doi.org/10.15407/usim.2019.05.023
УДК 364.2:331; 681.513

L.N. KOLIECHKINA, Doctor of Physical and mathematical sciences, Professor,
University of Lodz, 22 Banaha st.,
Lodz, 90-238, Poland,
ludapl@ukr.net

A.N. NAHIRNA, PhD, Physical and mathematical, Associate Professor,
National University of "Kyiv-Mohyla Academy",
2 Skovoroda st. , Kyiv, 04070, Ukraine
naghirnaalla@ukr.net

THE PRACTICAL ASPECT OF USING A COMBINATORIAL MODEL ON CONFIGURATION OF COMBINATIONS

The paper proposes the practical task of choosing a set of programs to protect information at the enterprise. An optimization combinatorial model is built on the configuration of combinations to solve the task. An algorithm for finding a solution to this optimization problem is presented. A practical example of the use of a optimization combinatorial model and the search for the best choice of a set of programs for data protection at the enterprise is given.

Keywords: *information security, combinatorial optimization, mathematical model, a configuration of combinations, objective function, restrictions.*

Introduction

Currently, the information security of an enterprise is one of the leading factors in its effective development. The information has a real value weight, which is clearly determined by the profit received during its use, or the damage that may be caused to an enterprise if it is used by other persons [1–2]. The share of organizations' expenses on ensuring the integrity of information and protecting it from possible external threats is constantly growing. However, the profitability of the enterprise depends on the profit and costs spent on making a profit. Therefore, enterprises are trying to optimize costs, and they want to buy only what is really necessary to build a reliable information protection system with minimal costs [3].

Various aspects of data protection and the use of various methods based on cryptography are described in [4–6].

An integrated information security system at an enterprise provides for the solution of a number of tasks that give a solution to security problems at the software, hardware and organizational levels [7, 8]. From a practical point of view, the software level of protection is the most strategically important. The market for data security software is very diverse. For reliable protection of information at the enterprise, it is necessary to have several programs in a package that should provide needed protection in terms of identifying destabilizing factors and successfully preventing various types of threats. At the same time, it should be noted that comprehensive software packages for data protection have a high cost, therefore it is necessary to be able to make the best choice from the provided software, taking into account the necessary conditions that form the basic principles of information security in an enterprise.

When modelling various processes and phenomena in various fields of activity, models are often used, which are presented as tasks of conditional optimization. Particularly noteworthy are the models of such problems considered on combinatorial sets. To date, a significant amount of work has been devoted to the study and investigation of models of combinatorial nature [9–10].

Despite the simplicity of constructing combinatorial sets, combinatorial optimization problems are complex and time-consuming from a computational point of view [11–12], so there is a need to develop new methods and algorithms for solving them.

Formulation of the Problem

In the software market, there are many software products to protect information. There is no need to purchase large quantities, but you need to make an effective choice that ensures the prevention of threats and minimal losses during unauthorized intrusions. It should be noted that the price policy in the software market plays the same important role when choosing.

Therefore, coming out of the main tasks of data protection and financial capabilities, as a rule, an enterprise needs to make a choice from the existing availability of programs of this type. It should be noted that data protection programs have a fairly wide range of overlapping functionalities. At the same time, vary significantly in price and implementation requirements.

Table 1. **Price range of programs depending on rating**

Rating of Programms	Price, $	
	p_1	p_2
$a_1 = 1$	c_{11}	c_{12}
$a_2 = 2$	c_{21}	c_{22}
$a_3 = 3$	c_{31}	c_{32}
…	…	…
$a_n = n$	c_{n1}	c_{n2}

Each program has a rating in a general database of programs for certain functions. For example, ratings of antivirus programs can be found on certain sites taking into account the assessment of the main characteristics, such as threat detection, performance, false positives and others.

For ease of presentation, we assume that 1 is the program with the lowest rating, respectively, n – with the highest rating. The main task is to choose a set of programs with the highest rating taking into account the conditions of an enterprise. We assume that the average statistical prices for programs of the corresponding rating are known, then the choice should provide for minimal costs for acquiring the programs with the highest rating.

