http://doi.org/10.35784/iapgos.6406

received: 17.07.2024 | revised: 16.02.2025 | accepted: 07.03.2025 | available online: 31.03.2025

MATHEMATICAL APPARATUS FOR FINDING THE OPTIMAL CONFIGURATION SECURE COMMUNICATION NETWORK WITH A SPECIFIED NUMBER OF SUBSCRIBERS

Volodymyr Khoroshko[1], Yuliia Khokhlachova[2], Oleksandr Laptiev[3], Al-Dalvash Ablullah Fowad[1]

[1]National Aviation University Department of Security of Information Technologies, Kyiv, Ukraine, [2]Kyiv National University of Trade and Economics, [3]Taras Shevchenko National University of Kyiv Department of Cyber Security and Information Protection, Kyiv, Ukraine.

Abstract. *Information flows in the world are growing very quickly. The exchange of information is growing rapidly. In connection with this fact, the existing mathematical apparatus and its practical application are constantly developing. The scientific and mathematical apparatus is aimed at finding the optimal configuration of the information communication network, solving the problem of building protected channels for the transmission of a large amount of data. A scientific task arises to develop a new and improve the existing mathematical apparatus for finding the optimal configuration of a protected communication network with a given number of subscribers. This scientific work is dedicated to the solution of this urgent task. The paper formulated and proved four Lemmas. The formulation of the Lemma made it possible to prove two new theorems that allow solving the task of finding the optimal configuration of a protected communication network with a given number of subscribers. Solutions to both partial and general tasks of the process of optimization and protection of transmission channels of a large amount of data are provided. Thus, the paper proposes a solution to the scientific task of finding the optimal configuration of a protected communication network with a given number of subscribers. The direction of further research may be the development of a software implementation of the given mathematical apparatus.*

Keywords: optimal configuration, communication network, subscriber, lemma, theorem, information protection

APARAT MATEMATYCZNY DO ZNAJDOWANIA OPTYMALNEJ KONFIGURACJI BEZPIECZNEJ SIECI KOMUNIKACYJNEJ Z OKREŚLONĄ LICZBĄ ABONENTÓW

Streszczenie. *Przepływ informacji na świecie rośnie bardzo szybko. Wymiana informacji szybko rośnie. W związku z tym istniejący aparat matematyczny i jego praktyczne zastosowanie stale się rozwijają. Aparat naukowo-matematyczny ma na celu znalezienie optymalnej konfiguracji sieci teleinformatycznej, rozwiązując problem budowy chronionych kanałów do transmisji dużej ilości danych. Powstaje zadanie naukowe polegające na opracowaniu nowego i udoskonaleniu istniejącego aparatu matematycznego do znajdowania optymalnej konfiguracji chronionej sieci komunikacyjnej przy zadanej liczbie abonentów. Niniejsza praca naukowa poświęcona jest rozwiązaniu tego pilnego zadania. W artykule sformułowano i udowodniono cztery lematy. Sformułowanie lematu umożliwiło udowodnienie dwóch nowych twierdzeń, które pozwalają rozwiązać zadanie znalezienia optymalnej konfiguracji chronionej sieci komunikacyjnej przy zadanej liczbie abonentów. Przedstawiono rozwiązania zarówno częściowych, jak i ogólnych zadań procesu optymalizacji i ochrony kanałów transmisji dużej ilości danych. W artykule zaproponowano zatem rozwiązanie naukowego zadania znalezienia optymalnej konfiguracji chronionej sieci komunikacyjnej przy zadanej liczbie abonentów. Kierunkiem dalszych badań może być opracowanie programowej implementacji zadanego aparatu matematycznego.*

Słowa kluczowe: konfiguracja optymalna, sieć komunikacyjna, abonent, lemat, twierdzenie, ochrona informacji

Introduction

The information needs of applied fields of knowledge are constantly growing. As a result, enhancing the efficiency of computers and information technologies remains a highly relevant and ongoing process. The primary function of communication systems is to provide users with a reliable and high-quality means of exchanging information. This includes ensuring secure data transmission over protected networks.

To achieve this goal, it is essential to design optimally configured information exchange or communication networks. In the past, the principle of minimizing the number of devices was a viable approach. However, in today's digital world, this principle is no longer applicable. The challenge lies not only in constructing an optimal network configuration but also in ensuring the security of the information transmitted within the network.

