Models and Methods of Evaluation the Vulnerability of Complex Hierarchical Network Systems

Olexandr Polishchuk[a] , Mykhailo Yadzhak[a,b]

[a] *Pidstryhach Institute for Applied Problems of Mechanics and Mathematics, National Academy of Sciences of Ukraine, Naukova str, 3"b", Lviv, 79060, Ukraine*
[b] *Ivan Franko Lviv National University, University str, 1, Lviv, 79000, Ukraine*

Abstract

Principles of formation of system hierarchies with direct subordination are described and threats that can destabilize their state and operation process are analyzed. Strategies for the protection of complex hierarchical network systems (CHNS) against targeted attacks of various types are studied. On the basis of structural and flow models of CHNS, the elements and subsystems that require priority protection against such attacks are determined. The problem of simultaneous group lesions of the most important CHNS components of different hierarchical levels is investigated. In order to counteract the lesions spreading and overcome its consequences, the principles of forming an information and complex evaluation models of the CHNS state and operation process are proposed. It is shown how the application of these models before, during and after targeted attack helps to support a decision-making directed to restoring the system and returning it to normal life activities.

Keywords

Complex network, hierarchical network system, flow, core, influence, betweenness, vulnerability, targeted attack, information model, evaluation model, aggregation

1. Introduction

Various internal and external influences constantly act on every natural or man-made system. These influences can be positive (implemention of modern technologies, useful public initiatives, medical practices) or negative (the spread of false information, infectious diseases, military aggression, etc). They can have a local, group or system-wide character, act sequentially or simultaneously, be unexpected or conditionally predictable, centralized and decentralized, affect the structure and/or system operation process and so on. [1]. All of the listed above influences can be characteristic of both targeted attacks on the system and its non-target lesions. Difficulties in classifying possible influences are caused by the fact that different reasons can lead to similar consequences (the scale of destruction and the number of victims as a result of destroyed by rushists Mariupol and the earthquake in Turkey in January 2023) and similar causes can generate different consequences (epidemics of coronaviruses Sars-Cov-1 in 2002 in China with lethality 11%, MERS in 2009 in the Middle East with lethality 34% and Sars-Cov-2 (Covid-19) in 2019 with lethality 3%, of which only the latter turned into a global pandemic). Understanding what impacts can affect a specific system, how this system will respond to this or another type of influence and what consequences it can lead to generally determines what management decisions and protection means must be made and used to minimize the outcomes of such influences [2].

The most of man-made systems (economic, financial, public administration, military, religious, etc) have a hierarchical network structure [3]. Methods of hierarchization are also often used in the process of studying natural systems (Linnaean hierarchy, division of the universe into separate galaxies, star clusters and systems, etc.) [4]. System hierarchies can be formed according to different principles [5] – ordering, when less is a part of more; subordination, if each element of a certain hierarchycal level is the manager for elements of lower and controlled by the elements of higher

ICST-2023: Information Control Systems & Technologies, September 21-23, 2023, Odesa, Ukraine.
EMAIL: od_polishchuk@ukr.net (Olexandr Polishchuk); yadzhak_ms@ukr.net (Mykhailo Yadzhak)
ORCID: 0000-0002-0054-7159 (Olexandr Polishchuk); 0000-0001-6070-6142 (Mykhailo Yadzhak)

hierarchycal level; hybrid, when up to a certain level, CHNS subsystems are formed according to the principle of subordination, and at higher levels – the ordering, etc. Most acutely, especially in crisis situations, the problem of decision-making support appears in complex man-made hierarchical network systems of direct subordination [6]. Therefore, the study of peculiarities of the structure and principles of functioning of such systems, which are usually called interdependent in the theory of complex networks (TCN), especially under the act of internal and external negative influences, arouses considerable interest of scientists in various subject areas [7-9]. In this article, we will analyze the behavior of CHNS depending on the nature of influence acting on it and the consequences to which such influence can lead (section 2), describe typical strategies for protecting the system against targeted attacks of various types and identify their main advantages and disadvantages (section 3), consider the structural (section 4) and flow (section 5) CHNS models and based on them methods of determining the system elements that require priority protection, formulate the principles of detection the most important from a structural and functional points of view CHNS components of different hierarchical levels (section 6), describe the main approaches to evaluating and overcoming the consequences of targeted attacks (Section 7) and optimizing the decision-making support process using the latest methods of calculations parallelization and the modern computing tools (Section 8).

2. Lesions of complex hierarchical network systems

When studying the real complex systems and intersystem interactions, we are actually investigating models of these systems and interactions, created on the basis of observations, empirical and theoretical data, etc. In TCN, the most general type of interacting systems are multidimensional multilayer networks (MLN) [10, 11], each layer of which reflects the structure of separate system, and interlayer connections – the structure of intersystem interactions. At the same time, each layer of such MLN ensures the movement of certain type of flows [12]. It is obvious that any CHNS of direct subordination can be represented in the form of two interdependent and interacting systems (Fig. 1):

1) basic system (BS), i.e. network, to ensure the movement of certain types of flows (railway, automobile, financial, informational, etc.) CHNS was created and exists; we will call these flows basic
2) a multilevel (multilayer) management system (MS), the main purpose of creation and existence of which is the effective organization of the movement of flows in the base system.

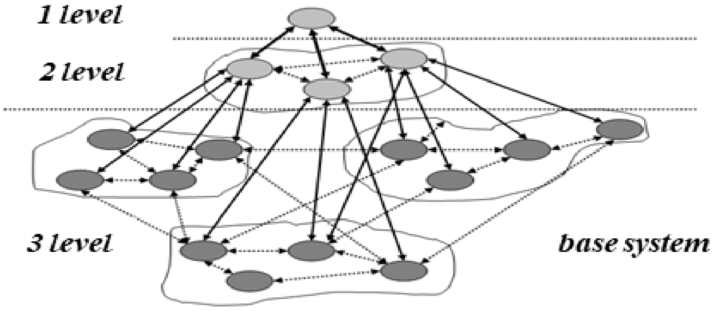


Figure 1: Example of CHNS with three-level hierarchically-network structure

It is obvious that the existence of management system without base system loses any meaning and the long-term effective operation of any complex network base system is impossible without appropriate management. To simplify the presentation, we will assume that the main type of flows that move through the CHNS management system are information flows. Of course, data exchange is possible between any two nodes of the same level of the CHNS hierarchy, including BS nodes, as it happens even in such strict hierarchies as military or security. Therefore, by information flows in the MS we understand data that relate to the description of state and operation process of elements and subsystems of CHMS, management and organizational decisions made on their basis, as well as notifications about the implementation of these decisions or problems that prevent their realization.

