On the Vulnerability and Protection Strategies of Complex Network Systems and Intersystem Interactions

Olexandr Polishchuk[1] and Mykhailo Yadzhak[1,2]

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

Abstract

The problems of protecting complex network systems (NS) and intersystem interactions in multilayer network systems (MLNS) from heterogeneous internal and external negative influences are considered. Among such influences, targeted attacks on real complex systems and their non-target lesions of various nature are primarily singled out. On the basis of structural and flow models of NS and MLNS, sequential and simultaneous local, group and system-wide lesions of the structure and operation process of complex network systems and intersystem interactions are considered. The existing structural and functional scenarios of consecutive attacks on the most important components of the system and the need to neutralize the sources of such attacks as one of the means of system protection are analyzed. The peculiarities of application of such scenarios for the protection of NS and MLNS from system-wide non-target lesions are considered. Approaches to evaluation and overcoming the consequences of negative impacts on the structure and operation process of complex network systems and intersystem interactions are proposed.

Keywords

Complex network, network system, intersystem interactions, multilayer network system, vulnerability, targeted attack, non-target lesion, information model, evaluation model

1. Introduction

Every natural or man-made system is vulnerable to many internal and external negative influences. The climate and state of the Earth's biosphere are deteriorating under the influence of industrial society, financial crises and armed conflicts negatively affect the economy and social attitudes of population, the spread of false information distorts the public opinion of citizens, terrorist or hacker attacks, natural or man-made disasters, epidemics of dangerous infectious diseases, computer viruses and so on create threats to the operation process of many real systems [1, 2]. In the theory of complex networks (CN), the main attention of researchers is focused on the study of random negative effects and targeted successive attacks on CN nodes [3, 4]. However, the system can be damaged by destabilizing the process of its functioning without direct injury the network nodes and edges. Negative impacts can be not only sequential, but also simultaneous and affect at once on certain sufficiently large system components or the system as a whole. Along with targeted attacks, the system can be negatively affected by other factors of a natural or artificial nature, which may be similar to such attacks in many ways, but have neither an obvious intruder nor a predetermined target of lesion. It is obvious that the most acute the problem of decision making support arises precisely in such crisis situations for the system. Each real NS interacts with many other systems [5]. The lesions of such NS can lead to destabilization of the functioning of all related systems. This was clearly shown by the spread of Covid-19 pandemic, which led to significant deterioration of financial and economic condition of many countries and the resulting social discontent of population, for which even the most developed countries of the world were unprepared.

International Scientific Symposium "Intelligent Solutions" (IntSol-2023), September 27-28, 2023, Kyiv-Uzhhorod, Ukraine
EMAIL: od_polishchuk@ukr.net (A. 1); yadzhak_ms@ukr.net (A. 2)
ORCID: 0000-0002-0054-7159 (A. 1); 0000-0001-6070-6142 (A. 2)

The consequences of russian-ukrainian war manifested themselves in the form of threat of global food, energy, financial and economic crisis and the possibility of turning into global military conflict.

Different types of lesions of any real complex NS require various, sometimes directly opposite actions aimed at its protection. Therefore, in order to ensure the system's resistance to different negative impacts, it is necessary to give answers to at least the following questions:

1) what negative internal and external influences can disrupt the structure and operation process of the system under study;

2) how to protect the system depending on the type of negative internal or external influence, and since any large complex system usually cannot protect all its elements, which of them must be protected first of all;

3) what are the consequences of a certain type of system lesion, despite all the protection measures in place, and how to evaluate and overcome them.

In this paper, we will try to give answers to these questions posed from the point of view of network modeling and informational technologies, and show how a clear understanding of possible ways of the system lesions and their features helps in the development of effective methods and means of decision making support for prevention, protection and overcoming the consequences of such lesions.