Since this set of programs should ensure the protection of information of the enterprise as a whole, it is natural to assume that each structural unit of the enterprise has its requirements for data protection software. Programs may coincide or differ, which mathematically can be formulated as a system of inequalities.

It is necessary to choose a set of programs that should have the highest rating possible and satisfy the conditions of the structural units of the enterprise. The choice of such programs should ensure the minimization of the costs of their acquisition. When detailing the choice, it is possible to perform additional calculations of the objective function in the range of maximum and minimum average prices of data protection programs, taking into account their rating.

Combination Optimization Model

Let suppose that in the software market for an enterprise in a certain industry, information protection n programs that have their own specific rating $A = (a_1, a_2, ..., a_n)$, $(n \in N)$. Having conducted a comprehensive assessment to identify destabilizing factors and possible losses from the invasion, taking into account the financial activities of the enterprise, it was found that there is a need to purchase k from n programs for the comprehensive protection of information.

The price of each program, depending on the rating, can fluctuate in the following range (тab. 1).

The company has m departments involved in the processing of information, which is a trade secret.

The main signs of the selection of programs is their ability to prevent threats of the following type: virus attacks, unauthorized intrusions into the network, leakage of confidential information.

Each department has formed its necessary conditions for the selection of data protection programs, which are illustrated by the following constraints:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n \geq (\leq) b_1, \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n \geq (\leq) b_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n \geq (\leq) b_m. \end{cases} \quad (1)$$

It is necessary to make a choice of k out of n possible programs, those.to find such an element of a multitude of combinations that, taking into account the fulfillment of restrictions (1), would provide the minimum costs for purchasing programs of this rating.

Then, the objective function will be:

$$\min F = c_1x_1 + c_2x_2 + \ldots + c_nx_n, \quad (2)$$

where $c_1 = c_{12} - c_{11}, \ldots, c_n = c_{n2} - c_{n1}$.

Since it is necessary to choose k programs from n $(n \geq k)$, taking into account their rating, we can find a solution on the combinatorial set of combinations without repetitions C_n^k.

Then, taking into account constraints and rating of programs, the mathematical model of the problem of choosing the best set of data protection programs for an enterprise is presented as:

$$Z(\Phi, C_n^k(A)) : \min\{\Phi(a) \mid a \in C_n^k\} \quad (3)$$

$$D = \{x \in R^n \mid Gx \leq (\geq) b\},\ G \in R^{m\times m},\ b \in R^m, \quad (4)$$

where $\Phi(\mathrm{a}) = \sum_{j=1}^{n} c_j x_j$ – the objective function of the combinatorial set of combinations C_n^k.

Definition 1. Let a set $A = (a_1, a_2, \ldots, a_n)$, $(n \in N)$. A combination without repetitions of n elements by k $(n \geq k)$ is called k-elemental subset C of the set A and is denoted by C_n^k. Since the order of writing elements of the set is irrelevant, therefore, as a rule, the elements in each combination are written in ascending order [13].

We realize the bijective mapping of the set C_n^k. into space R^n by assigning a relevant vector $x \in R^n$ to each element $a \in C_n^k$. The image of a set C_n^k is denoted by $E_k^n \subset R^n$. As a result, we have the problem of combinatorial optimization in the Euclidean formulation (the problem of Euclidean combinatorial optimization)

$$Z(F, C_n^k) : \min\{F(a) \mid X \in D \subset C_n^k\} \quad (5)$$

additional constraints

$$D = \{x \in C_n^k \subset R^n \mid Gx \leq (\geq) b\}, \quad (6)$$

where G - $m \times n$ matrix, $b \in R^m$, while $\Phi(a) = F(x)$, $a \in C_n^k$, $x \in E_n^k$.

Next, we consider linear objective functions of the form

$$F(x) = \sum_{j=1}^{n} c_j x_j\,. \quad (7)$$

Additional linear constraints form a multifaceted set $D \subset R^n$.

