Visnyk NTUU KPI Seriia – Radiotekhnika Radioaparatobuduvannia, 2020, Iss. 83, pp. 62–68

УДК 004.056,621.3.019.3

Метод раціонального керування системами кіберзахисту та забезпечення гарантоздатності радіотехнічних систем

Гулак Г. М.[1], *Лахно В. А.*[2], *Адилжанова С. А.*[3]

[1]Інститут проблем математичних машин і систем Національної академії наук України, Київ, Україна
[2]Національний університет біоресурсів і природокористування України, Київ, Україна
[3]Казахський національний Університет імені Аль-Фарабі, Алмати, Республіка Казахстан

E-mail: *h.hulak@ukr.net*

Досліджується актуальне завдання створення методу раціонального вибору засобів і підсистем кіберзахисту або забезпечення гарантоздатності радіотехнічних (також, інформаційних) систем, оптимізації управління відповідними засобами в умовах реалізації загроз антропогенного або техногенного характеру. В статті 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 гарантоздатних радіотехнічних систем (ГРС), а також інформаційних систем (ІС). Наукова новизна дослідження полягає у застосуванні в генетичному алгоритмі в якості критеріїв оптимізації конфігурації (складу) ЗЗІ сумарної величини ризиків від порушення конфіденційності, цілісності та доступності інформаційного ресурсу, а також вартісні характеристики відповідних ЗЗІ. Генетичний алгоритм в задачі оптимізації вибору конфігурації ЗЗІ для ГРС (ІС) і динамічного управління ресурсами підсистеми кібербезпеки розглядається як варіант розв'язання задачі мультивибору. В такій постановці завдання раціонального розміщення ЗЗІ на різних рівнях захисту ГРС (ІС) розглядається як варіант розв'язання NP-повної комбінаторної задачі оптимізації про укладку рюкзака (*Knapsack problems*). Запропонований підхід забезпечує можливість, з одного боку, виконати швидке опробування різних наборів ЗЗІ та варіантів їх застосування в ГРС (ІС), а з іншого боку, це утворює передумови для об'єднання запропонованого алгоритму з вже існуючими методами, моделями і алгоритмами для оптимізації кількості рівнів кіберзахисту ГРС (ІС) і динамічного управління ресурсами кібербезпеки для різних об'єктів інформаційної діяльності. Таке поєднання методів, моделей та алгоритмів створює передумови для швидкої зміни налаштування підсистеми захисту ГРС (ІС), змінюючи її конфігурацію з урахуванням можливості появи нових загроз інформації і кібератак.

Ключові слова: апаратно-програмні засоби захисту інформації; багатокритеріальна оптимізація; генетичний алгоритм; система підтримки прийняття рішень; задача про укладку рюкзака

DOI: 10.20535/RADAP.2020.83.62-68

Вступ

Зростання кількості та складності реалізованих кібератак на різні комп'ютеризовані радіотехнічні системи [1–4] потребує від їх володільців та менеджменту безпеки впровадження нових процедур та механізмів безпеки, що адекватні до визначених загроз, уточнення складових комплексів захисту інформації і кібербезпеки (КБ) на всіх рівнях захисту гарантоздатних радіотехнічних систем (ГРС) [5].

Зауважимо, що перманентне завдання з формування ефективних рубежів кибербезпеки ГРС (ІС) стало джерелом для багатьох досліджень, що присвячені питанням раціонального вибору складу засобів захисту інформації і КБ. Ці дослідження, перш за все, намагаються відповісти на питання, які пов'язані з рішенням багатокритеріальних оптимізаційних задач, що характеризуються такими властивостями як: вельми складна конфігурація припустимої галузі застосування окремих засобів захисту інформації (ЗЗІ); багатоекстремальність функцій, що розглядаються; алгоритмічне завдання функцій тощо.