Usually, an attack in TCN refers to actions aimed at the deliberate removal from the system structure (destruction) of a certain number of the most important nodes for a definite characteristic in order to change the structural properties of network [13, 14]. Another method of attack consists in destabilizing or stopping the operation process of separate components or the system at a whole without directly damaging its elements – creating conditions for a critical loading (DDoS attack), blocking separate nodes and connections (sea ports of Ukraine during the russian-ukrainian war and opportunities export of its agricultural and metallurgical products), desynchronization of network flows (prohibition of supplying high-tech components to russia due to sanctions), etc. The purpose of lesions of the MS elements is usually destabilization or stop the operation of CHNS subsystems subordinate to them. In this regard, one of the main tasks of management system is evaluation of existing or potential threats and risks that can destabilize CHNS structure and its operation process. It is obvious that decisions and actions aimed at their implementation should be different before, during and after the lesion depending on its type [15]. Thus, "before" the attack, the main efforts of MS are directed to evaluation of potential threats and development of effective protection means against them. At the same time, different types of lesions usually require different means of protection. Simultaneously, even systems of the same type may be protected differently from similar threats or require different types of protection (it is unlikely that the Rivne NPP needs protection from the threat of tsunami, like the Fukushima NPP). "During" the lesion, the main efforts of MS should be aimed at ensuring the maximum resistance to its spread (increase in the number of infected people, the epidemic becoming in pandemic or the capture of new territories of the country by enemy) and minimizing possible consequences. "After" the attack, the main task of MS is to objectively evaluate its consequences and develop effective strategies to overcome them for the fastest possible recovery of the system and its return to normal life activities.

The problem of CHNS vulnerability can be divided into two interrelated problems – the vulnerability of its base system and management system. The problem of BS vulnerability was discussed in detail in [12] and was divided into the problem of vulnerability to targeted attacks and the problem of critical load or sensitivity to small changes in the structure or operation process of network system. The main task of MS in the event of attack is to provide effective protection of the elements of BS's subsystems subordinate to it, and in the case of failure of this protection, to promptly restore the functioning of damaged BS components and minimize the consequences of this lesion. At the same time, the larger the damage zone of the base system, the higher the level of management must be involved in order to overcome the consequences of these lesions and to resist repeated attacks. The function of CHNS control nodes also includes anticipation of conditions of critical load and desynchronization of flow movement in subsystems subordinated to them, and in the event of such conditions, the fastest possible unloading and stabilization of flow movement in these subsystems [16]. However, attacks on MS nodes can be no less dangerous. Thus, defeating enemy command centers during hostilities is one of the main tasks of the Armed Forces of Ukraine (AFU). The problem of vulnerability of MS elements to targeted attacks can be divided into two interrelated components: attacks on the nodes of certain management layer, aimed at blocking intralayer control interactions, and attacks on the nodes of certain management layer with the aim of blocking the hierarchical network subsystems subordinate to them. At the same time, the higher the level of MS damage or the area of BS lesion, the potentially greater losses await the system. It is also necessary to take into account such feature of CHNS that the targets of attacks on it may be different (elements of base system or nodes controlling them), but the consequences of these attacks, in particular, the damaged areas, may be similar. Another feature of CHNS is the speed of reaction of BS subsystem to the blocking of the MS node controlling it, which significantly depends on the nature and operation laws of the original CHNS. Thus, lesion of separate parts of the human brain or the control unit of large automated technological complex almost instantly leads to disruption in the functioning of a part of body or production component subordinated to it. In other cases, the response may be delayed, and so much so that CHNS manages to restore the operation of control system without critical consequences for the operation process of base system. An example can be the real sudden death of top managers or owners of large international corporations (Steve Jobs), presidents (Olof Palme) or, as happened in Smolensk on April 10, 2010, the destruction of almost all leadership of the Republic of Poland [17]. These circumstances must also be taken into account during the analysis of system's vulnerability and the development of appropriate means of its protection. Among the reasons that can damage the components of CHNS management system should be singled out the conditions of critical loading of its nodes with information flows that are physically impossible to process in determined time intervals and can cause the effect of "analysis paralysis" [18] and unsynchronized arrival of data flows to certain node of managment system, which makes it impossible to make the right decision in a timely manner regarding the CHNS subsystem subordinate to it [19].

3. Strategies for the protection of complex hierarchical network systems

The first step in protecting the system from targeted attacks is the development of so-called scenarios of such attacks, that is, the most likely sequence of actions of intruder who will try with minimal means to cause as much damage as possible to the attacked system. The usefulness of such scenarios lies in the fact that, putting ourselves in the place of attacker, we can determine the most attractive attack targets from his point of view, i. e. those systems elements or components that require priority protection. Obviously, that the attractiveness of target is determined by its importance in the system according to certain features. We divide targeted attacks on CHNS into

1. sequential groups attacks, during which the most important elements of CHNS are gradually damaged, and the system is able to redistribute the functions of affected element among those elements that remained undamaged;
2. simultaneous group attacks, during which a group of the most important system elements is simultaneously damaged; examples of such attacks are each of the regular missile attacks on Ukrainian oil depots in May – June 2022, which led to fuel shortages in the country, and each of the air attacks on transformer stations of the Ukrainian power system during September 2022 – January 2023, which caused blackouts in all regions of the country; it is obvious that simultaneous group attacks, especially considering their consequences, are much more dangerous than sequential ones;
3. sequential-simultaneous attacks, during which the system after another simultaneous group attack cannot fully restore the functioning of all elements of the group damaged during the previous attack; examples of such attacks are the sequence of simultaneous missile attacks on the energy infrastructure of Ukraine mentioned above or phased sanctions against the financial and economic system and the defense and industrial complex of russia;
4. repeated group attacks, connected by the goal (the same group of system nodes) and the method of attack implementation, but not by the consequences, since the system has time to fully protect or restore its structure and operation process; examples of such lesions are hacker attacks on January 14 and February 14-16, 2022 on the more than 70 most important state, security, financial and social computer networks of Ukraine [20] or 17 missile attacks on Kyiv in May 2023.

It is clear that each type of attack requires the development of specific type of scenarios for its most likely implementation [21]. Thus, a typical scenario of sequential group attack involves the following steps:

1. Compile a list of system nodes in order of decreasing indicators of their importance in the system, determined according to a certain criterion.
2. Attack the first node from created list. If the goal of attack is achieved (a predetermined group of nodets is damaged), then finish the execution of scenario, otherwise go to the next step.
3. Since the system can redistribute the functions of node damaged in the previous step between those nodes that remained undamaged, the indicators of importance of CHNS elements may change. Therefore, proceed to step 1.

The simplest scenario of simultaneous group attack is obviously realized by attempt to simultaneously defeat a group of the most important according to defined criterion CHNS elements.

A typical scenario of sequential-simultaneous group attack involves the consecutive execution of following steps:

1. Compile a list of groups of nodes (subsystems) in order of decreasing indicators of their importance in the system, determined according to a certain criterion.

2. Attack the first group from created list. If the goal of attack is achieved (a predeterminated set of groups of elements is damaged), then finish the execution of scenario, otherwise go to the next step.
3. Since the system can redistribute the functions of group of nodes (subsystem) damaged in the previous step between those groups that remained undamaged, the indicators of importance of groups (subsystems) in CHNS may change. Therefore, proceed to step 1.

The simplest scenario of repeated group attacks is obviously realized by an attempt to defeat preselected and previously attacked CHNS subsystem.