Consider the algorithm of solving the problem (5)-(7).

Algorithm for Solving

The algorithm for solving the formulated problem consists of three steps, which ensure that the minimum of the objective function is found with additional restrictions on the set of combinations.

1. Finding the first reference solution.

According to Definition 1, the elements of a set of combinations are written in ascending order, so the first element of a set of combinations $(x_1, x_2, \ldots, x_{n-1}, x_n)$, where $(x_1 < x_2 < \ldots < x_{n-1} < x_n)$, must be taken as the starting point. Next, check the constraints (6).

If constraints (6) are satisfied, the first support solution is found and the target function is calculated. Next, go to step 2.

Otherwise, select the next point in ascending order. Notably, the number of elements in the set of combinations is a finite set.

2. Formation of the initial search conditions for the optimal solution.

A point of a set of combinations that satisfies all constraints (6) will be the first reference solution. For further search for the optimal solution, the initial conditions for finding the optimal solution are formed:

$$f(x_1, x_2, \ldots, x_n) = b,$$

$$\begin{cases} \Delta g_1(x_1,x_2,\ldots,x_n) \le (\ge)\Delta b_1, \quad \Delta b_1 = b_1 - g_1(x_1,x_2,\ldots,x_n), \\ \Delta g_2(x_1,x_2,\ldots,x_n) \le (\ge)\Delta b_2, \quad \Delta b_2 = b_2 - g_2(x_1,x_2,\ldots,x_n), \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ \Delta g_n(x_1,x_2,\ldots,x_n) \le (\ge)\Delta b_n, \quad \Delta b_n = b_n - g_n(x_1,x_2,\ldots,x_n). \end{cases} \quad (8)$$

The next point of the set of combinations is checked according to the constraints (8). If they are not fulfilled, then return to p. 1.1., if completed, go to step 3. For all subsequent points of calculating the growth of the constraints, be located behind the formula:

$$\Delta g = \Delta g_2 - \Delta g_1 = c_j(x_i^{g_2} - x_j^{g_1}) + c_i(x_j^{g_2} - x_i^{g_1}). \quad (9)$$

3. Improving the first reference solution.

The obtained point in step 2 is the optimal solution, it is necessary to check whether it can be improved. To do this, we find the increase in the objective function:

$$\Delta f = \Delta f_2 - \Delta f_1 = c_j(x_i^{f_2} * - x_j^{f_1}) + c_i(x_j^{f_2} - x_i^{f_1}) \ . \quad (10)$$

Since the minimum value of the objective function must be find, a necessary condition for improving the first reference solution is to reduce the growth of the objective function:

$$\Delta f \le 0. \quad (11)$$

If (11) is not satisfied, then the next point of the set of combinations in ascending order is considered and we verify it according to (8).

If (11) is satisfied, then the optimal solution is found.

Table 2. **The price range of programs depending on the rating for enterprise «OZONINVEST»**

Rating of Programms	Price, $	
	p_1	p_2
$a_1 = 1$	1500	2700
$a_2 = 2$	2300	3800
$a_3 = 3$	5300	7000
$a_4 = 4$	6000	8700
$a_5 = 5$	9000	10500
$a_6 = 6$	11200	14300

It should be noted that condition (8) is sufficient for the existence of an optimal solution, and condition (11) is necessary for its determination.

Example

In the software market for the «OZONINVEST» pharmaceutical industry, six information protection programs have been selected that have their own specific rating A = (1, 2, 3, 4, 5). After a comprehensive assessment at the enterprise, it was found that there is a need to purchase three of the six programs for comprehensive information protection. The price of each program, depending on the rating, can fluctuate in the following range (тab. 2).