Більш того, в реальних задачах побудови ефективних багаторівневих систем кібербезпеки [6, 7] варіанти рішень зазвичай оцінюють з допомогою декількох критеріїв. Тому, в подібних ситуаціях, дуже важливо не тільки знаходити допустимі паретооптимальні рішення, але і апроксимувати множину отриманих варіантів для того, щоб запропонувати

особі, яка приймає рішення, науково обґрунтований вибір ЗЗІ для відповідних ланок кібербезпеки та захисту інформації в ГРС (ІС). Рішення вищеописаних завдань побудови багаторівневих систем захисту інформації в умовах зростання кількості спроб деструктивних впливів на ГРС (ІС) та скорочення часу на прийняття рішень вимагає застосування не тільки класичних процедур оптимізації, але і більш універсальних методів, наприклад, генетичних алгоритмів (ГА), які довели свою ефективність при вирішенні багатьох складних завдань [8, 9].

Ефективність застосування ГА визначається їх ретельним налаштуванням і правильним вибором їх параметрів. Це дещо ускладнює їх застосування у випадках звичайних інженерних розрахунків ефективності застосування ЗЗІ по ланкам захисту в ГРС (ІС). У той же час використання ГА набуває сенсу, якщо окрім звичайної багатокритеріальної оптимізаційної задачі щодо вибору складу ЗЗІ для системи захисту ГРС (ІС), також враховують розмір ризиків для конкретних інформаційних активів (бази даних, бібліотеки програмних проектів тощо) та вартісні показники припустимих ЗЗІ. При цьому відомо, що процедура пошуку (вибору) рішення може бути значно більш ефективною, якщо застосувати потенціал інтелектуальних систем підтримки прийняття рішень (СППР), програмні продукти якого застосовують ГА.

Вищенаведені міркування і визначили актуальність досліджень, спрямованих на вдосконалення еволюційних алгоритмів і моделей для обчислювального ядра СППР в процесі багатокритеріальної оптимізації складу ЗЗІ по ланках КБ ГРС (ІС).

1 Огляд і аналіз попередніх досліджень

Генетичні алгоритми, що застосовуються при розв'язанні багатокритеріальних оптимізаційних задач, є варіантами еволюційних методів пошуку [10]. Дослідженням в цій області за останні кілька років присвячено досить велику кількість робіт. Так, наприклад, в [11] описана 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 роботі не вказано яким чином і де конкретно були використані запропоновані рішення на практиці.

У роботах [12, 13] були досліджені ГА, які можна віднести до двох груп. У першій групі досліджувалися ГА з бінарним кодуванням [13, 14], а у другій – ГА з дійсним кодуванням [15, 16]. У роботах [15–19] показано, що в першій групі можна домогтися більш високої ефективності пошуку екстремального значення на множині допустимих рішень.

У роботах [20–25] розглядалися особливості застосування модифікованого ГА в подібних багатокритеріальних оптимізаційних задачах. Відмінність ГА з відносною фітнес-функцією від стандартного ГА полягає в тому, що тут під час роботи алгоритму у якості фітнес-функції застосовувалася не сума ефективностей ЗЗІ, які власне і складали хромосому, а використовувалася сума відносин ефективностей до обмежуючих характеристик ЗЗІ, або так званий – коефіцієнт ефективності. Подібна модифікація ГА по суті являє собою диз'юнкцію стандартного ГА і жадібного алгоритму (*greedy algorithm*).

У роботах [20, 23] показано, що стандартні і модифіковані ГА досить ефективні для вирішення більшості складних оптимізаційних задач [26] і є перспективними для подальшого вивчення і вдосконалення.

Все вищезазначене і зумовило релевантність дослідження, спрямованого на розвиток ГА для обчислювального ядра СППР в завданнях оптимізації вибору ЗЗІ і КБ для ГРС (ІС) різних об'єктів інформатизації.

2 Мета і завдання роботи

Метою дослідження є розвиток генетичного алгоритму для обчислювального ядра системи підтримки прийняття рішень в процесі підбору, оптимізації та динамічного управління ресурсами кібербезпеки. Для цього слід врахувати ризики втрат у випадках реалізації загроз, а також вартісні характеристики різних типів ЗЗІ.

3 Основний матеріал статті

Інфраструктура ГРС (ІС) з точки зору забезпечення КБ і захисту інформації (ЗІ) є вельми складним об'єктом.