Although the formal theory of information security has developed relatively recently, numerous mathematical models now exist to address various aspects of cybersecurity. These models provide a theoretical foundation for building secure communication networks. Classic models such as Harrison-Ruzzo-Ullman, Take-Grant, Bell-LaPadula, and Biba have been extensively studied in scientific literature. They allow for a formal verification of network security. For instance, the Harrison-Ruzzo-Ullman access matrix model is based on relation theory, offering a structured approach to managing access control.

The Take-Grant access rights distribution model [5, 15] is built using the apparatus of graph theory.

The classic Bell-LaPadulla model and models based on it (secure transition model, authorized subject model, shared access model, secure transition model for a shared access system, authorized subject sharing model) are built using devices theories of relations and games. These models introduce the concepts of security functions and security level grids, which define all allowed relationships between system entities. In the models that develop the classic, various additional rules are also introduced that regulate the possibility of making transitions that change the security levels of the system's essence.

The Trusted Mach model is built using predicate theory. It is a model of states and events, uses the next value operator, which determines the new values of state variables after the events that have occurred.

The Law-Water-Mark (LWM) model is built using relational theory.

Despite the formal difference between these models, they all have in common that in one way or another, a set of subjects (users) U, objects (protected resources) R, access rights L, access requests Q (U, R), rules for providing access or denying access F(U,R,L).

Unfortunately, none of the above models incorporate concepts such as threats or protection mechanisms. As a result, they are of greater theoretical interest in terms of formally proving network security rather than practical applicability in constructing an optimally protected communication network with a specified number of subscribers. Therefore, the scientific challenge of designing an optimal secure communication network configuration for a given number of subscribers remains relevant.

1. Literature survey and problem statement

Modern data transmission networks are a complex complex of technical means, software, devices for managing the organizational structure, which allows the elements of the complex to function together and operate them with territorially distributed subscribers. Many publications are devoted to the problem of informatization of various structures, solving the problem of information security, and developing an optimal communication structure.

For example, works [1, 2] provide a description of the functions implemented by different levels of the protocol stack of the network reference model, and [8] describes the most widely used network protocol stacks and their relationship with the levels of the protocol stack of the information network reference model. But the process of general exchange of information is described, which does not answer the question of building an optimal, protected communication network.

In [9], the peculiarities the optimal topology of the transmission network are considered. Quality indicators have been determined a set of probabilistic-time characteristics of information transmission traffic packages. The conducted analysis showed the presence of the influence of changing the parameters on the bandwidth of data transmission. But the network optimization process is not given enough attention.

The principles of modeling computer networks at different architectural levels are considered in works [7, 10]. Models of procedures for managing a separate link of data transmission and a multi-link transport connection, which take into account distortion factors in communication channels, blocking of limited buffer memory of transit switching nodes, as well as the level of load on network connections and the conveyor effect, were studied. Methods of calculating operational characteristics of network topological structures, optimization of protocol parameters and structure of data transmission packets are proposed. But the processes of network optimization and information protection are not fully considered.

In work [6], general approaches related to the concept of "mechanism" in the cyber security system are considered. The primary definition of the mechanism in analytical dynamics systems is presented. The transformation of the concept of "mechanism" from mechanical systems to economic, social, and organizational-technological systems is traced. The definition of the mechanism that can be used in the analysis and design of decision-making systems is formulated, the features of the use of this concept in cyber security systems are considered. Special attention is given to the analysis and development of algorithmic mechanisms used in auction theory, as well as applications that leverage both classical and dynamic game theory. In works [13, 14], it is proposed to consider the decision-making mechanism in cyber security systems as a system of relations of various (individual, group, organizational) agents, whose interaction is aimed at solving the problem of ensuring adequate protection. It is noted that one of the variants of this approach is the decision-making mechanism. Unfortunately, only specific cases were considered. Generalization is not done.

In studies [3, 12], various security modules for information networks are examined, enabling the optimal regulation of external access to local information networks from an information security perspective. Numerical values for the likelihood of unauthorized access are determined based on the collected data, facilitating the optimal selection of protective mechanisms. However, the mathematical framework does not allow for a comprehensive, general solution to the problem. Thus, as a result of the study of scientific publications on the topic of the article, dissertations, patents and monographs, it was established that today there is an actual scientific task of improving the mathematical apparatus for finding the optimal configuration of a protected communication network with a given number of subscribers.

2. Concept and objectives of analysis

The purpose of the article. To propose a mathematical apparatus for finding the optimal configuration of a protected communication network with a given number of subscribers. For this, it is necessary to solve the scientific task of developing options for effective solutions for finding the optimal configuration of a protected network based on proven theorems.