From the above considered typical scenarios of targeted attacks of various types, it follows that in order to build the most effective scenarios, the problem of determining the importance indicators of elements and subsystems (both basic and management) arises at first [22]. We calculate these indicators on the basis of one or another CHNS model. At the same time, different models make it possible to determine indicators of importance, which for different elements establish their different priority in the system. Moreover, a similar situation can occur even when using one model. Thus, in TSM, the importance of network node is determined using the so-called centralities of various types (by degree, betweenness, closeness, eigenvalue, etc.) [23]. In total, more than 20 such centralities have been introduced [24]. D. Krakhard, using the example of sufficiently simple network, showed that the values of different centralities for the same node can differ significantly [25]. In particular, a node that is important for the network according to value of one centrality may be insignificant according to the value of another. We will show which indicators of elements and subsystems importance make it possible to determine the structural and flow models of CHNS.

4. Structural model of hierarchical network system

Let us M is the number of levels of the CHNS hierarchy, $G_m = (V_m, E_m)$ is the network of the m-th hierarchical level, in which V_m is the set of nodes G_m, E_m is the set of edges G_m, and N_m, L_m are the numbers of elements of the sets V_m and E_m, $m = \overline{1, M}$, respectively. The CHNS structure is fully described by the adjacency matrix

$$\mathbf{A} = \{\mathbf{A}^{mk}\}_{m,k=1}^{M}, \ \mathbf{A}^{mk} = \{a_{ij}^{mk}\}_{i=1,\ j=1}^{N_m\ \ N_k},$$

in which $a_{ij}^{mk} = 1$ if there is an edge between nodes n_i^m and n_j^k, and $a_{ij}^{mk} = 0$, $i = \overline{1, N_m}$, $j = \overline{1, N_k}$, $m, k = \overline{1, M}$, if there is no such edge. The dimensionality N of matrix $\mathbf{A}$ is determined by the ratio

$$N = \sum_{m=1}^{M} N_m .$$

The structure of adjacency matrix $\mathbf{A}$ of hierarchical network system with direct subordination is determined by its following features as a multilayer network:

1. Connections can exist between arbitrary network nodes of certain hierarchy level, regardless of their subordination, and loop connections are excluded. This means that blocks $\mathbf{A}^{mm}$, which describe the intralayer interactions in the m-th layer of CHNS, $m = \overline{1, M}$, are generally dense matrices with zero diagonal elements. The elements of matrices $\mathbf{A}^{m,m+1}$ determine the input connections of elements of (m+1)th layer that come to them from the control nodes of mth layer, and the elements of matrices $\mathbf{A}^{m+1,m}$ are the output (reverse) connections of elements of (m+1)th layer, which are sent from them to the control nodes of mth layer. That is, matrices $\mathbf{A}^{m,m+1}$ and $\mathbf{A}^{m+1,m}$ describe the interlayer interactions of mth layer of CHNS with the adjacent layer of a lower hierarchical level. Thus, the adjacency matrix $\mathbf{A}$ has a block threediagonal structure in which only the elements of blocks $\mathbf{A}^{mm}$, $\mathbf{A}^{m,m+1}$, $\mathbf{A}^{m+1,m}$, $m = \overline{1, M-1}$, and $\mathbf{A}^{MM}$ are nonzero, respectively.

2. The network G_m of m^{th} hierarchical layer is divided into N_{m-1} subnets $G_m^l = (V_m^l, E_m^l)$, the nodes of each of which are subordinate to l^{th} node of $(m–1)^{\text{th}}$ hierarchical layer, N_m^l is the number of nodes of the set V_m^l, $l = \overline{1, N_{m-1}}$, and

$$N_m = \sum_{l=1}^{N_{m-1}} N_l^m \,,\; m = \overline{1, M}\,.$$

Nodes of m^{th} hierarchical level are numbered sequentially by the sets V_m^l with increasing value of l, $l = \overline{1, N_{m-1}}$. Then the matrices $\mathbf{A}^{mm}$, $\mathbf{A}^{m,m+1}$, $\mathbf{A}^{m+1,m}$, $m = \overline{1, M-1}$, and $\mathbf{A}^{MM}$ also have a block structure. At the same time, the diagonal blocks $\mathbf{A}_{ll}^{mm}$ of matrix $\mathbf{A}^{mm}$, which describe the internal interactions in subsystem that includes the subnets G_m^l, are dense matrices with zero diagonal elements, and the off-diagonal blocks $\mathbf{A}_{lk}^{mm}$ of matrix $\mathbf{A}^{mm}$ describe the interactions between nodes of subnet G_m^l and other subnets of m^{th} system layer of CHNS, $l, k = \overline{1, N_{m-1}}$. With the above described method of numbering the layer nodes, matrices $\mathbf{A}^{m,m+1}$ and $\mathbf{A}^{m+1,m}$, $m = \overline{1, M-1}$, have a diagonal structure, the elements of which reflect descending and ascending interlayer connections between the controlling and controlled nodes of m^{th} and $(m+1)^{\text{th}}$ layers, respectively. It is obvious that the interlayer communications in CHNS of direct subordination are two-way, as they involve both the transmission of control messages and the return response – reaction to them. The described method of forming the adjacency matrix **A** allows us to calculate the most of local and global structural characteristics of the elements and components of CHNS in the simplest way, and therefore to determine their importance in the structure of intra- and interlevel interactions.

Intralayer local characteristics of nodes of each layer (input and output degrees of node, its clustering coefficient, etc.), as well as its global characteristics (centralities of various types) and layers (size, density, diameter, general clustering coefficients, average length of shortest path, etc.) are determined as for ordinary complex networks [26]. The interlayer input and output degrees of nodes of each layer in CHNS, which simultaneously determine their interlayer centrality by degree, are calculated:

1) for the node of first hierarchical level of CHNS

$$d_1^{1,\,in} = d_1^{1,\,out} = N_2\,,$$

2) for nodes of CHNS intermediate layers

$$d_l^{m,\,in} = d_l^{m,\,out} = 1 + N_{m+1}^l\,,\; l = \overline{1, N_m}\,,\; m = \overline{2(1)(M-1)}\,,$$

3) for nodes of CHNS base system

$$d_l^{M,\,in} = d_l^{M,\,out} = 1\,,\; l = \overline{1, N_M}\,.$$

By calculating the ratio of number of shortest paths that pass through a certain MS node to all shortest paths containing in MS, we determine the betweenness centrality of this node in CHNS control structure. In addition, as indicators of the importance of MS node, we can choose the specific weight in structure of base system the subsystem of BS subordinate to it or the specific weight of hierarchical network subsystem of CHNS controlled by this node. As indicator of importance, we can also use the weighted aggregate value of the above node characteristics, in which the weight of each characteristic is determined by specialists in relevant subject area.