2. Targeted attacks and non-target lesions of complex network systems

Under internal negative influences we understand the lesions of the system caused by the sources that are part of it (corruption in the country, accidents at dangerous industries, etc.). External negative impacts are generated by sources outside the system (foreign hacker groups, military aggression, etc.). In this article, we consider two main types of internal and external negative influences – targeted attacks and non-target lesions of complex network systems and intersystem interactions. A distinctive feature of targeted attacks is their intentionality and artificial nature (terrorist attacks, military actions and economic sanctions, dissemination of false information, etc.). A peculiarity of this type of lesions is the presence of attack target aimed at causing the greatest possible material and/or moral damage to the attacked system, and an intruder who carries out this attack. In contrast to targeted attacks, non-target lesions can include various unintentional negative impacts of a natural or artificial nature, the occurrence and consequences of which we cannot predict in a timely manner (natural and man-made disasters, the spread of infectious diseases, traffic jams in large cities, etc.). By many signs, non-target lesions can be similar to targeted attacks (the spread of computer viruses, *DDoS*-attacks, etc.). Such impacts are often unpredictable and have neither a clear "criminal" nor a predetermined target. They can be quite large-scale and the losses caused to the system by such non-target lesions often exceed the consequences of mass targeted attacks. The difficulty of accurate classifying the type of lesion is often related to the uncertainty of its source, because deliberate forest fire and carelessly thrown butt or sabotage at the enterprise and the use of poor-quality equipment often lead to similar consequences. At the same time, similar causes (epidemics of SARS Cov-1 in 2002 in China, MERS in 2010 in the Middle East, and SARS Cov-2 in 2019 in Wuhan) can lead to different consequences. The multifactorial effects, presence of many common signs, mode of action and often subjective factors that are practically impossible to take into account or predict are another reasons for the complexity of classification of system lesions. It should also be taken into account that a negative influence from the subject's point of view can be a positive impact from the object's side (introduction of new technologies that replace outdated ones, sanctions against aggressor countries, etc.).

Lesions of the system can be expected (conditionally predictable) and unexpected. Thus, earthquakes in regions that are at the junction of tectonic plates (California, Chile, Japan), powerful hurricanes in the Caribbean and Southeast Asia, forest fires in eastern Australia and California, Ebola epidemics in Central Africa, etc. can be called expected. Unexpected ones include the global spread of AIDS and Covid-19 or the earthquake in Haiti with a magnitude of 7 on the Richter scale in 2010, which killed more than 200,000 people and left more than a million people homeless. At the same time, less than 1,000 people were killed in the 8.8-magnitude earthquake in Chile in the same year. Expectations due to the recurrence of earthquakes forced the government of this and other countries to be particularly careful about the requirements for strength of buildings and critical infrastructure

facilities and the efficiency of relevant emergency units. The death toll from the devastating 7.8-magnitude earthquake that occurred on February 6, 2023 in Turkey and Syria is more than 45,000 people. However, in the city of Erzin (Hatai province, 42,000 inhabitants), which is located near the epicenter of this earthquake, all houses survived and not a single resident was injured. The mayor of Erzin explained this by the fact that during construction in the city, all rules and regulations were followed and no illegal structures were allowed. This means that a system prepared to protect against a certain lesion will suffer significantly less loss than an unprepared system. However, preventive measures may not be sufficient to protect the system even for conditionally predictable lesions. Thus, after the generally unexpected Chernobyl disaster, the requirements for the safety of nuclear power plants were significantly strengthened for almost all nuclear power plants (NPPs) in the world. However, they did not take into account the possibility of flooding cooling devices due to tsunami, as happened in 2011 at the Fukushima NPP (Japan). This means that even systems that are considered as well protected may not be sufficiently protected.

Both targeted attacks and non-target lesions of the system can be local, group or system-wide both from the point of view of subject and the object of negative impact, sequential or simultaneous, spread both in space and in time, negatively affecting on all areas associated with the damaged components of NS. Thus, a terrorist group can take hostage a school (Beslan, russia), DDoS attacks are usually carried out from several sources on one or a few computer networks, industrial society negatively affects on the entire biosphere of the Earth, and the Covid-19 pandemic has spread to all countries of the world. In the paper [6] was shown that defeating only 1% of Internet nodes-domains with the largest degrees reduces its performance by half, and blocking 4% of such nodes divides it into unconnected components. In Ukraine, the number of state-owned banks in the country's banking system at the beginning of 2022 did not exceed 0.7%. At the same time, the share of their assets in this system was equal to 55.2%, and the share of deposits of individuals – 61.6% [7]. A successful attack on this small group of banks will lead to the biggest losses in financial system of the state. Mass *DDoS*-attacks on January 14 and February 14-16, 2022 on more than 70 of the most important state, security, financial and social computer networks of Ukraine [8] can be considered as attempt to damage the system of its public administration. This means that in order to critically destabilize or stop the operation of real NS, it is necessary to simultaneously block the functioning of certain group of nodes. Indeed, successive attacks on separate, even the most important nodes of network system, as proposed in the scenarios of targeted attacks developed so far [9, 10] often allow us to redistribute their functions among other nodes. However, countering a simultaneous successful attack on a group of the most important by certain criteria elements of the NS , and most importantly overcoming the consequences of such attack, is much more difficult. Both targeted attacks and non-target lesions can be centralized, when the negative impact spreads from one source, and decentralized, when the affected element itself becomes the source of such impact, that is, a local damage can gradually grow into a group or system-wide one.