3. Presenting main material

To find the optimal configuration of a secure communication network with a given number of subscribers, it is necessary to select a set of minds that only shows the number of vertices $\left[X_o\right] = p$, so that the number of subscribers is specified [4, 11].

For this situation, in a strongly connected digraph with overlapped arc ends $l\left(u\right) > 0$, it is necessary to know the submultiple, $X_o \subset X$, $\left[X_o\right] = p$, *(p < n)* for which the minimum parameter $T^* = \left(X, U^*\right)$, $U^* \subset U$, with the base $X_o \subset X$ will be the smallest. These goals can be determined by searching through possible subsets $Y \subset C$, $\left|Y\right| = p$, but every decision, with *p* close to *n/2*, requires consideration (p^n) of options, which is a very difficult task.

For *p = 1*, the problem under consideration can be reduced to a simplified problem for some auxiliary digraph $G_1 = \left(X_1, U_1\right)$. It is obtained from *G* by adding a new vertex *Z* as a root and new arcs $V_1, V_2, ..., V_n$ emanating from *Z* and entering the corresponding vertices $x_1 \in X$; length $l\left(V_1\right) = C$, *i = 1 ,2 ,…, n*, where $C = \sum\limits_{u \in v} l\left(u\right)$.

Solving the problem for the digraph G_1, we find the minimum (by the sum of arc lengths) output tree $T_1^* = \left(X_1, U_1^*\right), U_1^* \subset U$, with root *z* = *X₁*. It is easy to see that the output tree T_1^* contains exactly one arc V_{i0} from the set of added arcs $V_1, V_2, ..., V_n$. If we remove Z from this tree together V_{i0}, then the resulting digraph will be, for the found digraph, the minimum outgoing tree T^* rooted at the desired vertex.

For the general case (arbitrary *p*), no good (in the sense of Edmond's algorithm) algorithm for solving the formulated problem is known [5, 11]. Let us present some initial data based on which an effective algorithm for solving it will be described. The following procedures will serve as a starting point for further reasoning:

1. we present the algorithm *G* according to $\sigma_G\left(\left\{x\right\}\right), \forall_x \in X$;
2. take *i* = 0;
3. find the digraph *Ĝi = (X Ûi)*, where *Ûi* is the set of all obtained selected arcs;
4. check whether *Ĝi* is strongly connected. If yes, then go to point 8, otherwise – to point 5;
5. find strongly connected components $\widehat{G}_j^i = (\widehat{X}_j^i, \widehat{U}_j^i)$, in the digraph *Ĝi*: *j = 1, 2,…, g*;
6. draw a digraph *G* along $\sigma_G(\widehat{X}_j^i)$, *j = 1, 2, ..., g*;
7. replace *i* with *i + 1* and go to step 3;
8. the procedure is completed.

When carrying out this procedure, the question may arise about the existence of a strongly connected component $\widehat{X}_r^i = \left(\widehat{X}_r^i, \widehat{U}_r^i\right)$ such that $\sigma\widehat{G}_i\left(\widehat{X}_r^i\right) \neq \phi$, if the digraph $\widehat{G}^i = \left(X, \widehat{U}^i\right)$, is not strongly connected.

The answer to this question is given by the following lemma.

Lemma 1. Let $G^1 = \left(X_1 U^1\right), U^1 \subset U_1$ an arbitrary digraph *G*. Then the digraph *G* is strongly connected if and only if for any $Y \subset X$.

Consequently, if the digraph $\widehat{G}^i$ at the *i*-th iteration of the procedure is not strongly connected, then there must be a strongly connected component $\widehat{G}_r^i = \left(\widehat{X}_r^i, \widehat{U}_r^i\right)$ such that $\sigma_{\widehat{G}^i}\left(\widehat{X}_r^i\right) \equiv \phi$.

We will assume that the digraph $\widehat{G}^i = \left(X, \widehat{U}^i\right)$, for *i* = 0 (i.e., at the zero iteration) is a digraph $\widehat{G}^o = (X, \phi)$, where each vertex represents a connected component. Let *M* be the set of all X_j^i, *i = 0, 1, 2, ..., k - 1*; *g = 1, 2, ..., g*, which is formed during the execution of this procedure (k is the number of its iterations). Consider the function *g*: M→D, where $g\left(\widehat{X}_j^i\right)$ is the value of the set reduction constant $\widehat{X}_j^i$ after performing the *i*-th iteration of the procedure.

