

змінити їх – ні. Існують симетричні та асиметричні методи шифрування. Принцип обох відрізняється в підході створення ключа безпеки, його передачі та алгоритмом розшифрування.

Оскільки в захисті інформаційної системи зацікавлений не лише виробник систем передачі (маршрутизатори та супутнє обладнання, захищені платформи управління), який у свою чергу створює, адаптує, модернізує існуючі алгоритми захисту у своє обладнання; не лише структура, що організовує цю інфосистему, яка звісно ж на своєму рівні забезпечує захист даних, починаючи з не значних DDOS-атак і закінчуючи розгалуженою системою побудови та аналізу поведінки мережі, створенням ізольованих мереж (VPN тунелі), контролю та відсіювання злочинного трафіку, що може спричинити НСД до конфіденційної інформації; а звісно ж, основним об'єктом – є людина, яка і створює увесь цей загальний об'єм інформації!

Тому в першу чергу, безпека в інформаційній системі залежить тільки від нас самих, адже кожна дія в мережі, кожне переглядання, скачування, розповсюдження інформації не відбувається безслідно і робити це з розумом та розумінням про те, що нехтування забезпеченням власної безпеки хоча б на рівні антивірусного забезпечення, може спричинити до неприємних наслідків. Так, деякою мірою втраті даних можна завдячити корпораціям, які на своєму рівні забезпечують алгоритми захисту в мережах, які працюють хоча б з якою інформацією, яка потребує шифрування, але в той же час, вдосконалюються і алгоритми обходу систем захисту, і ця боротьба буде відбуватися постійно.

УДК 004.023

*D.V. Ievliev, master's degree, 501TN
O. V. Skakalina, Ph.D., associate professor
National University "Yury Kondratyuk Poltava Polytechnic"*

APPLIED ASPECT OF SOLVING THE BACKPACK PROBLEM USING A POPULATION-GENETIC ALGORITHM

Approximate algorithms for solving combinatorial optimization problems turn out to be indispensable in situations where obtaining an exact solution requires excessive time costs. Evolutionary algorithms (EA) originate in the works of L. Fogel, A. Owens and M. Walsh, J. Holland, where it was proposed to model the process of biological evolution in order to synthesize structures that are effective in a sense and create artificial intelligence (AI) systems.

A.G. Ivakhnenko and L.A. Rastrigin independently proposed methods of random search, where the ideas of evolution were also used. A characteristic feature of EA is the imitation of the process of evolutionary adaptation of a

biological population to environmental conditions, while individuals correspond to test points in the space of solutions to the optimization problem, and the fitness of individuals is determined by the values of the objective function and penalties for violating the constraints of the problem, if any. Within the framework of this approach, evolutionary strategies, genetic algorithms, algorithms for random search with adaptation, evolutionary modeling, genetic programming, multicriteria EA are proposed. The EA class can also include the Metropolis algorithms, simulated annealing, taboo search, etc. These algorithms differ in the ways of modeling the evolutionary process and reflected aspects, but they have many common elements. The areas of application of these algorithms also differ somewhat.

The principles of heredity, variability, and selection in evolutionary algorithms are implemented when constructing new descendant solutions by means of randomized procedures (operators) that modify previously obtained test points, similar to the processes of mutation and crossing over in nature. The selection of such trial points is carried out taking into account the values of the fitness function (individuals with an advantage in fitness are given greater chances for selection as parental solutions). Evolutionary algorithms can be used both for problems with one optimization criterion and for multi-criteria problems, therefore, a multi-criteria fitness vector function is also allowed. Due to the ease of adaptation of computational schemes of evolutionary algorithms, these methods are actively used to solve combinatorial optimization problems that arise in control, planning, design, pattern recognition, and other areas.

The knapsack problem (also knapsack problem) is an NP-complete combinatorial optimization problem. It got its name from the ultimate goal: to put as many valuable things as possible in a backpack, provided that the capacity of the backpack is limited. Various variations of the knapsack problem can be encountered in economics, applied mathematics, cryptography, and logistics. In today's Ukrainian conditions, this task is relevant for the formation of the so-called "alarm backpacks", for the optimal acquisition of front-line first-aid kits, packing of front-line transport containers. In general, the problem can be formulated as follows: from a given set of items with the properties "cost" and "weight", it is required to select a subset with the maximum total cost, while observing the restriction on the total weight.

The general statement of the problem is as follows: a backpack with capacity $V=80$ units and $m = 15$ items, leather with any size V_i and value C_i , $i=1,2,\dots,m$. It is necessary to place items of the highest total value in the backpack. Setting the encoding type - *Binary Coding*, selection operation - *Roulette Wheel Selection*, crossover operator - *Single Point Crossover*, mutation operator - *Flip Bit Mutation*. The code for the genetic algorithm of prompting based on the DEAP library toolkit. Creations of the protest algorithm on the test functions of De Jong, Rastrigin, Griewank. The optimal result was achieved with victorious experiment No. 4.