2. Пат. 111448 Україна, МПК H04L 29/14 (2006.01) H04L 9/14 (2006.01) H04L 9/06 (2006.01). Спосіб криптографічного перетворення двійкових даних. Горбенко І. Д., Долгов В. І., Лисицька І. В. та інші (Україна); заявник АО ІІТ м. Харків. № a201503976; заявл. 25.04.2015; опубл. 25.04.2016, Бюл. № 8. 20 с.

The principles of construction Rijndael cipher, used by developers that allow this cipher take a leading position in technology design and development of block symmetric ciphers. As a second progressive development marked cipher IDEA NXT. The results of the analysis of the prospects of the decisions taken in these developments. It is noted that in spite of their novelty and achieved high performance solutions considered, studies conducted in recent years indicate the possibility of further improvement, the possibility of building a better design encryption transformation. These features included in the proposed new design concept of block symmetric cipher that is based on a number of provisions put forward. Its implementation is demonstrated by the example of the development of a new cipher designs and modifications, based on the principles of controlled use pidstanovlyuvalnyh change. The design of the simplicity and transparency of decisions in terms of evidence-based resistance to attack by differential and linear cryptanalysis, and in terms of performance is not inferior to the acknowledged leader of technology block symmetric encryption cipher Rijndael (AES), and the dynamics coming cipher to a state of random permutation they are superior to almost all known solutions.

Key words: *technology design and development of block symmetric ciphers, linear matrix conversion efficiency encrypting conversion, the new concept of design and development BSSH linear transformation of keruyemymy substitutions, random substitution cipher dynamic performance coming to vypadkovoi substitution.*

Одержано 24.02.2017

УДК 004.04:004.056.5

Н. О. Маслова, канд. техн. наук, доцент

Донецький національний технічний університет, м. Покровськ

ЗАСТОСУВАННЯ ЗАДАЧІ РОЗПОДІЛУ РЕСУРСІВ В СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ

Проаналізовано застосування задач розподілу ресурсів в системах захисту інформації та методів їх вирішення; описано програмне забезпечення, яке дозволяє проводити експериментальні дослідження з вибору ефективного за часом алгоритму.

Ключові слова: *розподіл ресурсів, захист інформації, метод, програмний продукт.*

Вступ. Задача розподілу ресурсів — одна з найважливіших задач прикладного спрямування кібернетики, що використовується для вирішення безлічі практичних проблем. Це задачі розподілу грошових коштів; матеріальних запасів; водних потоків; мережевих ресурсів. Розподі-

льні завдання виникають у випадках, коли наявних ресурсів недостатньо для ефективного виконання робіт і необхідно найкращим чином розподілити їх між вузлами, об'єктами або роботами відповідно до самої задачі та обраного критерію оптимальності. Однією з актуальних проблем сьогодні є задача захисту інформації, рішення якої вимагає значних матеріальних, технічних, обчислювальних ресурсів та витрат на її реалізацію та застосування методів ефективного розподілу цих витрат.

Мета роботи — аналіз застосування методів розподілу ресурсів в задачах захисту інформації та опис програмного продукту, що призначено для проведення експериментальних досліджень з вибору найбільш ефективного для рішення конкретної задачі алгоритму розподілу.

Основи методів рішення задач розподілу ресурсів закладені як в роботах вітчизняних вчених (В. С. Михалевича [1], В. В. Шкурби, Н. З. Шора, А. І. Кукси і ряду інших), так і зарубіжних (Р. Конвей, Б. Джонсон, У. Максвелл, Б. Гіффлер, Ж. Томпсон).

Дослідження і публікації, що з'явилися останнім часом показують, що одним з важливих питань є формулювання задач оптимального розподілу ресурсів в галузі захисту інформації. Дослідження з цього питання публікують відомі вітчизняні вчені В. В. Домарев, Г. Г. Гріздов, В. Кононович [2–4], тема є актуальною й на міжнародних конференціях та в роботі наукових шкіл.