For an arbitrary set and any *Y*, *X*, we introduce the following responsibilities:

$$N_{M_1}\left(Y\right) = \left\{X_j^i \in M_1 / X_j^i \bigcap Y \neq \varphi\right\};$$

$$R_{M_1}\left(Y\right) = \sum_{X_j' \in N_{M1(Y)}} g\left(\widehat{X}_j^i\right).$$

It is easy to check that for any $X_1, X_2 \subset X$ and $M_1 \subset M$ the relations are valid:

$$R_{M_1}\left(X_1 \bigcup X_2\right) = R_{M_1}\left(X_1\right) + R_{M_1}(X_2) \ ,$$

$$M_2 = M_1 / N_{M_1}\left(X_1\right) \tag{1}$$

where:

$$R_{M_1}\left(X_1 \bigcup X_2\right) = \\ = R_{M_1}\left(X_1\right) + R_{M_1}(X_2) - \sum_{X_j^i \in N_{M1}(X_1) \bigcap N_{M1}(X_2)} g\left(\widehat{X}_j^i\right) \tag{2}$$

Let us now assume that for the digraph *G* the algorithm for solving the problem from the previous problem within $t\left(G\right) = X_0$, where X_0 is an arbitrary p-element subset of *X*. As a result of the direct algorithm, we obtain the set $A = \left\{X_j^i\right\}$, *i = 0, 1, 2, ..., k*; *j = 1, 2, ..., g*.

Lemma 2. If $A^1 = \left\{X_j^i \in A / \ f\left(X_j^i\right) \succ 0\right\}$,

$M^1 = \left\{X_j^i \in M / g\left(\widehat{X}_j^i\right) \succ 0\right\}$:

$$A^1 = M^1 / N_{M^1}\left(X_0\right) \tag{3}$$

Moreover, the functions *f* and g^1 on the set $M^1 / N_{M^1}\left(X_0\right)$ coincide.

Proof. Let $A_g^| \subseteq A$, where *g = 1*, 2, …, *k - 1*, in which $A_g^| = \left\{X_j^g \in A / f\left(X_j^g\right) \succ 0\right\}$, $M_r^| \subseteq M_1$, *r = 1*, 2, …, *k - 1*, where $M_r^1 = \left\{X_j^r \in M / g\left(\widehat{X}_j^g\right) \succ 0\right\}$; in other words A_g^i it represents a set of those X_j^g, which are formed directly during the *u*-th iteration of the procedure, which does not include the marked arcs *u* – $\widehat{U}^z$, emanating from outside the set $\widehat{X}_j^r$.

It is easy to notice that if a strongly connected component is formed on the *g*-th interval of the forward progression of the algorithm $G_{j_0}^q = \left(X_{j_0}^q, U_{j_0}^q\right)$, for which $f\left(X_{j_0}^q\right) > 0$, i.e. $X_{j_0}^q \in A_q^1$, then at the corresponding *q*-th iteration of the procedure exactly the same strongly connected component should be formed, and $f\left(X_{j_0}^q\right) = q\left(X_{j_0}^q\right)$. The opposite also happens: if the *u* iteration of the procedure, a strongly connected component is formed, $\widehat{G}_{j_1}^r = \left(\widehat{X}_{j_1}^r, \widehat{U}_{j_1}^r\right)$, vertex-free X_0 such that, $g\left(X_{j_1}^r\right)$>0, those $\widehat{X}_{j_1}^r \in M_r$, then at the corresponding *th* iteration of the forward step of the algorithm, exactly the same strongly connected component should be formed, and $g\left(\widehat{X}_{j_1}^r\right) = f\left(\widehat{X}_{j_1}^r\right)$.

Therefore, $\widehat{k} \geq k$ and $A_q^1 = M_q^1 / N_{M_q^1}\left(X_0\right)$, *q = 1,…, k;* $M_r^1 / N_{M_r^1}\left(X_0\right) = \varphi$, *r = k+1, k+2, ...,* $\widehat{k}$.

Since, $A^1 = \bigcup_{g=1}^{k} {}_1 A_g^1$, and $M^1 = \bigcup_{r=1}^{\widehat{k}} M_r^1$, then $A^1 = M^1 / N_{M^1}\left(X_0\right)$ the functions *f* and *g* on this set coincide.