The enterprise «OZONINVEST» consists of 3 divisions, which have formed their necessary conditions for choosing information protection programs, represented by the following constraints:

$$\begin{cases} 10x_1 + 7x_2 + 4x_3 \ge 20, \\ 8x_1 - 5x_2 + 2x_3 \le 5, \\ 2x_1 + 4x_2 + 6x_3 \ge 43. \end{cases}$$

According to how much, it is necessary to form a set of programs with the highest rating, but at minimal cost, then you should consider the values of the coefficients of the objective function, as the values p_1, тable 2:

$$\min F = c_1x_1 + c_2x_2 + c_3x_3 + c_4x_4 + c_5x_5 + c_6x_6.$$

Therefore, unselected programs are rated 0 in the objective function.

Since the elements of many combinations are ordered in increasing order, it is natural to assume that with an increase in the rating of programs, the value of the objective function increases. Therefore, the search for a solution should begin with the lowest rating of programs, taking into account the growth of the objective function.

Consider the point of combination set (1, 2, 3). Find the values of the constraints: g_1 = 16 < 20, constraint is not satisfied.

Analogically, for the point (1, 2, 4): $g_1 = 20 \ge 20$, $g_2 = 6 > 5$ constraint is not satisfied.

For the point (1, 2, 5): $g_1 = 24 \ge 20$, $g_2 = 8 > 5$ constraint is not satisfied.

For the point (1, 2, 6): $g_1 = 28 \geq 20$, $g_2 = 10 > 5$ constraint is not satisfied.

For the point (1, 3, 4): $g_1 = 27 \geq 20$, $g_2 = 1 \leq 5$, $g_1 = 38 < 43$ constraint is not satisfied.

For the point (1, 3, 5): $g_1 = 31 \geq 20$, $g_2 = 3 \leq 5$, $g_1 = 44 \geq 43$ constraints are satisfied, $F(135) = 62400$. Accordingly, the first supporting solution is found. Then the initial search conditions for the next supporting solution:

$$\begin{cases} \Delta g_1 \geq -11, \\ \Delta g_2 \leq 2, \\ \Delta g_3 \geq -1. \end{cases}$$

Consider the next point (1, 3, 6): $\Delta g_1 = 4 \geq -11$, $\Delta g_2 = 2 \leq 2$, $\Delta g_3 = 6 \geq -1$ constraints are satisfied, not $\Delta F(136) = 22200$. Therefore, this solution is not better than the previous one.

Therefore, point (1, 3, 5) is optimal solution. The minimum values of the objective function $\min F(136) = \{62400 \; - 76200\}$.

Answer: for comprehensive data protection, the enterprise «OZONINVEST» needs to purchase programs that have a 1st, 3th and 5th rating. The minimum cost of acquiring them will range from $ 62400 to $ 7600.

Conclusion

The analysis of the problem of choosing a set of programs for protecting information at an enterprise of any industry is carried out. An optimization combinatorial model is constructed, taking into account the emerging conditions for the selection of data protection programs, as well as the financial activities of the enterprise. Using the bijective mapping of multiple combinations into Euclidean space, the mathematical model was considered on the configuration of combinations.

An algorithm for solving the problem, consisting of three steps. At the first and second steps, the search for the supporting solution was carried out, and the third step ensures the finding of the optimal solution. A numerical example of the implementation of the considered optimization combinatorial model on the set of configuration of combinations is given.

Further research is aimed at constructing mathematical models on other combinatorial configurations with nonlinear objective functions.

REFERENCE

1. *R. Islam, A. Siddiqa, P. Uddin, A. Kumar and M.D. Hossain*, "An Efficient filtering based approach improving LSB image steganography using status bit along with AES cryptography, 2014, " IEEE Dhaka, Bangladesh, ISBN:978-14799-5179-6, May 2014 [3rd International Conf. on Informatics], pp. 1–6 .

2. *N. Manjunath and S.G. Hiremath*, Image and text steganography based on RSA and chaos cryptography algorithm with hash-LSB technique, 2015 , Intl. J. Electr. Electron. Comput. Syst., 3:5-9.

3. *S. Roy and P. Venkateswaran*, "Online payment system using steganography and visual cryptography, 2014, " IEEE Bhopal, India, ISBN:978-1-4799-2525-4, pp. 1–5, May [International Conf. on IEEE Students Electrical, Electronics and Computer Science, p. 1-6, 2014].