The system lesions can spread at different speeds - from "almost instantaneous" (cascading phenomena in power grids) to those that last for decades (the impact of industrial and agricultural production on the Earth's climate). Infection with computer viruses takes a few seconds or minutes, the incubation period of infectious diseases is from several hours to several weeks, and the effect of economic sanctions is from several months to several years. It is obvious that the different speed of lesions require different speed of protection or countermeasures. Sometimes, due to many objective and subjective reasons, such means cannot be developed or used in a timely manner (Ebola or Covid-19 vaccines).

3. Lesions of the structure and operation process of complex network systems and intersystem interactions

Studying real network systems and intersystem interactions of various types, we actually investigate models of such systems and interactions (structural, functional, informational, mathematical, etc.) constructed on the basis of empirical and theoretical data. Identifying elements of the system that require priority protection, we determine their importance in one or another model,

based on those characteristics of elements that this model allows us to determine. Thus, the structural model of network system, which is usually represented in the form

$$G = (V, E),$$

where V is the set of nodes and E is the set of network edges connecting these nodes, is completely described by the adjacency matrix

$$\mathbf{A} = \{a_{ij}\}_{i,j=1}^{N},$$

in which the value a_{ij} =1, if there is an edge that connects the nodes n_i and n_j, and a_{ij} =0, $i, j = \overline{1, N}$, if there is no such edge, N is the number of network nodes. Based on this model, we can determine such structural indicators of the importance of nodes as degree, betweenness, closeness, eigenvalue centralities [11], etc.

In the theory of complex networks (TCN), the main attention of researchers is more focused on the study of random negative impacts and targeted attacks on the system structure. Much less attention is paid to the vulnerability of operation processes of complex network systems. Undoubtedly, lesions of structure have a negative effect on the process of system functioning, but malfunctions in its operation can also occur with an undamaged structure. The dynamics of complex networks in TCN is usually understood as a change in the composition of their nodes and the structure of interconnections [12]. At the same time, every real system is a dynamic entity even with an unchanged structure. These dynamics, which at least partially describe the process of system functioning, can be quantitatively reflected by the change in the volumes of flows moving through the network. This is naturally explained by the fact that in some cases ensuring the movement of flows is the main goal of the formation and functioning of such systems (transport, financial, trade, information, social NS, etc.), and in others it is a process that ensures their vital activity (movement of blood, lymph, neuroimpulses in the human body, etc.). Stopping the movement of flows can lead to significant destabilization or even the cessation of the system's existence [13].

In general, by a flow that passes through a network edge, we understand a certain positive function correlated to this edge. This function can reflect the density of the flow at each point of the edge or the volume of flow that is on the edge at the current moment of time $t \geq 0$, or the total volume of flows that have passed through the network edge up to the current moment for a certain period of time T>0, etc. Consider the case when the flows are continuously distributed by the network edges. Let us introduce the adjacency matrix $\mathbf{V}(t)$ of the network system, the structure of which is described by the matrix $\mathbf{A}$ [14]. The elements of matrix $\mathbf{V}(t)$ are determined by the volumes of flows that have passed through the edges of network for the period $[t-T, t]$ up to the current moment of time $t \geq T$, where T is a given time interval:

$$\mathbf{V}(t) = \{V_{ij}(t)\}_{i,j=1}^{N}, \quad V_{ij}(t) = \frac{\tilde{V}_{ij}(t)}{\max\limits_{m,l=\overline{1,N}} \{\tilde{V}_{ml}(t)\}},$$

where

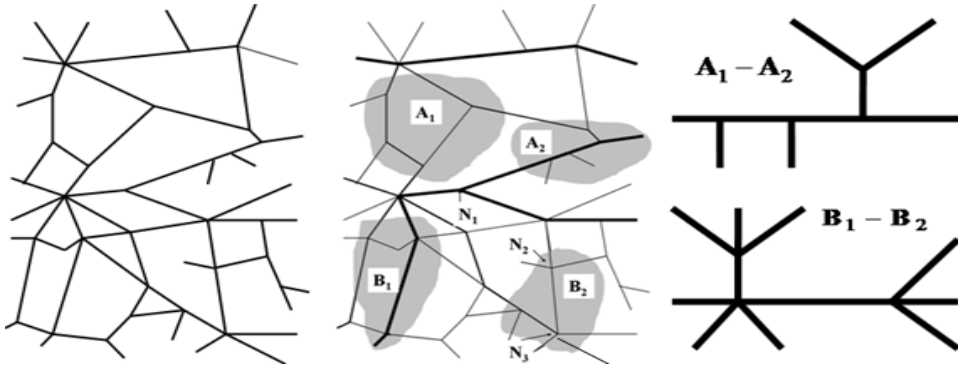
$$\tilde{V}_{ij}(t) = \int_{t-T}^{t} v_{ij}(\tau) d\tau, \quad t \geq T > 0;$$