Theorem 1. If $T^* = \left(X_1 U^*\right)$ is a minimal outgoing with a base $X_0 \subset X$ for a digraph $t\left(G\right) = X_0$ with, then:

$$L_{T^*} = \sum_{\widehat{X}_j \in M} g\left(\widehat{X}_j^i\right) - \sum_{X_j \in \widehat{N}_M(X_0)} g\left(\widehat{X}_j^i\right) \tag{4}$$

Proof. Let us assume that for the digraph G the $t\left(G\right) = X_0$ an algorithm for solving the problem was applied. As a result, a set was formed $A = \left\{X_j^i\right\}$, *i = 0, 1, 2, ..., k, j = 1, 2, ..., q_i*. Then, using Lemma 2 (relation 4), we obtain

$$L_{T^*} = \sum_{X_j^i \in A} f\left(X_j^i\right) = \sum_{X_j^i \in A^1} f\left(X_j^i\right) = \sum_{\widehat{X}_j^i \in M^1 / N_{M^1}(X_0)} g\left(\widehat{X}_j^i\right) = \\ \sum_{\widehat{X}_j^i \in M / N_M(X_0)} g\left(\widehat{X}_j^i\right) = \sum_{\widehat{X}_j^i \in M} g\left(\widehat{X}_j^i\right) - \sum_{\widehat{X}_j^i \in N_M(X_0)} g\left(\widehat{X}_j^i\right).$$

Q.E.D.

From formula (4) it immediately follows that problem reduces to the following auxiliary problem: find in the set *X* the quantity X_0^*, $\left|X_0^*\right| = p$, for which $R_M\left(X_0^*\right)$ the maximum.

Theorem 2. Let $X^0 \subset X$, $X^0 = \left\{x_1^0, x_2^0, ..., x_p^0\right\}$, where elements $x_1^0 \in X^0$ are obtained as follows: we x_1^0 take the vertex for which, $R_M\left(\left\{x_1^0\right\}\right) = \max_{x \in X} R_M\left(\left\{x\right\}\right)$, we take x_2^0 – the vertex for which $R_{M1}\left(\left\{x_2^0\right\}\right) = \max_{x \in X / \left\{x_1^0\right\}} R_{M_1}\left(\left\{x\right\}\right)$, where we take x_3^0 – the vertex for which $R_{M2}\left(\left\{x_3^0\right\}\right) = \max_{x \in X / \left\{x_1^0, x_2^0\right\}} R_{M2}\left(\left\{x\right\}\right)$, where $M_2 = M_1 / N_{M_1}\left(\left\{x_2\right\}\right)$ etc., as x_p^0 – we take the vertex, for which $R_{M\,p-1}\left(\left\{x_p^0\right\}\right) = \max_{x \in X / \left\{x_1^0, ..., x_{p-1}^0\right\}} R_{Mp-1}\left(\left\{x\right\}\right)$, where

$$M_{p-1} = M_{p-2} / N_{Mp-2}\left(\left\{x_{p-1}^0\right\}\right).$$

Then the quantity X_0 is the optimal solution to the auxiliary problem, and therefore to Problem (1), i.e. $X_0 = X_0^*$. The proof of the theorem is preceded by:

Lemma 3. Let $M^1 \in M$, $Y \subset X$ be arbitrary sets, and $x \in X$ be an arbitrary vertex. Then in the set *Y* there exists a vertex *y* such that:

$$N_{M^1}\left(\{x\}\right) \cap N_{M^1}\left(\{y\}\right) = N_{M^1}\left(\{x\}\right) \cap N_{M^1}\left(y\right)$$

Proof. Let *i₁* be the smallest of those j for which $\widehat{X}_{j_1}^{i_1} \in N_{M_1}\left(\{x\}\right) \cap N_{M_1}\left(Y\right)$. Since the structure of sets $\widehat{X}_j^i \in M^1$ is such that any two of them either do not have common vertices, or one of them is entirely contained in the other, then:

$$N_{M^1}\left(\{x\}\right) \cap N_{M^1}\left(Y\right) = \left\{X_j^i \in M^1 / \widehat{X}_j^i \cap \widehat{X}_{j_1}^{i_1} \neq \varphi\right\}$$

Hence:

$$N_{M^1}\left(\{x\}\right) \cap N_{M^1}\left(Y\right) = N_{M^1}\left(\{x\}\right) \cap N_{M^1}\left(\widehat{X}_{j_1}^{i_1}\right)$$

It's easy to see that $\forall y \in \widehat{X}_{j_1}^{i_1}$, $N_{M^1}\left(\{x\}\right) \cap N_{M^1}\left(\{y\}\right) = N_{M^1}\left(\{x\}\right) \cap N_{M^1}\left(\left\{\widehat{X}_{j_1}^{i_1}\right\}\right)$; together with the previous equality we get $N_{M^1}\left(\{x\}\right) \cap N_{M^1}\left(\{y\}\right) = N_{M^1}\left(\{x\}\right) \cap N_{M^1}\left(Y\right)$.

