theory meets network security: A tutorial / Q. Zhu, S. Rass // Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. – January 2018. – Pp. 2163-2165.

9. Dimitrov W. The Impact of the Advanced Technologies over the Cyber Attacks Surface / W. Dimitrov // Computer Science On-line Conference. Springer, Cham. – July 2020. – Pp. 509-518.

10. Ettiane R. Toward securing the control plane of 5G mobile networks against DoS threats: Attack scenarios and promising solutions / R. Ettiane, A. Chaoub, R. Elkouch // Journal of Information Security and Applications. – 2021. – Vol. 61. – Art. 102943.

11. Allocation of Organizational and Financial Resources of the Information Protection Side Using a Genetic Algorithm / V. Lakhno, S. Adilzhanova, O. Kryvoruchko, A. Desiatko, V. Buriachok // Lecture Notes in Networks and Systems. – 2021. – Vol. 228. – Pp. 41-53.

12. Bagane P. Comparison between traditional cryptographic methods and genetic algorithm based method towards Cyber Security / P. Bagane, D. K. Sirbi // International Journal of Advanced Research in Engineering and Technology (IJARET). – 2021. – Vol. 12(2). – Pp. 676-682.

13. Мурзакова Е. А. Проектирование оптимальной системы защиты информации с использованием генетического алгоритма / Е. А. Мурзакова, Т. И. Паюсова, А. А. Мурзакова // Математическое и информационное моделирование: сборник научных трудов. – 2018. – Вып. 16. – С. 331-340.

14. Прокопенко А. С. Разработка генетического алгоритма размещения средств технической защиты информации / А. С. Прокопенко, Н. И. Кушниренко, А. А. Яковенко // Современные информационные и электронные технологии. – 2016. – № 1(17). – С. 129-130.

15. Гулак Г. М. Метод раціонального керування системами кіберзахисту та забезпечення гарантоздатності радіотехнічних систем / Г. М. Гулак, В. А. Лахно, С. А. Адилжанова // Вестник НТУУ «КПИ». Серия Радиотехника. Радиоаппаратостроение. – 2020. – Вип. 83. – С. 62-68.

16. Demertzis K. A bio-inspired hybrid artificial intelligence framework for cyber security / K. Demertzis, L. Iliadis // Computation, cryptography, and network security. – Springer, Cham, 2015. – Pp. 161-193.

17. Hybrid-driven finite-time H∞ sampling synchronization control for coupling memory complex networks with stochastic cyber attacks / K. Shi, S. Zhong, Y. Tang, J Cheng. // Neurocomputing. – 2020. – Vol. 387. – Pp. 241-254.

18. Гладков Л. А. Гибридный генетический алгоритм решения задачи размещения элементов СБИС с учетом трассируемости соединений / Л. А. Гладков // Вестник Ростовского государственного университета путей сообщения. – 2011. – № 3 (43). – С. 58–66.

19. Гладков Л. А. Решение задач проектирования на основе гибридных генетических алгоритмов/ Л. А. Гладков // Вестник БФУ им. И. Канта. – 2012. – Вып. 10. – С. 86-93.

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

21. Information safety of Ukraine: Integral assessment and taxonomic analysis / A. Yakymchuk, N. Popadynets, T. Vasyltsiv, I. Irtyshcheva, R. Bilyk, Y. Khomosh, O. Irtyshchev // International Journal of Data and Network Science. – 2021. – Vol. 5(2). – Pp. 75-82.

22. Adaptive model of cybersecurity financing with fuzzy sets of threats and resources at the protection side / B.S. Akhmetov, V.A. Lakhno, V.P. Malyukov, A.A. Doszhanova, Z.K. Alimseitova // International Journal of Advanced Trends in Computer Science and Engineering. – 2020. – Vol. 9, № (4). – Pp. 5046-5052.

23. Deb K. Real-Coded Evolutionary Algorithms with Parent-Centric Recombination. Kanpur Genetic Algorithms Laboratory (KanGAL), Kanpur, PIN 208 016 / K. Deb, D. Joshi, A. Anand. – India: KanGAL Report. – № 2001003.