It is obvious that the ability to counter various challenges and threats that CHNS faces directly depends on the quality of its management system. The optimal CHNS management structure is characterized by such features as a small number of levels of MS hierarchy and a small number of management units (nodes) at each hierarchical level [3, 27]. The speed of reaction to changes in the basic system directly depends on these signs, which is especially important in crisis situations for the system. In particular, the quantitative characteristics of MS structure must satisfy the following conditions:

1) the total number of nodes of networks G_m, $m=\overline{1, M-1}$, (for example, management personnel) should not exceed the number of nodes of the base system, i.e.

$$\sum_{m=1}^{M-1} N_m \Big/ N_M < 1,$$

2) the number of levels of CHNS management system hierarchy should not exceed the number of subsystems of the base system, i.e.

$$M \big/ N_M^{M-1} \le 1.$$

Another sign of the effectiveness of CHNS management system is the level of interaction between management units, which should increase during the transition to a higher hierarchical layer, i.e.

$$N_m / L_m \ge N_{m+1} / L_{m+1}, \ m = \overline{2(1)(M-1)}.$$

Failure to comply with these requirements can become a negative internal factor that reduces the effectiveness of management system and its ability to quickly counter targeted attacks on the system and overcome the consequences of such attacks. The optimality of MS is also characterized by functional indicators, among which the qualification of management staff, motivation of personnel, promptness of reaction to various internal and external influences, effective organization of the movement of information flows (speed and synchronization of receipt for timely management decisions), the quality of information (usefulness, completeness, minimal sufficiency and so on), helping to achieve the goal of system's existence, etc.

An additional advantage of CHNS structural model is the possibility of its application to determine the system losses during and after a targeted attack on it. Thus, the ratio of structural model dimensionality during (after) attack to the dimension *N* of matrix **A** before the attack determines the specific weight of nodes damaged during (after) attack in the initial CHNS structure. Taking into account the above indicators of importance of CHNS nodes makes it possible to calculate these losses even more accurately. The ratio of non-zero elements number of CHNS structural model during (after) attack to the number of non-zero elements of matrix **A** before attack determines the specific weight of edges damaged during (after) attack in the initial CHNS structure. Similarly, the loss level can be determined not only for CHNS at a whole, but also for each of its hierarchical levels or separate hierarchical network subsystems of different hierarchical levels.

5. Flow model of hierarchical network system

The CHNS flow model is described by the flow adjacency matrix

$$\mathbf{V}(t) = \{\mathbf{V}^{mk}(t)\}_{m,k=1}^{M}, \quad \mathbf{V}^{mk}(t) = \{V_{ij}^{mk}(t)\}_{i=1,\ j=1}^{N_m\ \ N_k}, \ m,k=\overline{1,M},$$

structure of which coincides with the structure of adjacency matrix **A**. The main feature of blocks of matrix $\mathbf{V}(t)$ is the diversity of flows in the basic system and management system of CHNS, and therefore the different meaning load of values of their elements, which for matrix $\mathbf{V}(t)$ we define as follows:

1) elements of block $\mathbf{V}^{MM}(t)$, which describe the operation process of CHNS basic system, are equal to the relative volumes of basic flows that passed during the time interval $[t-T, t]$, $t \ge T$, through edges (n_i^M, n_j^M), namely

$$V_{ij}^{MM}(t) = \tilde{V}_{ij}^{MM}(t) \Big/ \max_{k,l=\overline{1,N_M}} \tilde{V}_{kl}^{MM}(t), \tag{1}$$

where $\tilde{V}_{ij}^{MM}(t)$ is the volume of basic flows that passed through the edge (n_i^M, n_j^M) during the time interval $[t-T, t]$, $t \ge T$, the values $\tilde{V}_{ij}^{MM}(t)$, $i,j=\overline{1,N_M}$, are determined on the basis of empirical data, which are currently quite simple to obtain for almost all man-made systems [28];

2) similar to formula (1), the elements of blocks $\mathbf{V}^{mm}(t)$, $\mathbf{V}^{m,m+1}(t)$ and $\mathbf{V}^{m+1,m}(t)$, $m=\overline{1,M-1}$, in the simplest case, are equal to the relative volumes of information flows that passed during the time interval $[t-T,t]$, $t \geq T$, through intra- and interlayer edges of the management part of CHNS.

Such way of forming the matrix $\mathbf{V}(t)$, $t \geq T$, the elements of which are dimensionless values which belong to the interval [0, 1], makes it possible to correlate the values of all flows that move through the CHNS edges, regardless of their type.

The input and output intralayer flow degrees of arbitrary node of *m*th hierarchical level are determined from the matrices $\mathbf{V}^{mm}(t)$, $m=\overline{1,M}$, by summing the values of corresponding column or row elements of these matrices, i.e. equal to the sum of input and output flows entering to (leaving from) this node from (to) adjacent nodes of this hierarchical level during the time interval $[t-T,t]$, $t \geq T$.

The input and output interlayer flow degrees of arbitrary node of the *m*th hierarchical level are equal to the total volumes of information flows that arrived at it or were sent from it to corresponding control and controlled nodes in the adjacent CHNS layers during the time interval $[t-T,t]$, $t \geq T$, and are determined as follows. Let us n_l^{m-1}, $l=\overline{1,N_{m-1}}$, is a some node of the (*m*–1)th hierarchical level and G_m^l is a subnet of *m*th level subordinate to it. Nodes n_p^m of subnet G_m^l managed by node n_l^{m-1} will be numbered as follows:

$$p=\sum_{i=1}^{l-1} N_m^i + j\,,\ \ j=\overline{1,N_m^l}$$

where N_m^l is the number of subnet G_m^l, $l=\overline{1,N_{m-1}}$, $m=\overline{2(1)(M-1)}$.

Let us G_{m+1}^p is a subnetwork of (*m*+1)th hierarchical level subordinate to node n_p^m, whose nodes n_k^{m+1} will be numbered as follows:

$$k=\sum_{i=1}^{p-1} N_{m+1}^i + j\,,\ \ j=\overline{1,N_{m+1}^p}\,,$$

where N_{m+1}^l is a number of nodes of subnet G_{m+1}^l, $l=\overline{1,\sum_{i=1}^{p} N_m^i}$, $p=\overline{1,N_{m-1}}$, $m=\overline{2(1)(M-1)}$. Then input $g_{n_p^m}^{in}(t)$ and output $g_{n_p^m}^{out}(t)$ interlayer flow degrees of the node n_p^m are calculated as follows:

1) for the node of first hierarchical level of CHNS

$$g_{n_1^1}^{in}(t)=\sum_{i=1}^{N_2} V_{i1}^{21}(t)\,,\ \ g_{n_1^1}^{out}(t)=\sum_{i=1}^{N_2} V_{1i}^{12}(t)\,;$$

2) for nodes of CHNS intermediate layers

$$g_{n_p^m}^{in}(t)=V_{pp}^{m,m-1}(t)+\sum_{i=1}^{N_{m+1}} V_{ii}^{m+1,m}(t)\,,\ \ g_{n_p^m}^{out}(t)=V_{pp}^{m-1,m}(t)+\sum_{i=1}^{N_{m+1}} V_{ii}^{m,m+1}(t)\,,\ \ m=\overline{2(1)(M-1)}\,;$$