The lemma is proven.

To prove Theorem 2, we need one more property of finite sets, which is proved by Lemma 4.

Lemma 4. If Y_1, Y_2, Y_3, Y_4 – arbitrary finite sets and if $Y_1 \cap Y_3 \subset Y_2 \cap Y_3$, then $Y_1 \cap \left(Y_3/Y_4\right) \subseteq Y_2 \cap \left(Y_3/Y_4\right)$.

The proof of the lemma is obvious.

Now after the proofs of Lemma 3 and Lemma 4, we can proceed to the proof of Theorem 2.

Proof of Theorem 2. Let be $X_0^* = \left(x_1^*, x_2^*, \ldots, x_p^*\right)$ – the optimal solution to the auxiliary problem; let's pretend that $X_0^* \neq X^0$. Let's consider the first of the vertices $X_r^0 \in X^0$, which is obtained according to the rule stated in the theorem, and does not belong to the set X_0^*.

A bunch of X_0^* let's represent it in the form $X_0^* = X_r^o \cup X_r^*$, where $X_r^0 = \left\{x_i^0 \in X^0 / i \prec 0\right\}$, $X_r^* = X_0^* / \ X_r^0$. Take an arbitrary vertex $x_s^* \in X_r^*$ and form a set:

$$Y_1^* = \left(X_0^* / \left\{x_s^*\right\}\right) \cup \left\{x_r^0\right\} = X_r^0 \cup \left(X_r^* / \left\{x_s^*\right\}\right) \cup \left\{x_r^*\right\}$$

According to (1) we have:

$$R_M\left(X_0^*\right) = R_M\left(X_r^0\right) + R_{M_1}\left(X_r^*\right) \tag{5}$$

where $M_1 = M / N_M\left(X_r^0\right)$;

$$R_M\left(Y_1^*\right) = R_M\left(X_r^0\right) + R_{M_1}\left[\left(X_r^* / \left\{x_s^*\right\}\right) \cup \left\{x_r^0\right\}\right] \tag{6}$$

Using relation (7) for $R_M\left(X_r^*\right)$ and:

$$R_{M_1}\left[\left(X_r^* / \left\{x_s^*\right\}\right) \cup \left\{x_r^0\right\}\right]$$

we get:

$$\begin{gathered} R_M\left(X_r^*\right) = R_{M_1}\left(\left\{x_s^*\right\}\right) + \\ + R_{M_1}\left(X_r^* / \left\{x_s^*\right\}\right) - \sum_{X_j^i \in \widehat{N}_{M_1}\left(\left\{x_s^*\right\}\right) \cap N_{M_1}\left(X_r^s / \left\{x_s^*\right\}\right)} g\left(\widehat{X}_j^i\right) \end{gathered} \tag{7}$$

$$\begin{gathered} R_{M1}\left[\left(X_r^* / \left\{x_s^*\right\}\right) \cup \left\{x_z^0\right\}\right] = R_{M_1}\left(\left\{x_r^0\right\}\right) + \\ + R_{M_1}\left(X_r^* / \left\{x_s^*\right\}\right) - \sum_{X_j^i \in \widehat{N}_{M_1}\left(\left\{x_r^*\right\}\right) \cap N_{M_1}\left(X_r^* / \left\{x_s^*\right\}\right)} g\left(\widehat{X}_j^i\right) \end{gathered} \tag{8}$$

According to Lemma 3, there is a vertex X_r^* in the set x_q^* such that:

$$N_{M_1}\left(\left\{x_r^0\right\}\right) \cap N_{M_1}\left(\left\{x_q^*\right\}\right) = N_{M_1}\left(\left\{x_r^0\right\}\right) \cap N_{M_1}\left(X_r^*\right) \tag{9}$$

Due to the fact that $N_{M_1}\left(\left\{x_q^*\right\}\right) \subseteq N_{M_1}\left(X_r^*\right)$, $N_{M_1}\left(\left\{x_r^0\right\}\right) \cap \ N_{M_1}\left(\left\{x_q^*\right\}\right) \subseteq N_{M_1}\left(\left\{x_q^*\right\}\right) \cap N_{M_1}\left(X_r^*\right)$. From this expression and from (9) it follows:

$$N_{M_1}\left(\left\{x_r^0\right\}\right) \cap N_{M_1}\left(\left\{x_r^*\right\}\right) \subseteq N_{M_1}\left(\left\{x_q^0\right\}\right) \cap N_{M_1}\left(X_r^*\right)$$