Для досягнення поставленої мети забезпечення кібербезпеки та захисту інформації на основі вимог та рекомендацій нормативних документів на вузлах ГРС (ІС) може бути встановлений типовий набір ЗЗІ [26], що має містити: антивірусні засоби; мережеві екрани; засоби криптографічного захисту інформації (включаючи шифрування даних та формування/перевірку цифрового підпису); обладнання розмежування доступу, автентифікації і ідентифікації; системи виявлення та попередження вторгнень; засоби забезпечення доступності даних та контролю їх цілісності; системи захисту серверів, тощо.

Залежно від конкретних умов експлуатації певної ГРС (ІС), інформації, що обробляється за її допомогою, моделі загроз та характеристик вірогідних порушників системи кібербезпеки наведений перелік ЗЗІ може бути доповнений або скорочений,

а конкретний тип ЗЗІ (програмний або апаратний) може бути змінений з урахуванням міркувань безпеки та швидкодії.

Розглянемо можливість застосування ГА для вирішення завдання мультивибору в процесі підбору оптимальної конфігурації (далі – набір) ЗЗІ (наприклад антивіруси, мережеві екрани, засоби виявлення вторгнень, тощо) в ГРС (ІС).

Далі формалізуємо задачу за допомогою понять генетичних алгоритмів.

Вважаємо, що хромосома – це набір засобів та заходів захисту інформації (наприклад, правила щодо дотримання політики інформаційної безпеки на об'єкті захисту). Кожний набір закодуємо двійковим числом [11, 12]. При цьому, якщо деякий двійковий розряд числа дорівнює одиниці (**1**), то відповідний ЗЗІ або захід із захисту інформації з відповідним номером включений в набір. Тоді діапазон змін коду може бути поданий як:

$$G = (d_0 d_1 \dots d_{NC})_2 = \left(2^{NC}\right)_{10}, \qquad (1)$$

де NC – кількість існуючих ЗЗІ та захисних заходів, які потенційно розглядаються для включення в оптимальний набір; d_i – розряд включення засобів або заходу захисту в склад ЗЗІ.

У термінах ГА популяція буде складатися із зразків з різними хромосомами. Розмір популяції обмежений максимальною кількістю зразків в ній. Кожен екземпляр популяції можна описати як:

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

де G – генетичний код примірника в 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 – ЗЗІ).

У процесі модифікації алгоритму для визначення ризику використовується наступне припущення. Абсолютна величина втрат в грошовому еквіваленті для конкретної ГРС (ІС) залежить від логічного ланцюга: загрози → вразливості → ЗЗІ → наслідки [2, 6]. Отже, кількість ризиків – це число комбінацій загроз і активів:

$$r = TH \cdot M, \qquad (3)$$

де TH – кількість загроз, M – кількість активів.

У формулі (3) не враховано поєднання декількох загроз, а також внутрішні зв'язки між ЗЗІ. Тому більш підходящим способом щоб визначити ризики для ГРС (ІС) є метод, який заснований на складанні профілів атак [6, 7]. При такому методі профілі атак розглядаються як послідовності атак, які складаються з поєднання різних загроз [1, 7]. Тоді кількість ризиків можна описати наступною залежністю:

$$r = \left(2^{TH}\right)^{TA}, \qquad (4)$$

де TA – кількість атак.

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

Якщо відсутня ланцюжкова реакція в ході атаки, то величину сумарного ризику можна уявити як математичне очікування збитку для кожного активу ГРС (ІС):

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

де $P_{i,j}$ – ймовірність виникнення інциденту інформаційної безпеки ГРС (ІС), обумовленого загрозою (i) для активу (j); $D_{i,j}$ – розмір збитку (в грошовому еквіваленті), що обумовлений інцидентом.

Хромосому (Ch) слід представити у вигляді матриці. Тоді, рядки матриці будуть являти собою точки розміщення, відповідно, стовпці – класи засобів, які включають в себе конкретні ЗЗІ (наприклад, в клас засобів антивірусне ПЗ можна віднести відомі продукти антивірусного захисту: Avast, Avira, AVG, Bitdefender тощо). Елемент матриці g_{ij} показує номер засобу захисту інформації з класу j, що розміщується на вузлу i. Якщо $g_{ij} = 0$, то вважаємо, що з класу j на вузлі i не використовується жоден засіб. Схема формування хромосоми (Ch) ГА представлена в таблиці 1.