24. Wang Z. A Golden Section-based Double Population Genetic Algorithm Applied to Reactive Power Optimization / Z. Wang, Y. Xu // IOP Conference Series: Earth and Environmental Science. – 2021. – Vol. 645, No. 1. – Pp. 012074.

25. A Model of Optimal Complexification of Measures Providing Information Security / P.D. Zegzhda, V.G. Anisimov, A.F. Suprun, E.G. Anisimov, T.N. Saurenko, V.P. Los // Automatic Control and Computer Sciences. – 2020. – Vol. 54(8). – Pp. 930-936.

References

1. Cisco Annual Report on Information Security. https://www.cisco.com/c/dam/global/ru_ru/assets/offers/assets/cisco_2018_acr_ru.pdf.

2. Report "Understanding Cyber Threats 2020". https://www.cloudav.ru/upload/iblock/b58/PandaLabs%20-%20Threat-Insights-2020.pdf.

3. Kalizhanova, A. et al. (2020). Optimization Model of Adaptive Decision Taking Support System for Distributed Systems Cyber Security Facilities Placement. *International Journal of Electronics and Telecommunications*, 493-498.

4. Puzis, R., Klippel, M. D., Elovici, Y., & Dolev, S. (2008, December). Optimization of NIDS placement for protection of intercommunicating critical infrastructures. In *European Conference on Intelligence and Security Informatics* (pp. 191-203). Springer, Berlin, Heidelberg.

5. Belov, S.V., Popova, E.A., Kalnov, M.V. (2012). Formalizaciya zadachi raspredeleniya resursov mezhdu razlichnymi funkciyami obespecheniya zashchity informacii [Formalization of the problem of resource allocation between various functions of ensuring information security]. *Vestnik AGTU. Seriia: Upravlenie, vychislitelnaia tekhnika i informatika – Bulletin of the Astrakhan State Technical University. Series: Management, Computer Engineering and Informatics*, (1), 112–116.

6. Bykov, A.Yu., Shmatova E.S. (2015). Algoritmy raspredeleniia resursov dlia zashchity informatsii mezhdu obektami informatsionnoi sistemy na osnove igrovoi modeli i printsipa ravnoi zashchishchennosti obektov [Algorithms of resource allocation for information protection between objects of the information system based on the game model and the principle of equal security of objects]. *Mashinostroenie i kompiuternye tekhnologii – Mechanical engineering and computer technologies, 9*, 160–187.

7. Oh, S. J., Fritz, M., & Schiele, B. (2017, October). Adversarial image perturbation for privacy protection a game theory perspective. In *2017 IEEE International Conference on Computer Vision (ICCV)* (pp. 1491-1500). IEEE.

8. Zhu, Q., & Rass, S. (2018, January). Game theory meets network security: A tutorial. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security* (pp. 2163-2165).

9. Dimitrov, W. (2020, July). The Impact of the Advanced Technologies over the Cyber Attacks Surface. In *Computer Science On-line Conference* (pp. 509-518). Springer, Cham.

10. Ettiane, R., Chaoub, A., & Elkouch, R. (2021). Toward securing the control plane of 5G mobile networks against DoS threats: Attack scenarios and promising solutions. *Journal of Information Security and Applications, 61*, 102943.

11. Lakhno, V., Adilzhanova, S., Kryvoruchko, O., Desiatko, A., & Buriachok, V. (2021). Allocation of Organizational and Financial Resources of the Information Protection Side Using a Genetic Algorithm. *Lecture Notes in Networks and Systems*, *228*, 41-53.

12. Bagane, P., & Sirbi, D. K. (2021). Comparison between traditional cryptographic methods and genetic algorithm based method towards Cyber Security. *International Journal of Advanced Research in Engineering and Technology (IJARET), 12*(2), 676-682.

13. Murzakova, E.A., Payusova, T.I., & Murzakova, A.A. (2018). Design of an optimal information protection system using a genetic algorithm. *Mathematical and information modeling: a collection of scientific papers, 16*, 331-340.