Those:

$$\begin{gathered} N_{M_1}\left(\left\{x_r^0\right\}\right) \cap \Big[N_{M_1}\left(X_r^* / \left\{x_q^*\right\}\right) \cup N_{M_1}\left(\left\{x_q^*\right\}\right)\Big] \subseteq \\ N_{M_1}\left(\left\{x_q^*\right\}\right) \cap \Big[N_{M_1}\left(X_r^* / \left\{x_q^*\right\}\right) \cup N_{M_1}\left(\left\{x_q^*\right\}\right)\Big] \end{gathered}$$

whence, based on Lemma 4, we get:

$$\begin{gathered} N_{M_1}\left(\left\{x_r^0\right\}\right) \cap N_{M_1}\left(X_r^* / \left\{x_q^*\right\}\right) \subseteq \\ N_{M_1}\left(\left\{x_q^*\right\}\right) \cap N_{M_1}\left(X_r^* / \left\{x_q^*\right\}\right)\Big] \end{gathered} \tag{10}$$

Thus, if we take $X_s^* = X_q^*$, then by virtue of the obtained relation (10) the inequality will always hold:

$$\sum_{X_j^i \in N_{M_1}\left(\left\{x_r^0\right\}\right) \cap N_{M_1}\left(X_r^* / \left\{x_s^*\right\}\right)} g\left(\widehat{X}_j^i\right) \leq \sum_{X_j^i \in N_{M_1}\left(\left\{x_s^*\right\}\right) \cap N_{M_1}\left(X_r^* / \left\{x_s^*\right\}\right)} g\left(\widehat{X}_j^i\right)$$

Because $R_M\left(\left\{x_r^0\right\}\right) \geq R_M\left(\left\{X_s^*\right\}\right)$, then taking into account expressions (5)-(8) $R_M\left(\left\{X_r^0\right\}\right) \leq R_M\left(\left\{Y_1^*\right\}\right)$.

From this and from what is the optimal solution to the auxiliary problem, it follows that $R_M\left(X_0^*\right) = R_M\left(Y_1^*\right)$ also the optimal solution for this problem.

If $Y_1^* \neq X^0$, then relatively Y_1^* it is possible to carry out similar reasoning and find a new solution Y_2^*. Continuing this process, after a certain number of steps we obtain the set $Y_1^* = X^0$, which will be the optimal solution to the auxiliary problem, and, consequently, to our problem. Those. The theorem is proven.

Note that the problem can be solved effectively in the case when the set X_0^* is defined in a certain subset $Y \subset X$, $|Y| = P_1 \succ P$. Rules for choosing a set under X_0^* such a restriction can be obtained if, in the conditions of Theorem 2, we replace *X* with *Y*.

Note also that the considered auxiliary problem is a special case of another, more general one, which is convenient to formulate on the basis of the theory of hypergraphs: given a hypergraph, $\xi = (X, \varepsilon)$, $|X| = n$, where to each hyper edge $E_j \subset \varepsilon$ number is matched; $g\left(E_j\right) \geq 0$; need to find a subset $Y^* \subset X$, $\left|Y^*\right| = p$, for which $R\left(Y^*\right) = \max\limits_{\substack{Y \subset X \\ |Y| = p}} P(Y)$, where $R(Y) = \sum\limits_{\substack{E_i \subset \varepsilon \\ E_i \cap Y \neq \varphi}} g\left(E_i\right)$.

In fact, the pair (*X*, *Y*) denotes a hypergraph, and the skin sub multiplier is assigned the number $g = \left(\widehat{X}_j^i \geq 0\right)$. One hypergraph (*X*, *M*) has such power: even if there are two hypergraphs, either they do not have hidden vertices, or one of them is embedded in the other. As has been shown (Theorem 2), in this case the problem is effectively observed. In general, if the hypergraph can and does not mother power, it is unlikely that optimal algorithms will be discovered, since it is not important to show that they can be brought to the class of combinatorial tasks.

4. Summary

A well-founded mathematical apparatus for finding the optimal configuration of a protected communication network with a given number of subscribers is proposed. The novelty of the proposed mathematical apparatus is based on proven four lemmas and proven two theorems. Thus, the goal of the work on the development of a new variant of the mathematical apparatus for finding the optimal configuration of a protected communication network with a given number of subscribers has been achieved. The direction of further research may be the development of a software implementation of the given mathematical apparatus.