Табл. 1 Схема формування хромосоми

Вузли мережі	Засоби/заходи захисту			
	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}	…	$g_{KC,NC}$

В такому форматі уявлення хромосоми і в контексті розв'язуваної задачі вважаємо, що K_{KC}, N_{NC} – відповідно, кількість вузлів ГРС (ІС) і ЗЗІ на вузлі.

Щоб розрахувати ризик (R) скористаємося такою моделлю.

Підберемо за генетичним кодом для кожного носія відповідні ЗЗІ.

Введемо в ГА функцію корисності – U. Ця функція необхідна для оцінювання ефективності відбору ЗЗІ в деякий набір. Зауважимо, що ЗЗІ, які відбираються, повинні відповідати профілю атаки. Адже абсолютно зрозуміло, що марним є використання безкоштовного антивірусного програмного забезпечення з обмеженим функціоналом для боротьби з DoD/DDoS атаками, а інструкції щодо дотримання політики безпеки для ГРС (ІС) самі по собі не захистять від інсайдера.

Тоді функцію корисності (U) можна подати так:

$$U\,(Ch) = R_0 - Ch.R, \qquad (6)$$

де Ch – один з варіантів складу ЗЗІ; R_0 – величина ризиків, пов'язаних з втратою інформації, якщо не

застосовувати відповідний набір ЗЗІ; $Ch.R$– величина ризиків з урахуванням застосування відповідного варіанту складу ЗЗІ $Ch.G$.

Однак, досягнута результативність щодо захисту ГРС (ІС) від атак, відповідно, вимагає додаткових витрат на ЗЗІ. Врахуємо вплив витрат на ЗЗІ, застосовуючи наступний вираз:

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

де $Ch.C$ – вартість складу ЗЗІ.

Вираз (7) свідчить про те, як можна знизити (або збільшити) ризик втрати інформації на кожну вкладену одиницю вартості.

Далі розглянемо, як отримані вирази можна застосувати в ГА. Генетичний алгоритм базується на генетичних операторах кросинговеру (схрещування), мутації і селекції, які можуть бути виражені у синтаксисі високорівневих мов програмування.

В процесі програмної реалізації СППР на базі ГА було розглянуто два види кросинговеру. Аналізувалися можливості застосування одноточкового і n–точкового кросинговеру. Вибір цих двох видів обумовлений такими міркуваннями. Стандартний підхід, заснований на одноточковому кросинговері підходить до більшості завдань, в яких доцільно здійснювати пошук рішення за допомогою ГА. Водночас зауважимо, що для завдання мультивибору ЗЗІ для вузлів ГРС (ІС) стандартний ГА виявиться вельми неточним. Це обумовлено тим, що хромосома не буде являти собою єдину неподільну структуру. У постановці даного завдання хромосому можна інтерпретувати як систему, що потребує процедури декомпозиції. Декомпозиція дозволить розбити хромосому на ділянки. При цьому кожній ділянці буде відповідати свій клас вузлів ГРС (ІС).

Створимо для кожної пари хромосом 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 обумовлено наступними припущеннями: 1) постійна мутація використовується в більшості програмних реалізацій ГА; 2) змінні нашої задачі вимагають більшої гнучкості і для нашої задачі залежність успішної роботи ГА від мутації більша ніж від кросинговеру; 3) припущення 2 пов'язано з тим, що існують об'єктивні особливості вирішення завдань, пов'язаних з формуванням ланок кібербезпеки ГРС (ІС). Це зумовлює великі розміри хромосом, а також наявність обмежень.

Отже, змінна мутація, для якої характерні елементи випадковості на ранніх стадіях роботи алгоритму, буде більш кращою з точки зору пошуку оптимального варіанту укладання рюкзака [8].

В 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. У цьому випадку ймовірність мутації буде залежати від поточних потреб ГА. Коефіцієнт мутації буде вар'ірюватися в межах 1-6%.

В даному ГА з відносною фітнес-функцією в якості фітнес-функції використовувалася не сума ефективностей ЗЗІ, які, власне і становили хромосому, а застосовувалася сума відносин ефективностей або інтегральних показників ЗЗІ, які входять в клас відповідних ЗЗІ.