Так, у роботі [4, с. 152–161] проаналізовано задачу оптимізації витрат на інформаційну безпеку системи документальних телекомунікацій, яка зводиться до задачі багатокритеріального вибору. Запропоновано інтерактивну процедуру раціонального вибору варіанта розподілу витрат.

В роботі [5] наведено шість різних формулювань задачі оптимального розподілу ресурсів між різними функціями управління механізмами забезпечення захисту інформації. Пропонуються постановки задачі розподілу ресурсів, призначені для застосування як на стадії проектування систем забезпечення інформаційної безпеки, так і на стадіях її вдосконалення і розвитку. Автори виділяють сім основних функцій забезпечення захисту інформації [5, с. 113] і пропонують два підходи до деталізації і формалізації розподілу коштів між різними функціями системи захисту. Перший — облік складу і кількості засобів забезпечення захисту інформації та другий — заснований на аналізі узагальнених закономірностей і зв'язках між вкладеними в процес забезпечення захисту інформації засобами і ефективністю їх застосування. В роботі розглянуті ймовірні і вартісні моделі. Останні з яких представляють значних інтерес для авторів, уточнюючи фізичний зміст параметрів завдання розподілу ресурсів при введенні даних в пропонований авторами програмний продукт.

В роботі [6, с. 164–167] розглядається модель, коли розподіл ресурсів між об'єктами систем захисту інформації пропонується вико-

нувати на основі ігрової моделі і принципу рівної захищеності об'єктів. Задача розподілу ресурсів сформульована як турнір двох гравців — захисника і нападника з нульовою сумою. Кожен гравець вирішує завдання лінійного програмування при фіксованому вирішенні іншого гравця. В роботі запропоновано три алгоритми, які можуть застосовуватися послідовно для гарантованого отримання результату. Алгоритми обґрунтовані математично, отримані результати підтверджені тестовими прикладами і узагальнені.

Більшість програмних розробок, що реалізують ті чи інші математичні методи, є досить універсальним продуктом, таким, що дозволяє вирішувати безліч задач в залежності від підготовлених вхідних даних і сенсу, що в них вкладається. Основною особливістю програмного пакета, що пропонується в [7, с. 84], є наявність інтелектуального агента, що дозволяє вибрати найбільш ефективний за критерієм кількості обчислювальних операцій і часу виконання алгоритм, що вельми важливо при побудові систем захисту і своєчасному розподілі ресурсів, які цю роботу забезпечують.

Вирішення задач розподілу ресурсів проходить в online-режимі з урахуванням вимоги розміщенням інструментарію для вирішення завдання на «хмарному» сервісі, який дозволить користувачеві, минаючи пошук необхідного програмного забезпечення і процес інсталяції, отримати рішення необхідної задачі з описом цього рішення.

При підборі методів, які мають бути включені в пакет, слід виконати постановку задачі дослідження, що дозволяє визначити тип задачі та підготувати відповідним чином вхідні дані. Через різноманіття задач розподілу ресурсів, безлічі областей їх застосування, програмний продукт було розширено розділом рішення прикладних задач. Перелік розділів, що включено до пакету:

- розділ для вирішення класичних задач розподілу ресурсів (завдання розподілу ресурсів між підприємствами та завдання управління запасами);
- розділ для вирішення мережевих задач розподілу ресурсів (задачі про пошук найкоротшого шляху і про максимальний потік);
- розділ для рішення прикладних задач (включено задачу розподілу грошових ресурсів з метою зниження ризиків інформаційної безпеки за рахунок ліквідації деяких видів погроз);
- контрольний розділ, що містить методи і алгоритми (метод умовної оптимізації, метод гілок і меж, алгоритми прямого і зворотного прогону, алгоритми Качмажа і Балаша).

Розглянемо постановку задачі, яка реалізована в додатку [7, с. 83].