4. *M.E. Saleh, A.A. Aly and F.A. Omara,* Data security using cryptography and steganography techniques, 2016, Intl. J. Adv. Comput. Sci. Appl., 7:390-397.

5. *R.K. Sheth and R.M. Tank,* Image steganography techniques, 2016, Intl. J. Comput. Eng. Sci., 1:10-15.

6. *V. Yadav, V. Ingale, A. Sapkal and G. Patil,* Cryptographic steganography, 2014, J. Comput. Sci. Inf. Technol., pp. 17-23.

7. *G. Khalimov, E.V. Kotukh, Yu.O. Sherhiychuk and A. Marukhnenko,* Analysis of the implementation complexity of cryptosystem based on the Suzuki Group, 2019 , J. Telecommunications and Radio Engineering, 78(5):419-427.

8. *A.A. Gerasimov, R. E. Zhuchkov,* The mathematical models of information security mechanisms in personal data automated information systems of the state administration bodies, 2014, Vestnik Voronezhskogo instituta MVD Rossii, 4: pp. 282—289.

9. *Koliechkina L., Pichugina O.,* 2018, Multiobjective Optimization on Permutations with Applications, In DEStech Transactions on Computer Science and Engineering, IX International Conference on Optimization and Applications (OPTIMA 2018) (Supplementary Volume), pp. 61-75.

10. *Liudmyla Koliechkina, Alla Nahirna, Olena Dvirna*: Quadratic optimization problem on permutation set with simulation of applied tasks, 2019 , CEUR Workshop Proceedings Vol. 2353, pp. 651-663 .

11.*Тимофієва Н.К., Гриценко В.І.*. Комбинаторика в задачах штучного інтелекту. 2017. Управляющие системы и машины. № 2. С. 6-19, 37.

12. *Тимофієва Н.К.* Розв'язні задачі та комбінаторна оптимізація. Електротехнічні та комп'ютерні системи. 2014. № 13. С. 46-51.

13. *Koliechkina L., Pichugina O.* Multiobjective Optimization on Permutations with Applications, 2018, In DEStech Transactions on Computer Science and Engineering, IX International Conference on Optimization and Applications (OPTIMA 2018) (Supplementary Volume), pp. 61-75

14. *Liudmyla Koliechkina, Alla Nahirna, Olena Dvirna*. Quadratic optimization problem on permutation set with simulation of applied tasks, 2019, CEUR Workshop Proceedings Vol. 2353, pp. 651-663 .

15. *Yakovlev S., Kartashov O., Pichugina O., Koliechkina L.*, The Genetic Algorithms in Optimization Problem on Combinatorial Configurations, 2018, In 2018 International Conference on Innovations in Engineering, Technology and Sciences (ICIETS). Proceedings, Karnataka, India, 106–111.

16. *Semenova N.V., Kolechkina L.N., Nagornaya A.N.* On Approach to Solving Vector Problems with Fractionally Linear Functions of the Criteria on the Combinatorial Set of Arrangements. Journal of Automation and Information Sciences. 2010, Vol. 42, N 2. P. 67-80.

17. *Донець Г.П., Колєчкіна Л.М.* 2011. Екстремальні задачі на комбінаторних конфігураціях. Полтава: РВВ ПУЕТ, 309 с.

18. *Стоян Ю. Г., Яковлев С.В., Пичугина О.С.* 2017. Евклидовы комбинаторные конфигурации: монография. Харьков : Константа, 404 с.