Для цього випадковим чином будемо інвертувати два двійкових розряди в 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:

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

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

Перед застосуванням селекції попередньо обчислюємо $Ch(X)\,.C$ і для популяції хромосом. Відповідно до [9, 10] прийнято, що початкова популяція як мінімум включає два примірника. Тоді кожна епоха в ГА [10, 11] буде складатися з послідовного застосування основних функцій, розглянутих вище. Відповідно маємо:

$$func\ E() := ((PA = K(PA), M(PA)), (P = S(PA)))\,. \tag{10}$$

Розглянуті в статті уточнення до ГА лягли в основу обчислювального ядра СППР у процесі багатокритеріальної оптимізації розміщення ЗЗІ в вузлах ГРС (ІС) [26]. На першому етапі роботи СППР за допомогою методу аналізу ієрархій (метод Т. Сааті), або іншого експертного методу, формується набір складу ЗЗІ для ГРС (ІС).

Оскільки як правило даний набір має надлишкову функціональність, а його вартість буде досить високою для звичайної ГРС (ІС) підприємства, що не відноситься до критично важливої інфраструктури, застосовуємо ГА для вирішення завдання з мультивибору, тобто вирішуємо задачу про рюкзак. Оскільки ГРС (ІС) складається з досить великої кількості вузлів, що потребують захисту, то фактично мова йде про рішення задачі мультивибору, де відразу для декількох рюкзаків (вузлів ГРС (ІС))

необхідно відібрати перелік предметів (ЗЗІ), які складаються в кожен рюкзак. При цьому головні критерії відбору предметів – це інтегральний показник (ІНП) і вартість ЗЗІ.

У якості ІНП ЗЗІ прийнятий так званий індекс якості або ступінь досяжності бажаних цілей для конкретного ЗЗІ [1]. Також ІНП можна трактувати як узагальнений показник якості найбільш важливих характеристик конкретного ЗЗІ. При цьому вважаємо, що ІНП обчислений як ступінь близькості параметрів ЗЗІ до ідеальних характеристик в просторі виділених часткових показників [1].

Для перевірки адекватності алгоритму і СППР з багатокритеріальної оптимізації розміщення ЗЗІ по вузлах ГРС (ІС) були проведені відповідні обчислювальні експерименти, результати яких наведені на рис. 1 і рис. 2.

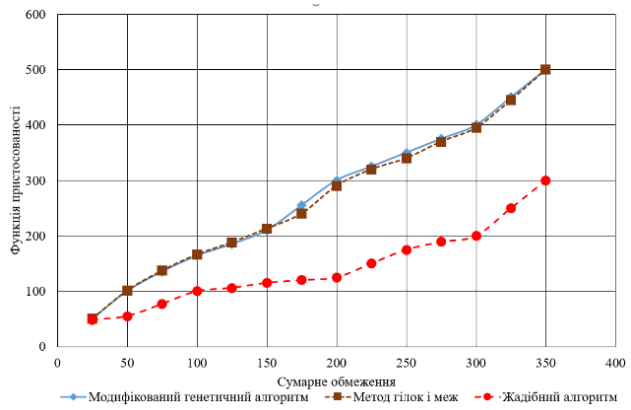

Рис. 1. Результати обчислювальних експериментів з порівняння ефективності алгоритмів, що використовуються в СППР

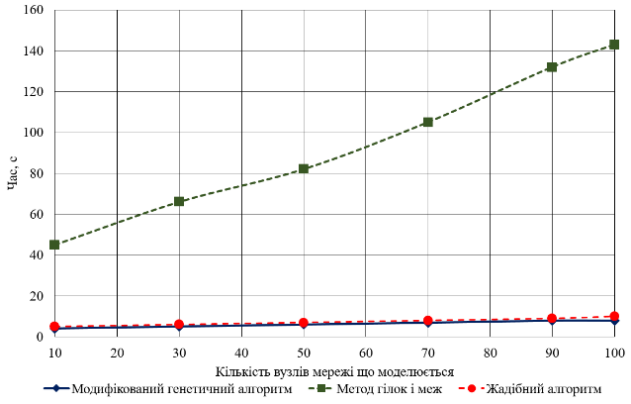

Рис. 2. Результати обчислювальних експериментів з порівняння часу роботи алгоритмів

Обчислювальні експерименти проводились для випадково згенерованого складу ЗЗІ. Порівнювалася ефективність роботи модифікованого ГА, методів гілок і меж та жадібного алгоритму.