$$v_{ij}(t) = \int_{(n_i, n_j)} \rho_{ij}(t, \mathbf{x}) dl, \quad t > 0; \ \boldsymbol{\rho}(t, x) = \{\rho_{ij}(t, \mathbf{x})\}_{i,j=1}^{N},$$

and $\rho_{ij}(t, \mathbf{x})$ is the density of the flow at each point of the edge (n_i, n_j) at the current moment of time t, $\mathbf{x} \in (n_i, n_j) \subset R^m$, $m = 2, 3, \ldots$, $i, j = \overline{1, N}$, $t \geq T$. The elements of NS flow adjacency matrix $\mathbf{V}(t)$ are determined on the basis of empirical data about the movement of flows that passed through its edges. Currently, with the help of modern information and communications technologies (ICT) means, such data are quite easy to obtain for many natural and the vast majority of man-made systems (transport, economic, financial, informational, etc.) [15]. On the basis of this model, we can determine such indicators of the functional importance of NS elements, as parameters of the influence of its

nodes, which are the global flow analogue of structural degree centrality and determine the importance of a node in the system as a generator or receiver of flows, and parameters of the flow betweenness of system elements, which are the functional analogue of the structural betweenness centrality and determine the node importance in the NS as a transitor of flows [13], etc.

Greater adequacy of functional indicators of elements' importance compared to its structural centralities follows from the next example. In fig. 1a shows a binary network that describes the structure of a fragment of only one layer of the general transport system of Ukraine, namely the railway transport system (RTS) of its western region. In fig. 1b shows a weighted network, which, based on the values of the corresponding flow adjacency matrix fixed at a certain point in time, describes the operation process of this part of the RTS with a schematic representation of the volumes of cargo flows that passed through the edges of this network during 2020 (the thickness of lines is proportional to the weights – flow volumes). It is obvious that from a functional point of view, node $\mathbf{N_1}$ with degree 3 is more important in this system than nodes $\mathbf{N_2}$ and $\mathbf{N_3}$ with degrees 4 and 5, respectively, because much larger volumes of cargo flows pass through it. Similarly, subnetworks $\mathbf{A_1}$, $\mathbf{A_2}$ and $\mathbf{B_1}$, $\mathbf{B_2}$ (Figs. 1b and 1c) are absolutely equivalent from a structural point of view, but play a significantly different role in the functioning of railway transport system of the region [13]. This means that the choice of NS or MLNS model and the calculation of elements' importance indicators based on its can significantly affect on the choice of system protection strategies and the effectiveness of these strategies.



a) b) c)

Figure 1: Examples of networks that reflect the structure and operation process of the railway transport system of the western region of Ukraine

Usually, lesions of structural elements, for example, a traffic jam or an accident at a city intersection, leads to the redistribution of flows movement in other ways, which can already create critical load conditions on them and, as a result, traffic jams and blocking of new structural elements (other intersections), as is often happens on the highways of a big city during rush hours. At the same time, the more such elements are damaged, the more difficult it is to redistribute the movement of flows. Such processes are often interconnected and can have a chain character, and lesion of one element can lead to damage of entire system or a significant part of it, as happens during cascade phenomena.

Each real NS interacts with many other systems, in combination with which it forms suprasystem formations of various types. Lesions of such NS can lead to destabilization of the functioning of all related systems in such formation. This was clearly demonstrated by the spread of Covid-19 pandemic, which led to a significant reduction in passenger and cargo transport flows, the deterioration of financial and economic condition of many countries and the resulting social discontent of the population, for which even the most developed countries of the world were unprepared. This means that studying the problem of stability of intersystem interactions is no less important than determining the vulnerability of a separate network system that participates in them. This also applies to any real system and ICT that supports or monitors its operation. Currently, studies of the stability of such interactions are mainly focused on interdependent multilayer networks (MLN), i.e. hierarchical-network structures of direct subordination with a linear control model [16].