3) for nodes of CHNS base system

$$g_{n_p^M}^{in}(t)=V_{pp}^{M,M-1}(t)\,,\ \ g_{n_p^M}^{out}(t)=V_{pp}^{M,M-1}(t)\,,\ \ t \geq T\,.$$

On the base of matrix $\mathbf{V}(t)$ we can determine such global characteristics of BS and MS nodes as input and output parameters of their influence on the system [29]. Namely, the input (output) force of influence of a node – the final receiver (generator) of flows is equal to the total volumes of flows that were received (generated) in this node during the period $[t-T,t]$; the input (output) area of influence of a node – the final receiver (generator) of flows is considered the set of CHNS nodes, in which the flows directed to (from) it were generated (finally received) during the period $[t-T,t]$, $t \geq T$; the input (output) influence power of a node – the final receiver (generator) of flows is equal to the number of elements of the input (output) influence areas of this node, respectively. Another type of global flow characteristics of a node in CHNS are its betweenness parameters [29], namely, the measure of betweenness, which is equal to the volume of transit flows passing through this node during the period $[t-T,t]$, $t \ge T$, the betweenness area, which includes all generator nodes and nodes – receivers of CHNS that direct (receive) the flows transiting through this node, and the power of betweenness, which is equal to the number of nodes in the betweenness area of this node. In the article [29] was shown that the total (as sum of input and output) flow degree (local characteristic) of a node is equal to the sum of its input and output flow forces and the measure of betweenness (global characteristics) of this node in the hierarchical network system. Therefore, it is most convenient to build scenarios of targeted attacks, using precisely the flow degrees of CHNS nodes as functional indicators of importance.

The values of parameters of input and output interlayer influence and betweenness for arbitrary node n_l^m of the mth hierarchical level, $m=\overline{1,M}$, extends on the structures that include the shortest path to control node of the first level of CHNS hierarchy and $(M-m+1)$-layer hierarchical subnet, $m=\overline{2(1)(M-1)}$, subordinate to this node. The final formulas for calculating the values of these parameters, which we do not present here due to their cumbersomeness, can be easily obtained similarly [29].

An additional advantage of CHNS flow model is the possibility of its application to determine the functional system losses during and after a targeted attack on it. Thus, the ratio of sum of elements of the matrix $\mathbf{V}(t)$ during (after) attack to the sum of elements of this matrix before attack determines the relative decrease in the volume of flows that move through the system during (after) attack. Similarly, the level of functional losses can be determined not only for CHNS at a whole, but also for each of its hierarchical levels or separate hierarchical network subsystems. Thus, the comparison of CHNS structural and flow models makes it possible to draw up a sufficiently objective quantitative picture of the level of damage to the structure and operation process of the system or its separate subsystems as the attack result.

6. Structural and flow characteristics of the subsystems of hierarchical network system

The indicators of structural and functional importance of CHNS nodes calculated in the previous sections make it possible to build effective scenarios of sequential group attacks on the system. However, for organization of simultaneous or repeated group attacks, it is necessary to determine the most important subsystems of CHNS, the lesion of which can lead to significantly greater losses than sequential ones. The structural characteristics of CHNS subsystems formed in certain layer are determined by the specific weight of their elements in the set of all elements of the layer. Also, analogs of the concepts of input and output intra- and interlayer structural degrees can be introduced for subsystems of a layer, as the number of input and output connections of this subsystem with adjacent subsystems of this layer. The structural characteristic of hierarchical network subsystem of CHNS is the specific weight of its elements in the set of all system elements. The so-called *k*-cores i.e. hierarchical network structures, the degree of each node of which is at least *k* [30], can be also singled out as the most important components of CHNS from a structural point of view. The adjacency matrix $\mathbf{A}_k$ of *k*-core, which fully describes its structure, is obtained from the matrix $\mathbf{A}$ by removing rows and columns whose sum of elements is less than the value *k*. The structural characteristic of CHNS's *k*-core is the specific weight of its elements in the set of all system elements.

In previous section, the mth layer-system of CHNS was divided into a set of subsystems G_m^l subordinate to nodes n_l^{m-1} of $(m–1)$th hierarchical level, $l=\overline{1,N_{m-1}}$, $m=\overline{2(1)M}$, respectively. The importance of subsystems G_m^l in operation process of the mth layer is determined by the specific weight $\sigma_{G_m^l}^{int}(t)$ of internal flows of subsystem G_m^l compared to the total volumes of flows in mth layer-system, that passed in it during the time period $[t-T,t]$, $t \ge T$, which is calculated by formula

$$\sigma_{G_m^l}^{int}(t) = s(\mathbf{V}_{ll}^{mm}(t)) \big/ s(\mathbf{V}^{mm}(t)),$$

where $\mathbf{V}_{ll}^{mm}(t)$ is the lth diagonal block of matrix $\mathbf{V}^{mm}(t)$ with dimension N_m^l, $l=\overline{1,N_{m-1}}$, $m=\overline{2(1)M}$, $t \geq T$, and parameter $s(\mathbf{F})$ is equal to sum of all elements of matrix **F**. Parameters $\sigma_{G_m^l}^{int}(t)$ determine not only the importance of subsystem G_m^l in operation process of mth layer-system, but also indirectly the importance of node n_l^{m-1} in the set of nodes of (m–1)th layer-system, as the control node of subsystem G_m^l in the sense of effective organization of its work and bilateral and general intersystem interactions with other subsystems of mth hierarchical level of CHNS. Obviously, the subsystems of mth layer with the largest values of $\sigma_{G_m^l}^{int}(t)$, $l=\overline{1,N_{m-1}}$, $t \geq T$, are the most attractive attack targets among subsystems of mth layer of CHNS, $m=\overline{2(1)M}$.

Consider the hierarchical network subsystem $G_{n_l^{m-1}}$ of CHNS, controlled by node n_l^{m-1} of (m–1)th hierarchical level, $l=\overline{1,N_{m-1}}$, $2 \leq m \leq M-1$. The flow model $\mathbf{V}_{G_{n_l^{m-1}}}(t)$ of subsystem $G_{n_l^{m-1}}$ is constructed similarly to the one described in section 5. The importance of subsystem $G_{n_l^{m-1}}$ and its control node n_l^{m-1} in operation process of CHNS are determined by two parameters:

1) specific volumes of flows $\vartheta_l^{m-1}(t)$ in corresponding subsystem of the base system, which pass through it during the time interval $[t-T,t]$, $t \geq T$, i.e.

$$\vartheta_l^{m-1}(t) = s(\mathbf{V}_{G_{n_l^{m-1}}}^{MM}(t)) \Big/ s(\mathbf{V}^{MM}(t)),$$

where $\mathbf{V}_{G_{n_l^{m-1}}}^{MM}(t)$ is the flow adjacency matrix of subsystem of the base system controlled by node n_l^{m-1}, $l=\overline{1,N_{m-1}}$, $m=\overline{2(1)M}$, $t \geq T$;

2) specific volumes of flows $\theta_l^{m-1}(t)$ in subsystem $G_{n_l^{m-1}}$, which pass through it compared to all subsystems controlled by nodes of (m–1)th hierarchical level during the time period $[t-T,t]$, i.e.

$$\theta_l^{m-1}(t) = s(\mathbf{V}_{G_{n_l^{m-1}}}(t)) \Bigg/ \sum_{k=1}^{N_{m-1}} s(\mathbf{V}_{G_{n_k^{m-1}}}(t)),\ l=\overline{1,N_{m-1}},\ m=\overline{2(1)M},\ t \geq T.$$

It is clear that subsystems $G_{n_l^{m-1}}$ with the largest values of $\vartheta_l^{m-1}(t)$ and/or $\theta_l^{m-1}(t)$, $l=\overline{1,N_{m-1}}$, $m=\overline{2(1)M}$, $t \geq T$, are the most attractive attack targets among hierarchical network subsystems controlled by nodes of (m–1)th CHNS layer, $m=\overline{1,M-1}$.