В ході обчислювальних експериментів встановлено, що ГА відрізняється досить високою ефективністю, а також швидкодією, у порівнянні з методами гілок і меж та жадібного алгоритму. Встановлено, що час, витрачений на вирішення завдання при використанні ГА, приблизно в 16-25 разів менше в порівнянні з показниками методу гілок і меж. Жадібний алгоритм суттєво поступається як ГА так і методу гілок і меж с точки зору придатності до розв'язання багатокритеріальної оптимізаційної задачі з урахуванням обмежень і кількості змінних.

Висновки

В статті розглянута можливість модифікації генетичного алгоритму для вирішення завдання, пов'язаного з підбором і оптимізацією варіантів конфігурацій засобів захисту інформації і динамічним управлінням ресурсами кібербезпеки для радіотехнічних та інформаційних систем. 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 вартісні показники для кожного класу ЗЗІ. Генетичний алгоритм в задачі оптимізації вибору складу ЗЗІ для ГРС (ІС) розглянуто як варіація задачі, пов'язаної з мультивибором. У такій постановці оптимізація розміщення ЗЗІ по ланках захисту ГРС (ІС) розглянута як модифікація комбінаторної задачі про укладання рюкзака. Практична цінність дослідження полягає в реалізації системи підтримки прийняття рішення на основі запропонованої модифікації ГА.

References

[1] Okutan A., Yang S. J., McConky K., Werner G. (2019) CAPTURE: Cyberattack Forecasting Using Non-Stationary Features with Time Lags. *IEEE Conference on Communications and Network Security (CNS)*, pp. 205-213. DOI: 10.1109/CNS.2019.8802639.

[2] Barreto C., Koutsoukos X. (2019) Design of Load Forecast Systems Resilient Against Cyber-Attacks. In: *Alpcan T., Vorobeychik Y., Baras J., Dán G. (eds) Decision and Game Theory for Security*. GameSec 2019. Lecture Notes in Computer Science, vol 11836. Springer, Cham. DOI: 10.1007/978-3-030-32430-8_1.

[3] Zinov'ev N.V., Kot M.A. (2017) Obzor metodov radioelektronnoi bor'by [Review of electronic warfare methods]. *Issledovaniya i razrabotki v perspektivnykh nauchnykh oblastyakh, Sbornik materialov II Mezhdunarodnoi nauchno-prakticheskoi konferentsii*. Novosibirsk, OOO "Tsentr razvitiya nauchnogo sotrudnichestva", pp. 59-62 [In Russian]

[4] Zatuchnyy D. A. (2018) Methods of preventing unauthorized electronic attacks on navigation system of the aircraft of civil aviation. *RELIABILITY & QUALITY OF COMPLEX SYSTEMS*, Vol. 1 (21), pp. 21-27. DOI:10.21685/2307-4205-2018-1-3.

[5] Bondaruk A. V., Hlukhov V. S., Yevtushenko K. S., Oliiarnyk B. O. (2008) Harantozdatna intehrovana systema navihatsii rukhomykh nazemnykh obiektiv [Guaranteed integrated navigation system for moving ground objects].

Kompiuterni systemy ta merezhi [Computer systems and networks], Vol. 630, pp. 24-30.

[6] Chandra Y., Mishra P. K. (2019) Design of Cyber Warfare Testbed. *In: Hoda M., Chauhan N., Quadri S., Srivastava P. (eds) Software Engineering. Advances in Intelligent Systems and Computing*, Vol 731, pp. 249-256. Springer, Singapore. DOI:10.1007/978-981-10-8848-3_24.

[7] 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*, Vol. 25, pp. 152-168. DOI:10.1016/j.ijcip.2019.04.002.

[8] 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 (IJCNIS)*, Vol. 11, Iss. 1, pp. 61-84.

[9] Nozaki Y., Yoshikawa M. (2019) Security Evaluation of Ring Oscillator PUF Against Genetic Algorithm Based Modeling Attack. *In: Barolli L., Xhafa F., Hussain O. (eds) Innovative Mobile and Internet Services in Ubiquitous Computing. IMIS 2019. Advances in Intelligent Systems and Computing*, vol 994, pp. 338-347. Springer, Cham. DOI:10.1007/978-3-030-22263-5_33.