14. Prokopenko, A.S., Kushnirenko, N.I., & Yakovenko, A.A. (2016). Development of a genetic algorithm for the placement of means of technical protection of information. *Modern Information and Electronic Technologies*, *1*(17), 129-130.

15. Hulak, H.M., Lakhno, V.A., & Adiljanova, S.A. (2020). Metod ratsionalnoho keruvannia systemamy kiberzakhystu ta zabezpechennia harantozdatnosti radiotekhnichnykh system [Method of rational management of cyber defense systems and ensuring the warranty of radio systems]. *Visnyk NTUU «KPI». Radiotekhnika Radioaparatobuduvannia – Bulletin of NTUU «KPI». Radio Engineering Series. Radio equipment construction*, (83), 62-68.

16. Demertzis, K., & Iliadis, L. (2015). A bio-inspired hybrid artificial intelligence framework for cyber security. In Computation, cryptography, and network security (pp. 161-193). Springer, Cham.

17. Shi, K., Zhong, S., Tang, Y., & Cheng, J. (2020). Hybrid-driven finite-time H∞ sampling synchronization control for coupling memory complex networks with stochastic cyber attacks. *Neurocomputing*, *387*, 241-254.

18. Gladkov, L.A. (2011). Gibridnyj geneticheskij algoritm resheniya zadachi razmeshcheniya elementov SBIS s uchetom trassiruemosti soedineniш [Hybrid genetic algorithm for solving the problem of placing VLSI elements taking into account the traceability of connections]. *Vestnik Rostovskogo gosudarstvennogo universiteta putei soobshcheniia – Bulletin of the Rostov State University of Communications,* (3), 58–66.

19. Gladkov, L.A. (2012). Reshenie zadach proektirovaniiana osnove gibridnykh geneticheskikh algoritmov [Solving design problems based on hybrid genetic algorithms]. *Vestnik Baltiiskogo federalnogo universiteta im. I. Kanta. Seriia: Fiziko-matematicheskie i tekhnicheskie nauki – Bulletin of the IKBFU. I. Kant*, (10). 86-93.

20. Lakhno, V., Akhmetov, B., Adilzhanova, S., Blozva, A., Svitlana, R., & Dmytro, R. (2020). The use of a genetic algorithm in the problem of distribution of information security organizational and financial resources. *ATIT 2020 - Proceedings: 2020 2nd IEEE International Conference on Advanced Trends in Information Theory*, 9349310, 251-254.

21. Yakymchuk, A., Popadynets, N., Vasyltsiv, T., Irtyshcheva, I., Bilyk, R., Khomosh, Y., & Irtyshchev, O. (2021). Information safety of Ukraine: Integral assessment and taxonomic analysis. *International Journal of Data and Network Science, 5*(2), 75-82.

22. Akhmetov, B.S., Lakhno, V.A., Malyukov, V.P., Doszhanova, A.A., & Alimseitova, Z.K. (2020). Adaptive model of cybersecurity financing with fuzzy sets of threats and resources at the protection side. *International Journal of Advanced Trends in Computer Science and Engineering, 9*(4), 5046-5052.

23. Deb, K., Joshi, D., Anand, A. (n.d.). Real-Coded Evolutionary Algorithms with Parent-Centric Recombination. Kanpur Genetic Algorithms Laboratory (KanGAL), Kanpur, PIN 208 016. KanGAL Report. № 2001003.

24. Wang, Z., & Xu, Y. (2021). A Golden Section-based Double Population Genetic Algorithm Applied to Reactive Power Optimization. In *IOP Conference Series: Earth and Environmental Science* (Vol. 645, No. 1, p. 012074). IOP Publishing.

25. Zegzhda, P. D., Anisimov, V. G., Suprun, A. F., Anisimov, E. G., Saurenko, T. N., & Los, V. P. (2020). A Model of Optimal Complexification of Measures Providing Information Security. *Automatic Control and Computer Sciences, 54*(8), 930-936.