In order to develop the ways of protecting the structure of intersystem interactions, it is necessary to understand the features of this structure. The structural model of such interactions is described by multilayer networks [12] and is represented as

$$G^M = \left(\bigcup_{m=1}^{M} G_m, \bigcup_{\substack{m,k=1 \\ m \neq k}}^{M} E_{mk} \right), \quad (1)$$

where $G_m = (V_m, E_m)$ determines the structure of m-th network layer of MLN; V_m is the set of nodes of network G_m; E_m is the set of edges of network G_m; E_{mk} is the set of connections between the nodes of the sets V_m and V_k, $m \neq k$, $m,k = \overline{1,M}$, where M is a number of MLN's layers (network systems which take a part in intersystem interactions). The set

$$V^M = \bigcup_{m=1}^{M} V_m$$

will be called the total set of MLN nodes, N^M is a number of elements of V^M.

The multilayer network G^M is completely described by the adjacency matrix

$$\mathbf{A}^M = \{\mathbf{A}^{km}\}_{m,k=1}^{M},$$

in which the value $a_{ij}^{km}=1$ if there is an edge connecting nodes n_i^k and n_j^m, and $a_{ij}^{km}=0$, $i,j = \overline{1,N^M}$, if there is no such edge. At the same time, blocks $\mathbf{A}^{mm}$ describe the structure of intralayer interactions in m-th layer, and blocks $\mathbf{A}^{km}$ describe the structure of interlayer interactions between m-th and k-th layers of MLN, $m \neq k$, $m,k = \overline{1,M}$. If all blocks of the matrix $\mathbf{A}^M$ are defined for the total set of MLN nodes, then the problem of coordination of node numbers in case of their independent numbering for each layer is removed. From a structural point of view, the most general type of multilayer networks can be considered partially overlapped MLN, the intersection of sets of nodes V_m of which is non-empty (Fig. 2) [12]. Borderline cases of partially overlapped multilayer networks are multiplexes, i.e. MLN, the sets of nodes V_m of which completely coincide, and multi-networks, i.e. MLN, the sets of nodes V_m of which do not intersect, $m = \overline{1,M}$. As in the case of ordinary NSs, the structural model of multilayer network system and calculated on its basis local and global characteristics of MLN elements (centralities of various types) allow us to determine the most important its components from structural point of view [14].

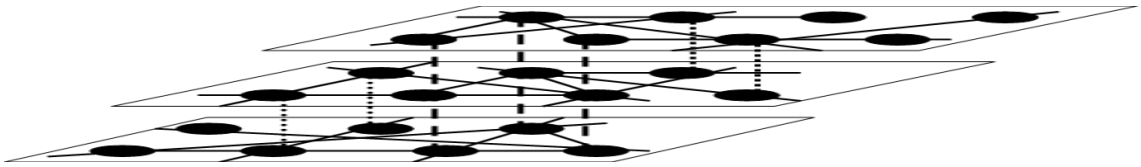


Figure 2: An example of structure of partially overlapped multilayer network

A number of practically important problems of system analysis can be solved on the basis of structural model of MLN. Among such problems, we can call [12, 17] the construction of shortest paths through a multilayer network, the search of alternative paths through different network layers during isolation a certain area in separate network layer, finding a path from arbitrary node of one layer to any node of another layer of partially overlapped MLN, especially if they lie outside the intersection of the sets of nodes of these layers, etc. At first glance, these problems are not directly related to the vulnerability of multilayer networks. However, as the experience of russian-ukrainian war has shown, lesions of the shortest and alternative to them ways of supplying weapons and ammunition significantly reduces the effectiveness of aggressor's hostilities and increases its losses.

Blocking remote sources of supply of minerals or energy carriers can significantly affect the country's economy, etc. That is, solutions of problems listed above can be the goal of targeted attacks on MLN.