[10] Dwivedi S., Vardhan M., Tripathi S. (2020) Incorporating evolutionary computation for securing wireless network against cyberthreats. *The Journal of Supercomputing*, Vol. 76, pp. 8691–8728. DOI:10.1007/s11227-020-03161-w.

[11] 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*, Vol. 15, No. 7, pp. 4362-4369. DOI: 10.1109/TII.2019.2891261.

[12] 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*, Vol. 138, pp. 90-97. DOI: 10.1016/j.comcom.2019.03.008.

[13] Shang Q., Chen L., Wang D., Tong R., Peng P. (2020) Evolvable Hardware Design of Digital Circuits Based on Adaptive Genetic Algorithm. *In: Abawajy J., Choo KK., Islam R., Xu Z., Atiquzzaman M. (eds) International Conference on Applications and Techniques in Cyber Intelligence ATCI 2019. ATCI 2019. Advances in Intelligent Systems and Computing*, vol 1017, pp 791-800. Springer, Cham. DOI:10.1007/978-3-030-25128-4_97.

[14] Yang Y. (2019) Yang Y. (2020) Research on Hybrid Quantum Genetic Algorithm Based on Cross-Docking Delivery Vehicle Scheduling. *In: Xu Z., Choo KK., Dehghantanha A., Parizi R., Hammoudeh M. (eds) Cyber Security Intelligence and Analytics. CSIA 2019. Advances in Intelligent Systems and Computing*, Vol. 928, pp. 893-900. Springer, Cham. DOI:10.1007/978-3-030-15235-2_119

[15] Saenko I., Kotenko I. (2019) A role-base approach and a genetic algorithm for VLAN design in large critical infrastructures. *Proceedings of the Genetic and Evolutionary Computation Conference Companion*, pp. 1643-1650. DOI:10.1145/3319619.3326853.

[16] Aleksieva Y., Valchanov H., Aleksieva V. (2019) An approach for host based botnet detection system. *16th Conference on Electrical Machines, Drives and Power Systems (ELMA)*, pp. 1-4. DOI: 10.1109/ELMA.2019.8771644.

[17] 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*, Vol. 7, pp. 41525-41550. DOI:10.1109/ACCESS.2019.2895334.

[18] Malarvizhi N., Selvarani P., Raj P. (2020) Adaptive fuzzy genetic algorithm for multi biometric authentication. *Multimedia Tools and Applications*, Vol. 79, pp. 9131–9144. DOI:10.1007/s11042-019-7436-4.

[19] Alhijawi B., Kilani Y., Alsarhan A. (2020) Improving recommendation quality and performance of genetic-based recommender system. *International Journal of Advanced Intelligence Paradigms*, Vol. 15, Iss. 1, pp. 77-88. DOI:10.1504/IJAIP.2020.104108.

[20] 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*, Vol. 10, pp. 1325-1338. DOI: 10.1007/s12652-018-0906-0.

[21] Llansó T., McNeil M., Noteboom C. (2019) Multi-Criteria Selection of Capability-Based Cybersecurity Solutions. *Hawaii International Conference on System Sciences*, pp. 7322-7330. DOI: 10.24251/HICSS.2019.879.

[22] 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. *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. DOI: 10.1109/HPCC/SmartCity/DSS.2019.00251.

[23] 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*, Vol. 81, pp. 1-10. DOI:10.1016/j.asoc.2019.105487 105487.

[24] 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: *Liu F., Xu S., Yung M. (eds) Science of Cyber Security*. SciSec 2018. Lecture Notes in Computer Science, vol 11287. Springer, Cham. DOI:10.1007/978-3-030-03026-1_5.

[25] Lee Y., Choi T. J., Ahn C. W. (2019) Multi-objective evolutionary approach to select security solutions. *CAAI Transactions on Intelligence Technology*, Vol. 2, Iss. 2, pp. 64-67. DOI:10.1049/trit.2017.0002.