References

[1] Al-Dalvash A.: Models of optimal fuel functioning of remote access security in information networks. Ukrainian Scientific Journal of Information Security 26(3), 2021, 126–131 [https://doi.org/10.18372/2225-5036.27.16513].

[2] Barabash O. V. et al.: Target Programming with Multicriteria Restrictions Application to the Defense Budget Optimization. Advances in Military Technology 14(2), 2019, 213–229.

[3] Buryachok V. L. et al.: Information and cyber security: socio-technical aspect. DUT, Kyiv 2015, 24–30.

[4] Khoroshko V. et al.: Optimization of information structures of local networks. Informatics and mathematical methods in modeling 10(1-2), 2020, 45–54.

[5] Khoroshko V. et al.: Synthesis of the optimal topology of the data transmission network. Legal, regulatory and metrological support of the information protection system in Ukraine 2(28), 2022, 20–28.

[6] Kyrychok R. et al.: Development of a method for checking vulnerabilities of a corporate network using Bernstein transformations. Eastern-European journal of enterprise technologies 1(9), 2022, 93–101 [https://doi.org/10.15587/1729-4061.2022.253530].

[7] Laptiev O. et al.: The method of spectral analysis of the determination of random digital signals. International Journal of Communication Networks and Information Security (IJCNIS) 13(2), 2021, 271–277 [https://doi.org/10.54039/ijcnis.v13i2.5008].

[8] Lukova-Chuiko N. et al.: The method detection of radio signals by estimating the parameters signals of eversible Gaussian propagation. IEEE 3rd International Conference on Advanced Trends in Information Theory, ATIT 2021, 67–70.

[9] Milov O. et al.: Mechanisms of cyber security: the problem of conceptualization. Ukrainian Scientific Journal of Information Security 25(2), 2019, 110–116 [https://doi.org/10.18372/2225-5036. 25.13841].

[10] Mukhamadieva Z. B.: Algorithms of the optimal structure of a computer network. A young scientist 22(102), 2015, 29–30.

[11] Sobchuk V. et al.: Algorithm for solution of systems of singularly perturbed differential equations with a differential turning point. Bulletin of the Polish Academy of Sciences Technical Sciences 71(3), 2023, e145682 [https://doi.org/10.24425/bpasts.2023.145682 WoS].

[12] Sobchuk V. et al.: Ensuring the properties of functional stability of manufacturing processes based on the application of neural networks CEUR Workshop Proceedings, 2021, 2845, 106–116.

[13] Sobchuk V. et al.: The limited solutions method for telecommunications network information security models. IEEE 3rd International Conference on Advanced Trends in Information Theory, ATIT 2021. 2021, 126–131.

[14] Tolyupa S. et al.: Formation of a strategy for managing the modes of operation of protection systems based on the game management model. Security of information systems and technologies 3, 2020, 78–86.

[15] Zamrii I. V. et al.: Algorithm of control and prediction of functional stability of complex information and technical systems. Telecommunications and information technologies 1(74), 2022, 4–15.

Prof. Volodymyr Khoroshko
e-mail: professor_va@ukr.net

Doctor of Technical Science, professor, Department of Information Technology Security of the National Aviation University.
Over 500 scientific publications, including scientific articles, monographs, textbooks and educational and methodological manuals.
He has been working in the field of higher education for more than fifty years.

https://orcid.org/0000-0001-6213-7086

D.Sc. Oleksandr Laptiev
e-mail: olaptiev@knu.ua

Doctor of Technical Science, Associate Professor, Department of cyber security and information protection of the Taras Shevchenko National University of Kyiv.
Over 110 scientific publications, including scientific articles, monographs, textbooks and teaching aids.
He has been working in the field of higher education for more than thirty years.

https://orcid.org/0000-0002-4194-402X

Prof. Yuliia Khokhlachova
e-mail: yuliiahohlachova@gmail.com

Candidate of Technical Science, professor, Department of Software Engineering and Cyber Security of the Kyiv National University of Trade and Economics.
Over 100 scientific publications, including scientific articles, monographs, textbooks and teaching aids.
She has been working in the field of higher education for more than thirty years.

https://orcid.org/0000-0002-1883-8704

M.Sc. Al-Dalvash Ablullah Fowad
e-mail: abdullah.dalosh@gmail.com

Postgraduate student, Department of information technology security, National Aviation University, Kyiv, Ukraine.

https://orcid.org/0000-0001-1003-9182