Another class of the functionally most important subsystems of the initial CHNS is its flow λ-cores, which are determined from the matrix $\mathbf{V}(t)$ by the ratio

$$\mathbf{V}_\lambda(t) = \{V_{\lambda,ij}^{mk}(t)\}_{i,j=1}^{N^M}{}_{m,k=1}^{M},\quad V_{\lambda,ij}^{mk}(t) = \begin{cases} V_{ij}^{mk}(t), \text{if } V_{ij}^{mk}(t) \geq \lambda \\ 0, \text{if } V_{ij}^{mk}(t) < \lambda \end{cases},\ \lambda \in [0,1], t \geq T, i,j=\overline{1,N}, m,k=\overline{1,M}.$$

It is obvious that λ-cores of hierarchical layers of initial CHNS (Fig. 2a) are sequentially quasi-similar (Fig. 2b), that is, the nodes of flow λ-core of mth hierarchical level are subordinate to the nodes of λ-core of (m–1)th level, $m=\overline{2(1)M}$. In other words, λ-core of CHNS is a complex hierarchical network system that combines the most important elements of CHNS from a functional point of view i.e., it is the most attractive target of simultaneous group attack.

Let us denote by $N_\lambda(t)$ the dimension of matrix $\mathbf{V}_\lambda(t)$ with removed zero rows and columns, which is equal to the dimension of flow λ-core of CHNS (the number of λ-core nodes), and by

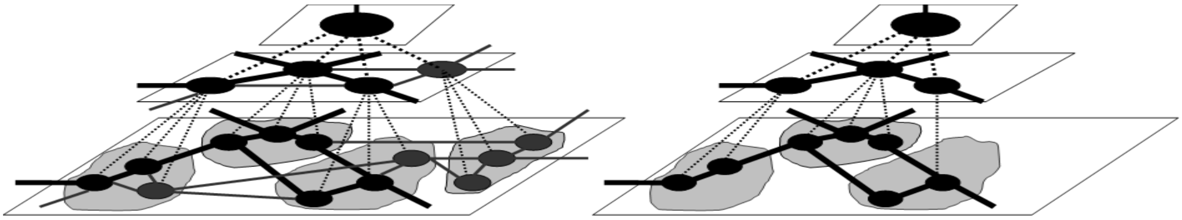
$L_\lambda(t)$ the number of matrix $\mathbf{V}_\lambda(t)$ non-zero elements (the number of λ-core edges). Then parameters

$$\eta_\lambda(t) = N_\lambda(t) \big/ N$$

and

$$\mu_\lambda(t) = L_\lambda(t) \big/ L\ ,$$

where L is the number of non-zero elements of matrix $\mathbf{V}(t)$, $t \geq T$, determine the dimensional and connection specific weights of λ-core in CHNS structure.



a) b)

Figure 2: Fragments of structures of hierarchical network system (a) and its flow λ-core (b)

To determine the functional specific weight of λ-core in CHNS, we will use parameter $\sigma_\lambda(t)$, which is equal to the ratio of volumes of flows that pass through λ-core to the volumes of flows that pass through hierarchical network system as a whole for the period $[t-T,t]$, namely

$$\sigma_\lambda(t) = s(\mathbf{V}_\lambda(t)) \big/ s(\mathbf{V}(t))\ ,\ \ t \geq T\ .$$

It is obvious that parameters $\eta_\lambda(t)$, $\mu_\lambda(t)$ and $\sigma_\lambda(t)$ make it possible to determine the level of damage of structure and process of CHNS functioning as a result of simultaneous group targeted attack on its λ-core.

The use of flow λ-cores compared to structural *k*-cores is much more effective when building scenarios of sequential, simultaneous or repeated group attacks, both from a point of view of possible damage to the most functionally important elements of CHNS, and for the purpose of optimizing these scenarios in terms of the number of attack objects. Let us consider the next variant of targeted attack on the basis system of real hierarchical network system, namely, the railway transport system (RTS) of western region of Ukraine. In Fig. 3a is shown the structure of this basic system, and in Fig. 3b – the same structure, but in the form of weighted network, which schematically displays the volumes of freight flows that passed through its edges during 2020 [31] (the thickness of lines is proportional to the weights – volumes of flows). Note that this network contains 354 nodes in total, but in Fig. 3a-b only 29 nodes and 62 edges are reflected (transit nodes with structural degree 2 are not displayed). In Fig. 3c is contained the *4*-core of RTS, which includes 12 nodes and 35 edges, and in Fig. 3d is its flows 0,8-core, which contains 4 nodes and 12 edges (an edge is considered a line connecting two nodes with degree greater than 2). It is obvious that the flow core represents a functionally more important subsystem of RTS and the target of group attack on it is a much smaller number of nodes than on the 4-core of corresponding structure. That is, the goal of attack can be achieved with significantly less (three times from the point of view of nodes number) efforts.

Another confirmation of the greater effectiveness of functional importance indicators use when building targeted attack scenarios is reflected in Fig. 3b nodes A, B and C. From a structural point of view, node C with a structural degree 5 and even node B with a structural degree 4 are more attractive targets than node A with a structural degree 3 (in the list of nodes whose importance is determined by their degree, node C may occupy the 3rd and node B – 6th place out of 354, respectively). At the same time, much larger volumes of flows pass through node A than through nodes B and C, and stopping its operation will cause much more damage to the system. The issue of determining the level of real losses suffered by the system as a result of attack on certain of its subsystem is also important. In addition to the directly damaged elements of this subsystem, all CHNS nodes connected to them are usually affected to one degree or another. From a structural point of view, such nodes are the set of all system nodes adjacent to damaged in the subsystem. From a functional point of view, all nodes that belong to the union of areas of input and output influence, as well as betweenness of damaged CHNS subsystem (which are determined in the same way as for separate its nodes [29]), can be considered affected. This is explained by the fact that nodes – receivers and generators of flows need to be replaced in some way, and for transit nodes, alternative paths of flows movement must be found.