Intersystem interactions can be described in the form of a flow model of multilayer network system, each layer of which reflects the process of functioning of separate NS that participates in such interactions. The most general type of multilayer systems are multidimensional (multifunctional, multiflow [17]) MLN, each layer of which ensures the movement of specific, i.e. different from other layers, type of flow. Examples of such MLN are the system of international cooperation, which includes financial, economic, military, security, scientific, cultural, sports and other layers; the system of ensuring the vital activities of a large city or a region of the country, which includes systems for the supply of electricity, gas, water, telephone and Internet communication, cable television and security, etc. Multidimensional MLN are generally characterized by the impossibility of flow transition from one layer to another (turning passengers into cargo or a team of weightlifters into a ballet troupe). Therefore, in order to simplify the study of intersystem interactions, we use an approach that consists in the decomposition of multidimensional MLN into monoflow multilayer systems, which ensure the movement of flows of only one type by different carriers or operator systems and the possibility of flow transition from one layer to another through the so-called transition points, i.e. nodes that have connections with elements of other system layers. Transition points can have multiple connections with nodes of other layers (e-mail or telephone communication) or provide communication only with points with the same number from the general set of nodes of multilayer network (common transport MLNS). From a functional point of view, the last case means that the corresponding node is an element of several system-layers and performs one function in them in different ways. Using this approach, it is advisable to divide the general transport system into two monoflow four-layer systems, each of which ensures the movement of passenger or cargo flows by road, rail, air or water (sea or river) transport, respectively. Monoflow MLNS are quite common in the real world, and interlayer interactions are usually the most intense in them. On the one hand, such MLNS are less vulnerable than its separate layers, due to the possibility of "duplication" of flow paths, and on the other hand, it is precisely in such MLNS the lesions of one layer can have the greatest impact on the functioning of other system layers. They also accelerate the spread of negative impacts of various nature (epidemics, computer viruses, etc.). The process of intra- and intersystem interactions in monoflow MLNS can be quantitatively described using the flow adjacency matrix $\mathbf{V}^M(t)$, the structure of which coincides with the structure of matrix $\mathbf{A}^M$. Blocks $\mathbf{V}^{mm}(t)$ of this matrix are flow adjacency matrices of *m*-th system-layer of the MLNS, and blocks $\mathbf{V}^{km}(t), \quad k \neq m, \quad k,m = \overline{1,M}$, are flow adjacency matrices of interlayer interactions at the transition points of multilayer network system. On the basis of this model, we can determine such indicators of functional importance as flow degrees of nodes, parameters of influence of nodes, and parameters of betweenness of nodes and edges, as well as separate layers of MLNS [14], etc. With the help of these indicators, it is possible to determine the role of these elements and layers in the process of intra- and intersystem interactions, the peculiarities of their behavior depending on the processes unfolding in multilayer systems, in particular, to which part of MLNS the lesion of a separate node, edge or layer will spread and to what losses this will lead etc. Forecasting the values of flow characteristics make it possible to determine at least short-term trends of changes in the real importance of elements and layers in the process of intersystem interactions, which can significantly affect the priorities of MLNS protection.

A number of practically important problems of system analysis can be solved on the basis of flow model of MLNS. Among such problems, we can call [14, 18] the search of fictitious and hidden elements of multilayer system, study of processes that unfold in the MLNS at all stages of its life cycle, communities detection in multilayer system, determination of controllability and observability of MLNS, etc. At first glance, solving these problems is not directly related to the resistance of intersystem interactions to negative internal and external influences. At the same time, solutions of above problems allows us to track the sources of spread of false information and propaganda that distorts the public opinion of citizens and can influence on the results of democratic elections and referenda, to distinguish between the lesions of MLNS and the natural processes of aging of its separate components, to detect dangerous for the normal functioning of multilayer system components (radical or extremist groups of various orientations, formations such as "Blue Whale" or

"PKV Redan", national or religious minorities dissatisfied with their position), to identify elements of MLNS, the lesion of which can disrupt the controllability or observability of intersystem interactions, etc. That is, the solutions of these problems can be the purpose of targeted attacks or contribute to the spread of non-target lesions of multilayer network system.

It is obvious that the problem of vulnerability of multilayer network system is much deeper and more difficult than the problem of resistance to the negative impacts of its separate layer. We distinguish two main types of MLNS lesions. The first of them consists in the initial lesion of one layer, which in one way or another consistently leads to damage of structure or operation process of other layers-systems, i.e., the affected layer-system becomes an external source of negative influence on related systems. Well-known lesions of power supply networks of large cities (New York, 1977), regions of the country (USA and Italy, 2003), or the state (Ukraine, 2022), which caused failures in functioning of many industrial and life support systems of this city, region or the state. The Covid-19 pandemic has destabilized the operation of almost all economic, financial, transport and social systems of most countries of the world. During the russian-ukrainian war, the blockade of Ukraine's seaports (the water layer of the country's general transport system), through which about 60% of its exports were carried out, not only created a threat of starvation for 400 million people in 38 countries of the world, but also reduced by about 40% the railway and road cargo transport flows within the country, which ensured this export. The second type of MLNS lesions consists in simultaneous negative impacts on the part or all its layers. Examples of such impacts include modern hybrid wars, which are carried out by combining economic, financial, informational, military attacks or "comprehensive sanctions" against countries that pose a threat to world security, etc. The multidimensional MLNS allow us to simulate such negative influences and their consequences sufficiently adequate.