Є початкова кількість ресурсів (можливо, грошових коштів) $\overline{\xi}_0$, яку необхідно розподілити протягом n умовних періодів (кроків, прохо-

дів) між s погрозами (направити ресурси на зниження ризиків реалізації погроз). Ресурси, $u_{ki}\,(k=1,...,n;i=1,...,s)$, виділені на k-му кроці на подолання *i*-ї погрози, впливають на аналогічні погрози, що виникають на інших вузлах інформаційної системи і знижують ризики реалізації погрози у розмірі $f_{ki}(u_{ki})$ і до кінця умовного періоду знижують ризик реалізації погрози у розмірі $\varphi_{ki}(u_{ki})$. В подальшому розподілі це значення може або брати участь (частково або повністю), або не брати участь.

Потрібно знайти спосіб розподілу ресурсів, щоб сумарне зниження ризиків від реалізації s погроз за n умовних періодів було максимальним.

Як показник ефективності процесу розподілу ресурсів за n умовних періодів приймається сумарне зниження ризиків реалізації погроз:

$$Z=\sum_{i=1}^{s}\sum_{k=1}^{n}f_{ki}(u_{ki}). \qquad (1)$$

Кількість ресурсів на початку *k*-го умовного періоду характеризує величина ξ_{k-1}. Управління на *k*-му кроці полягає у виборі змінних $u_{k1},u_{k2},...,u_{ks}$, що позначають ресурси, виділені на *k*-му кроці на подолання і-ї погрози.

Якщо припустити, що зниження ризиків реалізації *i*-ї погрози у подальшому розподілі участі не бере, то рівняння стану процесу має вигляд

$$\xi_k=\xi_{k-1}-\sum_{i=1}^{s}u_{ki}+\sum_{i=1}^{s}\varphi_{ki}(u_{ki}). \qquad (2)$$

На рис. 1 показано прототип архітектури додатку, призначеного для вирішення задач розподілу ресурсів. При виборі методу рішення в розділі рішення задачі розподілу, пропонується перелік з шести методів.

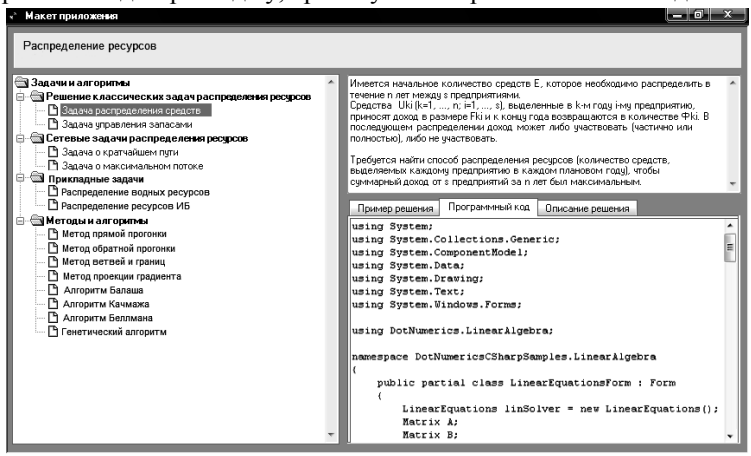

Рис. 1. *Прототип архітектури додатку*

Додаток має двох фреймову структуру.

Лівий фрейм містить навігаційну панель, представлену у вигляді дерева тем. Вибір відповідної теми користувачем впливає на зміст правого фрейму. Рис. 2 демонструє рішення умовної задачі розподілу ресурсів на забезпечення інформаційної безпеки за допомогою генетичного алгоритму.