[26] Akhmetov B., Lakhno V., Akhmetov B., Alimseitova Z. (2018) Development of Sectoral Intellectualized Expert Systems and Decision Making Support Systems in Cybersecurity. *In book: Intelligent Systems in Cybernetics and Automation Control Theory*, pp.162-171, Springer, Cham. DOI:10.1007/978-3-030-00184-1_15.

Метод рационального управления системами киберзащиты и обеспечения гарантоспособности радиотехнических систем

Гулак Г. Н., Лахно В. А., Адилжанова С. А.

Исследуется актуальная задача создания метода рационального выбора средств и подсистем киберзащиты или обеспечения гарантоспособности радиотехнических (также, информационных) систем, оптимизации управления соответствующими средствами в условиях реализации угроз антропогенного или техногенного характера. В статье изучается возможность применения модифицированного генетического алгоритма для решения задачи рационального выбора средств защиты информации (СЗИ) и динамического управления конфигурациями таких средств в различных сегментах безопасности гарантоспособных радиотехнических систем (ГРС), а также информационных систем (ИС). Научная новизна исследования заключается в применении в генетическом алгоритме в качестве критериев оптимизации конфигурации (состава) СЗИ суммарной величины рисков от нарушения конфиденциальности, целостности и доступности информационного ресурса, а также стоимостные характеристики соответствующих СЗИ. Генетический алгоритм в задаче оптимизации выбора конфигурации СЗИ для ГРС (ИС) и динамического управления ресурсами подсистемы кибербезопасности рассматривается как вариант решения задачи мультивибора. В такой постановке задачи рационального размещения СЗИ на рубежах (уровнях) защиты ГРС (ИС) рассматривается как вариант решения NP-полной комбинаторной задачи оптимизации про укладку рюкзака (*Knapsack problems*). Предложенный подход обеспечивает возможность, с одной стороны, выполнить быстрое опробование различных наборов СЗИ и вариантов их применения в ГРС (ИС), с другой стороны, это создает предпосылки для объединения предложенного алгоритма с уже существующими методами, моделями и алгоритмами для оптимизации состава рубежей киберзащиты ГРС (ИС) и динамического управления ресурсами кибербезопасности для различных объектов информационной деятельности. Такое сочетание методов, моделей и алгоритмов создает предпосылки для быстрого изменения настроек подсистемы защиты ГРС (ИС), изменяя ее конфигурацию с учетом новых угроз и кибератак.

Ключевые слова: аппаратно-программные средства защиты информации; многокритериальная оптимизация; генетический алгоритм; система поддержки принятия решений; задача об укладке рюкзака

Method for Rational Management of the Cybersecurity and Reliability Radio Technical Systems

Hulak H. M., Lakhno V. A., Adiljanova S. A.

The urgent problem of creating a method for the rational choice of means and subsystems of cyber protection or ensuring the reliability of radio engineering (also, information) systems, optimizing the management of appropriate means in the context of the implementation of anthropogenic or technogenic threats is investigated. The article studies the possibility of using a modified genetic algorithm to solve the problem of rational choice of information security means (ISM) and dynamic configuration management of such means on various security segments of reliable radio engineering systems (RRS), as well as information systems (IS). The scientific novelty of the study is the use in the genetic algorithm as criteria for optimizing the configuration (composition) of the ISM total amount of risks of breach of confidentiality, integrity and availability of information resources, as well as the cost characteristics of the respective ISM. The genetic algorithm in the problem of optimizing the choice of ISM configuration for RRS (IS) and dynamic resource management of the cybersecurity subsystem is considered as a variant of solving the multichoice problem. In this formulation, the problem of rational placement of ISM at the boundaries (levels) of RRS (IS) protection is considered as a variant of solving the NP-complete combinatorial optimization problem of backpacking (*Knapsack problems*). The proposed approach provides an opportunity, on the one hand, to perform rapid testing of different sets of ISM and options for their application in ISM, on the other hand, this creates prerequisites for combining the proposed algorithm with existing methods, models and algorithms to optimize the boundaries of RRS (IS) cybersecurity and dynamic management of cybersecurity resources for various objects of information activities. This combination of methods, models and algorithms creates the preconditions for a rapid change in the settings of the RRS (IS) protection subsystem, changing its configuration to take into account new threats and cyberattacks.

Key words: hardware-software for information security; critical optimization; genetic algorithm; decision making system; Knapsack problems