4. The main approaches to protection against targeted attacks and non-target lesions

Since the lesions of MLNS are usually carried out by successive or simultaneous damage of its separate layers, the approaches to protection of intersystem interactions are formed primarily on the basis of development of protection methods for the NS, which are the part of multilayer network system. A feature of modern studies of the NS resistance to heterogeneous negative influences is the development of scenarios of separate elements lesions or the sequential lesions of a group of the most structurally important network nodes. At the same time, it is obvious that a simultaneous attack on such group or a system-wide attack that affects on all elements of the NS to one degree or another is significantly more dangerous for any real network system. The usefulness of such scenarios lies in the fact that, by providing a picture of the possible development of attack, they allow us to create effective means of protection against it. The most effective attack scenarios are formed when their developer "puts himself" in the place of attacker who, with minimal means, tries to cause maximum damage to the most important from structural or functional point of view NS elements. The creation of each scenario should be preceded by the development of attack success criteria. From a structural point of view, such criteria can be the division of NS into unconnected components, the elimination of intersystem interactions between separate layers of MLN and so on [19], and from the functional point of view – the termination or significant limitation of the movement of flows or the creation of critical load conditions of the most important elements or subnetworks of NS or MLNS [20].

The structural scenarios of NS lesions developed so far, which can be divided into two main groups, are based on the use of various indicators of the importance of nodes in the system structure (degree, betweenness, closeness, eigenvalue centralities [7], etc.). Each of scenarios of the first group begins with the arrangement of a set of NS nodes in the order of decreasing values of their centrality of corresponding type and further sequential removal from the structure of nodes according to this order. The scenarios of this group do not involve changing the centrality values of nodes that remained in the network. In the second group of scenarios, it is taken into account that with each removal of node, the NS structure may albeit slightly change due to the establishment of new connections between the remaining nodes. This requires a new ordering of the sequence of NS nodes according to the changed values of their centralities. The next step in this group of scenarios removes

a node from the beginning of the newly created list that takes these changes into account. The existence of more than ten types of structural centralities means a certain ambiguity in their use as indicators of the NS nodes importance.

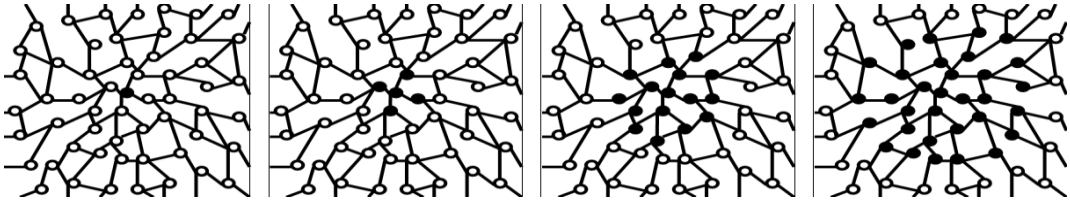
The construction of functional scenarios of targeted attacks is carried out according to the same principles as structural ones, with the difference that more adequate, as it was shown above, parameters of their flow influence and betweenness are used as indicators of the importance of NS nodes [14]. This significantly increases the effectiveness of such scenarios. The structural and functional approaches to construction the scenarios of targeted attacks on the system discussed above can be combined. For example, if there are groups with the same values of a certain type of structural centrality in the sequence of NS nodes, they can be ordered by the values of selected type of functional centrality and vice versa. These approaches can also be used to build scenarios of simultaneous group attacks on the system. So, if at the beginning of ordered list there is a group of equally important nodes according to a certain centrality, then it is possible to carry out a simultaneous attack on this group of NS elements.

Along with determining the primary targets of lesion, it is equally important to find and neutralize the sources of such lesion, because sometimes it is much easier to eliminate the source of negative impact on the system than to overcome the consequences of a global targeted attack or non-target lesion of NS. Often, such source is obvious (an active volcano, a known terrorist or hacker group, an area of chemical or radiation contamination, an aggressor country, etc.). In many cases, it is easy enough to find. Thus, centralized generators of fakes are characterized by the large volumes of output flows and minimal volumes of input flows, which makes it quite easy to identify them by analyzing the values of parameters of the input and output influence of network nodes [19]. The situation is much more complicated in the case of non-centralized lesions of the system. So, even in the most developed countries of the world, the so-called "zero patient" from which the spread of Covid-19 in these countries began was not found. One of the ways to neutralize the source of negative influence can be a counterattack on it, as is done during the implementation of economic sanctions against countries that pose a threat to global security. Obviously, all of the above approaches to system protection work best in combination.