Колєчкіна Л.М., доктор фіз.-мат. наук, професор,
Лодзький університет, вул. Банаха 22, Лодзь 90-238, Польща,
ludapl@ukr.net,

*Нагірна А.М.***,** канд. фіз.-мат. наук, доцент,
Національний університет «Києво-Могилянська академія»,
вул. Г. Сковороди, 2, м. Київ, 04070, Україна,
naghirnaalla@ukr.net

ПРАКТИЧНИЙ АСПЕКТ ЗАСТОСУВАННЯ КОМБІНАТОРНОЇ МОДЕЛІ НА КОНФІГУРАЦІЇ СПОЛУЧЕНЬ

Вступ. На ринку програмного забезпечення є багато програмних продуктів із захисту інформації. Виходячи з головних задач захисту інформації та фінансових можливостей, підприємству зддебільшого необхідно здійснювати вибір з поміж наявних програм цього типу. Вибір таких програм має забезпечувати мінімізацію витрат на їхнє придбання. При деталізації вибору, можна виконати додаткові розрахунки цільової функції в діапазоні максимуму та мінімуму середньо-статистичних цін програм захисту інформації, враховуючи їхні рейтинги. Для розв'язання цієї проблеми доцільно використовувати комбінаторну оптимізаційну модель на множині сполучень.

Мета статті — демонстрація використання комбінаторної оптимізаційної моделі на множині сполучень і представлення методу розв'язання задач цього типу.

Методи. Метод розв'язання задачі умовної оптимізації на комбінаторній множині сполучень.

Результати. Сформульовано проблему вибору програмного забезпечення із захисту інформації та запропоновано спосіб її розв'язання. Наразі задача моделюється комбінаторною оптимізаційною моделлю на множині сполучень. Запропоновано метод розв'язання задач цього типу. Наведено практичний приклад використання комбінаторної оптимізаційної моделі на множині сполучень.

Висновки. Запропоновану модель можна використовувати для моделювання задач, які передбачають сполучення об'єктів, процесів і т.ін. за умови мінімізації функції мети. Подальші дослідження будуть спрямовані на побудову оптимізаційних моделей на інших комбінаторних множинах із нелінійними функціями мети.

Ключові слова: *інформаційна безпека, комбінаторна оптимізаційна модель, множина сполучень, цільова функція, обмеження.*

Колечкина Л.Н., док. физ.-мат. наук, профессор,
Лодзинский университет, ул. Банаха 22, Лодзь 90-238, Польша,
ludapl@ukr.net,

Нагорная А.Н., канд. физ.-мат. наук, доцент,
Национальный университет «Киево-Могилянская академия»,
ул. Г. Сковороды, 2, м. Киев, 04070, Украина,
naghirnaalla@ukr.net,

ПРАКТИЧЕСКИЙ АСПЕКТ ПРИМЕНЕНИЯ КОМБИНАТОРНОЙ МОДЕЛИ НА КОНФИГУРАЦИИ СОЧЕТАНИЙ

Введение. На рынке программного обеспечения существует множество программных продуктов по защите информации. Выходя из основных задач о защите информации и финансовых возможностях, как правило, предприятию необходимо осуществлять выбор из имеющегося наличия программ данного типа. Выбор таких программ должен обеспечивать минимизацию затрат на их приобретение. При детализации выбора, можно произвести дополнительные расчеты целевой функции в диапазоне максимума и минимума среднестатистических цен программ по защите информации с учетом их рейтинга. При решении данной проблемы можно использовать комбинаторную оптимизационную модель на множестве сочетаний.

Целью данной статьи является демонстрация использования комбинаторной оптимизационной модели на множестве сочетаний и представления метода решения задач данного типа.

Методы. Метод решения задачи условной оптимизации на комбинаторном множестве сочетаний.

Результаты. Сформулирована проблема выбора программного обеспечения по защите информации и предложен подход к ее решению. В данном случае задача моделируется комбинаторной оптимизационной моделью на множестве сочетаний. Предложен метод решения задач данного типа. Рассмотрен практический пример применения комбинаторной оптимизационной модели на множестве сочетаний.

Выводы. С помощью предложенной модели можно моделировать задачи, которые предусматривают сочетание объектов, процессов и т.п. при условии минимизации функции цели. Дальнейшие исследования будут направлены на построение оптимизационных моделей на других комбинаторных множествах с нелинейными функциями цели.

Ключевые слова: *информационная безопасность, комбинаторная оптимизационная модель, множество сочетаний, целевая функция, ограничения.*