Отримано 06.08.2021

UDC 004.056.57-048.34

Valerii Lakhno[1], Dmytro Kasatkin[2], Andrii Blozva[3], Borys Husiev[4], Tetiana Osypova[5], Yuriy Matus[6]

[1]Doctor of Technical Sciences, Professor, Head of Department of Computer Systems, Networks and Cybersecurity
National University of Life and Environmental Sciences of Ukraine (Kyiv, Ukraine)
E-mail: valss21@ukr.net. **ORCID:** http://orcid.org/0000-0001-9695-4543

[2]PhD in Pedagogical Sciences, Associate Professor,
Associate Professor of the Department of Computer Systems, Networks and Cybersecurity
National University of Life and Environmental Sciences of Ukraine (Kyiv, Ukraine)
E-mail: d.kasatkin@nubip.edu.ua. **ORCID:** http://orcid.org/0000-0002-2642-8908

[3]PhD in Pedagogical Sciences, Associate Professor of the Department of Computer Systems, Networks and Cybersecurity
National University of Life and Environmental Sciences of Ukraine (Kyiv, Ukraine)
E-mail: andriy.blozva@nubip.edu.ua. **ORCID:** http://orcid.org/0000-0002-4377-0916

[4]PhD of Technical Sciences, Associate Professor,
Associate Professor of the Department of Computer Systems, Networks and Cybersecurity
National University of Life and Environmental Sciences of Ukraine (Kyiv, Ukraine)
E-mail: gusevbs@nubip.edu.ua. **ORCID:** http://orcid.org/0000-0003-1658-7822

[5]PhD in Pedagogical Sciences, Associate Professor of the Department of Computer Systems, Networks and Cybersecurity
National University of Life and Environmental Sciences of Ukraine (Kyiv, Ukraine)
E-mail: t_osipova@nubip.edu.ua. **ORCID:** http://orcid.org/0000-0002-9199-3436

[6]Senior Lecturer of the Department of Computer Systems, Networks and Cybersecurity
National University of Life and Environmental Sciences of Ukraine (Kyiv, Ukraine)
E-mail: umatus@nubip.edu.ua. **ORCID:** http://orcid.org/0000-0003-0974-4789

OPTIMIZATION OF THE CHOICE OF INFORMATION PROTECTION USING GENETIC ALGORITHM

There is still a question of determining the optimal composition of the Information System Security (ISS) complex for nodes of the distributed computer system (DCS). It is also important to automate the selection of hardware and technical means for various information security circuits. This leads to the problem of finding efficient algorithms for determining the optimal composition of ISS complexes, in particular, by improving the genetic algorithm, for which the criterion of the maximum of success in counteracting ISS is chosen as a target function for the probability to achieve all objectives.

In contrast to the existing approaches, the proposed MGA and corresponding target function imply the realization of the crossover in cases when parents' pairs are selected on the basis of the principle of «elitism» of one individual and «randomness» of the other. Chromosomes were recorded by encoding the actual numbers. Chromosomes were selected on the basis of a strategy responsible for the crossover's result. The modification of the ISS's sizes by DCS's nodes is carried out until the necessary metric of IS (information security) for the informatization object will be reached. The practical value of the research lies in the programmatic implementation of the proposed MAG. This made it possible to automate the procedure of analysis of options of different ISS behind the DCS's node. Accordingly, it is possible to design high-reliability system of IS (or Integrated information security system) for DCS in a short time and in comparatively low computing costs.

With the aid of the developed software, computational experiments are carried out to test the performance of the MGA in the process of determining the probability of successful counteraction of the ISS on the DCS's nodes realization of all tasks of the attacking side. It has been shown that the implementation of MGA has made it possible to speed up the search for optimum variants of ISS placement on DCS's nodes by 7-15 times.

Keywords: *optimization; modified genetic algorithm; information security; informatization object; distributed computing system.*
Fig.: 4. Referenses: 25.

Оптимізація вибору засобів захисту інформації за допомогою генетичного алгоритму / Лахно В. А., Касаткін Д., Блозва А. І., Гусєв Б. С., Осипова Т. Ю., Матус Ю. В. *Технічні науки та технології.* 2021. № 3(25). С. 138-149.