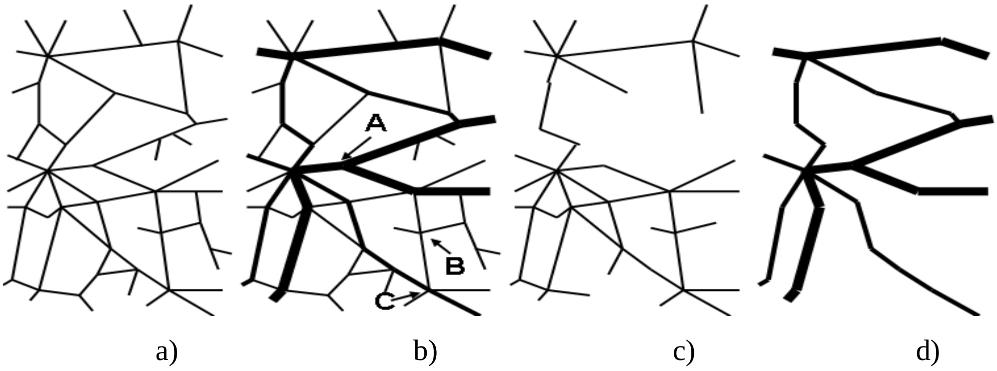


Figure 3: Examples of structure (a), operation process (b), *4*-core (c), and flow 0,8-core (d) of the railway transport system of western region of Ukraine

All this has a specific financial dimension, which can be used to calculate the level of losses that the system experiences. Indeed, as a result of sanctions against russia due to its aggression in Ukraine, many of the world's leading companies have lost their sales markets (final receivers of flows). Many of them, at least temporarily, had serious problems with the supply of energy resources and raw materials (generators of flows). The movement of transit flows through the russian territory was also significantly limited. Ukraine faced similar circumstances, but as a result of hostilities on its territory (restriction of production, export and import of various products, stoppage of transit flows, etc).

7. Analysis and overcoming the consequences of system lesions

A mandatory prerequisite for making the right decision concerning further actions regarding CHNS or its separate elements and subsystems is the availability of information sufficient for analysis of the system state, process of its functioning and interaction with other systems (including all negative influences from their side). For operational analysis of information, it must be appropriately structured and presented in a form that is understandable for the decision-maker. It is obvious that the state and behavior both the separate elements and subsystems and the system as a whole before, during and after targeted attack can differ significantly. Moreover, the behavior of even systems of the same type during these periods can also be different and require various actions to return to their normal life activities (people of the same age can tolerate Covid-19 differently, various cities are differently prepared for earthquakes, and various countries – before a military invasion and so on). To solve this problem, in article [5] were developed the principles of forming an *information model* (IM) and a *model of complex evaluation* (MCE) of the state, effectiveness of operation and interaction of CHNS with the surrounding system environment in noncrisis situations. However, these models can be used to organize effective protection of the system against targeted attacks and to overcome the consequences of such attacks as soon as possible. The CHNS information model is a dynamic data structure that fully describes the behavior of all elements of the system and its subsystems. The main problem that arises when working with IM is extremely large volumes of data, which is physically impossible to process in "manual mode" in practically acceptable time intervals. To solve this problem, MCE is used, the main components of which are

1) a *model of interactive evaluation*, which, based on continuous monitoring of system elements behavior, allows us to evaluate the current state of all CHNS components, for example, destruction and casualties during a sudden missile attack; the results of interactive evaluation contribute to

adoption the operational decisions and implementation of actions directed to overcoming the consequences of such lesions as soon as possible and returning the system to normal life activity;
2) a *model of regular evaluation* of CHNS elements behavior during a certain period of time, for example, after series of sequential-simultaneous or repeated attacks on the system or after another wave of Covid-19; analysis of regular evaluation results makes it possible to prioritize the restoration of system objects damaged by such lesions and redistribute the available means of its protection to minimize the negative consequences;
3) a *model of regressive evaluation* of CHNS elements behavior over a sufficiently long period of time, which allows us to detect lesions in its structure and operation process, which were intentionally or unintentionally neglected during previous interactive and regular system evaluations; after the end of russian-ukrainian war, the regressive evaluation of events that took place during it will make it possible to identify the shortcomings of country's defense system and eliminate them, strengthening Ukraine's defense capabilities.

At the same time, the more objective, complete and versatile is information about the CHNS and formed on its basis evaluations about the system state, the greater is the hope for making the right decisions as a result of analysis of these data and actions, directed on the fastest possible restoration of CHNS and its return to normal life activities. Therefore, both for information model and for all evaluation models, structures of priority (elements and subsystems) and fullness (data about the system elements) are created, which allow us to make a representation about objectivity and validity of conclusions formed on the basis of data contained in these models. The events of recent years testify the importance of objective versatile evaluation of system state and its readiness to overcome various types of threats. The overestimation of capabilities of the health care systems of even the most developed countries has led to the late creation of vaccines against Covid-19 and multimillions of victims among the world's population. The underestimation of Ukraine's defense capabilities and overestimation of military power of russian army caused the late supply of weapons and prolongation of russian-ukrainian war.

In all MCE models listed above, the methods of local, prognostic, and aggregated refined point evaluation are used to analyze the behavior of CHNS elements and subsystems, which allow us not only to draw more accurate conclusions, but also to at least partially identify the causes of identified deficiencies [32]. It is obvious that objective local evaluationss of CHNS elements behavior are one of the most important prerequisites for the formation of well-founded generalized conclusions about the state and operation process of subsystems of all hierarchical levels. Simultaneously, from the point of view of decision-making support, aggregation methods play a crucial role in the process of forming such conclusions. We used different types of aggregation methods: "weakest" element, linear, weighed linear, and nonlinear aggregation, as well as based on them hybrid aggregation procedures [32]. The practice of forming generalized conclusions about the state and operation process of real complex network systems (biological, transport, industrial) different in origin and purpose has shown that various systems require the use of diverse methods of aggregation. Thus, method of "weakest" element is the best for evaluating the efficiency of conveyor, the speed of which is determined by the speed of operations of the "slowest" worker or device. However, this method is completely unsuitable for evaluating, for example, the average performance of students in a class. Here, it is more appropriate to use the methods of linear or nonlinear aggregation, which, at the same time, are not suitable for evaluation the combat capability of military unit in which both recruits and experienced fighters can serve. In this case, the weighted linear aggregation method is used. Moreover, within one CHNS, different subsystems or even elements may require the application of various aggregation procedures, that is, their hybridization within the evaluation framework of different components of the same system, in order to obtain an objective generalized conclusion about their state and operation process.

Analysis of information that comes from controlled system elements to the control node of higher hierarchical level and formation, on the basis of this information and appropriate methods of aggregation, the generalized conclusions about the state and operation efficiency of subsystem controlled by this node and presentation of these conclusions to the control node of the next hierarchical level is one of the main tasks of CHNS management system. On the basis of thus formed hierarchy of generalized conclusions, decisions are made that "go down the hierarchical ladder" to subsystems and elements of CHNS base system to ensure the system protection from targeted attacks and lesions of other types and to overcome the consequences of these lesions. It is clear that speeding up this process can play a decisive role in minimizing the losses that may be or have already been caused to the system. So far, we have developed time-optimal parallel algorithms for calculating aggregated evaluations, which are used in models of interactive and regular evaluation of the state and operation process of CHNS components of all hierarchical levels. These algorithms are intended for implementation on modern computer systems with shared (multicore computers) and distributed (clusters, hybrid architectures, high-performance computing environments) memory with a known (limited) amount of resources in advance [33].