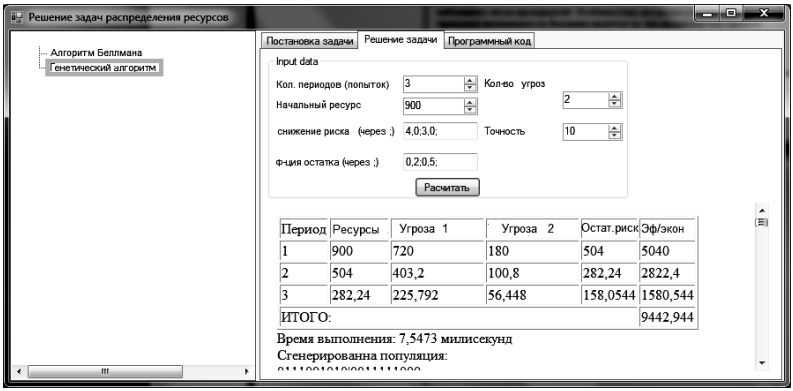

Рис. 2. *Рішення задачі генетичним алгоритмом*

Правий фрейм має три закладки, на яких відображені базова постановка задачі, що дозволяє користувачеві швидко зорієнтуватися у вхідних даних задачі, результат рішення і програмний код відповідного алгоритму.

В пакет включено додатковий режим «інтелектуальний агент», основним завданням якого є надання допомоги користувачеві в підборі найбільш ефективного за часом виконання алгоритму. Інформаційне повідомлення, що при необхідності формує агент, відображено на рис. 3.

Робота інтелектуального агента описана в [7, с. 84], архітектура пакета передбачає можливість установки на хмарі, що було протестоване з застосуванням Windows Azure.

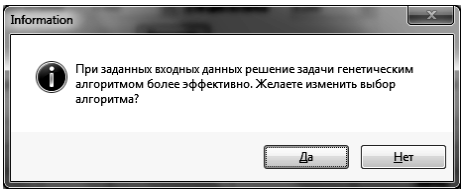

Рис. 3. *Робота інтелектуального агента*

Висновки. Проаналізовано застосування задач розподілу ресурсів в процесах захисту інформації. Показані сучасні підходи до обрання методів та побудови моделей розподілу ресурсів. Описано програмне забезпечення, яке за допомогою інтелектуального агента до-

зволяє проводити експериментальні дослідження з вибору ефективного за часом алгоритму.

Список використаних джерел:

1. Михалевич В. С., Кукса А. И. Методы последовательной оптимизации в дискретных сетевых задачах оптимального распределения ресурсов. М.: Наука, 1983. 208 с.
2. Домарев В. В. Безопасность информационных технологий. Методология создания систем защиты. К.: ООО «ТИД «ДС», 2002 688 с.
3. Грездов Г. Г. Способ решения задачи формирования комплексной системы защиты информации для автоматизированных систем 1 и 2 класса [Текст]. (Препринт/ НАН Украины. Отделение гибридных управляющих систем в энергетике ИПМЭ им. Г.П. Пухова НАН Украины; № 01/2005). К.: ЧП Нестреровой, 2005. 64 с.
4. Кононович В., Тардаскіна Т. Алгоритм розподілу ресурсів інформаційної безпеки документальних телекомунікацій. *Прав., нормат. та метрол. забезп. системи захисту інформації в Україні*. 2004. Вип. 9. С. 152–161.
5. Белов С. В., Попова Е. А., Кальнов М. В. Формализация задачи распределения ресурсов между различными функциями обеспечения защиты информации. *Вестник АГТУ. Серия: Управление, вычислительная техника и информатика*. 2012. № 1. С. 112–116.
6. Быков А. Ю., Шматова Е. С. Алгоритмы распределения ресурсов для защиты информации между объектами информационной системы на основе игровой модели и принципа равной защищенности объектов. *Наука и образование*. 2015. Вып. № 9. С. 160–187.
7. Маслова Н. А., Мовчан О. В. Использование интеллектуальных агентов при решении задач распределения ресурсов. *Штучний інтелект*. 2014. № 3. С. 80–89.

The resource allocation problems in the protection of information; methods of solving; described software for experimental research and choice effective over time algorithm.

Key words: *resource allocation, information security, method, software.*

Одержано 14.02.2017