8. Conclusions

Humanity constantly faces with many global challenges – wars, epidemics of dangerous infectious diseases, financial and economical crises, threat of famine, natural and man-made disasters, etc. Both targeted attacks and nontarget lesions of real large complex systems often share many common features (the spread of natural and computer viruses, traffic jams and *DDoS* attacks) and similar consequences (the destruction of cities and the loss of population due to hostilities and powerful earthquakes). Despite the predictability and repeatability of such events, their occurrence often causes the confusion of relevant management structures and their inability to respond in a timely manner to the threats that have arisen. Therefore, understanding the risks that can destroy structure and destabilize operation process of many real systems and organizing timely protection against them is one of the main tasks of CHNS management systems. In the article were analyzed strategies of such protection for various types of targeted attacks on the system and on the base of structural and flow models of complex hierarchical network system were determined the structural and functional indicators of importance of its elements and subsystems, which require the priority protection before or recovery during or after the lesions. It was shown that the structural and flow models of CHNS make it possible to quantitatively evaluate the level of losses caused to the system. Expanding the areas of application of information models and models of complex evaluation during and after targeted attacks allow us to organize effective countermeasures against the spread of lesions and optimize the decision-making process directed on restoring the system and returning it to normal life.

9. References

[1] O. Polishchuk, About group and system-wide lesions of complex network systems and intersystem interactions, arXiv: 2211.11207 (2022).

[2] J. Walker, M. Cooper, Genealogies of resilience: From systems ecology to the political economy of crisis adaptation, Security dialogue, 42 2 (2011) 143-160.

[3] M. D. Mesarovic, D. Macko, Y. Takahara, Theory of hierarchical, multilevel, systems. Elsevier, 2000.

[4] A. Bejan, Freedom and evolution: hierarchy in nature, society and science. Springer Nature, 2019.

[5] O. Polishchuk, M. Yadzhak, Network structures and systems: III. Hierarchies and networks, System Research and Information Technologies, 4 (2018) 82-95.

[6] A. Proletarsky et al, Decision support system to prevent crisis situations in the socio-political sphere, Cyber-Physical Systems: Industry 4.0 Challenges, (2020) 301-314.

[7] M. M. Danzigerhael et al, Vulnerability of interdependent networks and networks of networks, Interconnected networks, (2016) 79-99.

[8] C. Simone, F. R. Medda, A. Wilson, An interdependent multi-layer model: resilience of international networks, Networks and Spatial Economics, 15(2) (2015) 313-335.

[9] J. Johansson, Risk and vulnerability analysis of interdependent technical infrastructures: addressing socio-technical systems. Lund University, 2010.

[10] S. Boccaletti et al, The structure and dynamics of multilayer networks, Physics Reports, 544 1 (2014) 1-122.

[11] M. Berlingerio et al, Multidimensional networks: foundations of structural analysis, World Wide Web 16 (2013) 567–593.

[12] O. Polishchuk, Vulnerability of complex network structures and systems, Cybernetics and Systems Analysis 56 2 (2020) 312-321.

[13] R. Albert, H. Jeong, A.-L. Barab´asi, Error and attack tolerance of complex networks, Nature, 406 (2000) 378–382.

[14] M. Bellingeri, D. Cassi, S. Vincenzi, Efficiency of attack strategies on complex model and real-world networks, Physica A: Statistical Mechanics and its Applications, 414 (2014) 174-180.

[15] S. Wandelt et al, A comparative analysis of approaches to network-dismantling, Scientific Reports, 8 1 (2018) 13513.

[16] N. Pankratova, N. Nedashkovskaya, Estimation of sensitivity of the DS/AHP method while solving foresight problems with incomplete data, Scientific Research Publishing, 2013.

[17] All the President's Men: The story of the Smolensk Air Disaster and the death of Lech Kaczyński. URL: https://admiralcloudberg.medium.com/all-the-presidents-men-the-story-of-the-smolensk-air-disaster-and-the-death-of-lech-kaczyński-590a3977f.

[18] D. Bawden, L. Robinson, The dark side of information: overload, anxiety and other paradoxes and pathologies, Journal of information science, 35 2 (2008) 180-191.

[19] N. D. Pankratova, N. I. Nedashkovskaya, Evaluating multifactor risks under conceptual uncertainty, Cybernetics and Systems Analysis, 45 (2009) 223-231.

[20] Everything about the cyber attack on Ukraine on February 15: banks, the government and websites of law enforcement agencies were affected. URL: https://24tv.ua/use-pro-kiberataku-ukrayinu-15-lyutogo-postrazhdali-golovni-novini_n1868773.

[21] A. M. Piraveenan et al, Quantifying topological robustness of networks under sustained targeted attacks, Social Network Analysis and Mining, 3 (2013) 939-952.

[22] Q. Nguyen et al, Conditional attack strategy for real-world complex networks, Physica A: Statistical Mechanics and its Applications, 530 (2019) 12156.

[23] L. Glenn, Understanding the influence of all nodes in a network, Science Reports, 5 (2015) 8665.

[24] A. Saxena, S. Iyengar, Centrality measures in complex networks: A survey, arXiv: 2011.07190 (2020).

[25] D. Krackhardt, Assessing the political landscape: Structure, cognition, and power in organizations, Administrative Science Quarterly, 35 (2) (1990) 342–369.

[26] S. Boccaletti et al, Complex networks: Structure and dynamics, Physics reports, 424 (4) (2006) 175-308.

[27] C. Bull, J. A. Ordover, Market structure and optimal management organizations, The Rand Journal of Economics, (1987) 480-491.

[28] A.-L. Barabasi, The architecture of complexity, IEEE Control Systems Magazine, 27 4 (2007) 33-42.

[29] O. D. Polishchuk, M. S. Yadzhak, Network structures and systems: I. Flow characteristics of complex networks, System Research and Information Technologies, 2 (2018) 42-54.

[30] S. N. Dorogovtsev, A. V. Goltsev, J. F. F. Mendes, K-core organization of complex networks, Physical review letters, 96 4 (2006) 040601.

[31] The official website of the Lviv Railway. URL: https://lv.uz.gov.ua.

[32] D. O. Polishchuk, O. D. Polishchuk, M. S. Yadzhak, Complex deterministic evaluation of complex hierarchically-network systems. III. Aggregated evaluation, System Research and Information Technologies 1 (2015) 21-31.

[33] O. D. Polishchuk, M. S. Yadzhak, Network structures and systems: IV. Parallel processing of continuous monitoring results, System Research and Information Technologies, 2 (2019) 105-114.