Nodes of transport MLNS, which ensure the movement of the largest volumes of flows in the system, and have the largest values of influence and betweenness parameters in the process of intra- and intersystem interactions, are subject of priority protection from targeted attacks. At the same time, during non-target lesion, such as the spread of epidemics of dangerous infectious diseases, such nodes need to block the passenger traffic as soon as possible. Similar situations arise when providing protection against cyber attacks and the spread of computer viruses or fakes. That is, blocking a certain component of the NS can be both the goal of an attack on the system and a way to protect it. It follows that the problem of system vulnerability can be conditionally divided into two problems – direct and inverse. The direct problem consists in determining those elements of NS that must be protected first of all in order to prevent destabilization or termination of the system operation, and the inverse problem is reduced to determination of those elements, the blocking of which will lead to the minimization of losses that await network system as a result of lesion. As the example of transport system shows, scenarios aimed at preparing the defense of NS against targeted attacks can be no less successfully used to counter the spread of non-target lesions. On the other hand, the process of propagation of non-target lesions can become the basis for building effective scenarios of targeted attacks. Thus, the measures taken to combat the spread of Covid-19 pandemic actually turned the world into a network of isolated zones-countries, the movement of flows between which (especially human) has decreased by orders of magnitude due to the suspension or significant limitation of rail, air and road connections. Moreover, many states, in particular Ukraine, as a result of implementation of such restrictions, have also turned into networks of isolated zones – regions, communities and separate settlements. The self-isolation of the majority of citizens, which was caused by traffic restrictions, large fines for non-compliance with quarantine conditions and the suspension of business operations or their work in remote access mode, significantly reduced the volume of not only external, but also internal flows in such isolated zones. Under the unchanged structure of network, a kind of "granulation" of NS took place, which was divided into a hierarchy of successively isolated subsystems in the sense of limitation of interactions. These circumstances naturally led to reduction in production and trade, losses from which significantly accelerated and deepened another financial and

economic crisis and even led to social unrest in some countries of the world. Such "granulation", which has become an effective means of combating the spread of Covid-19 pandemic, is at the same time a very effective way of a global targeted attack on the system. An example of such attack is the financial and economic crisis that began in the Soviet Union as a result of embargo due to the war in Afghanistan and, unexpectedly for the initiators of sanctions, became almost the most important factor in disintegration of the USSR into separate independent republics.

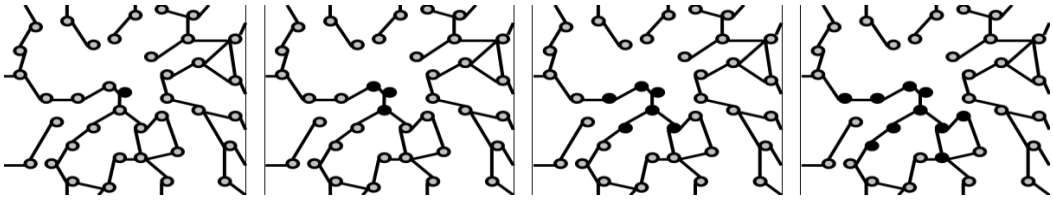
The strategies for protecting systems were considered above, in which a certain gradation of elements importance can be introduced. However, both presidents of large countries and cesspool cleaners were sick with Covid-19. That is, there are negative influences that damage unprotected elements of the system, despite their importance by any criteria. Vivid examples of such lesions were and are the spread of dangerous infectious diseases. The main means of protection and countermeasures against such lesions are the introduction of quarantine zones and/or vaccination. Based on the network approach, we modeled the process of infection spreading in the case of unprotected and to varying extent vaccinated population. Fig. 3 shows such process in the case of unvaccinated network nodes. Fig. 3a contains the network structure with painted in black so-called "zero patient" and at each subsequent step (Figs. 3b-3d) the nodes adjacent to already infected (also painted in black) are infected.



a) b) c) d)

Figure 3: Infection spreading through an unprotected network system

Fig. 4 contains the process of infection spreading in the network depicted in Fig. 3a, from which 33% of randomly vaccinated nodes were removed. In fig. 4a shows the network of vulnerable nodes obtained in this way (protected nodes and their connections are not displayed on it). From the subsequent steps, at each of which (Fig. 4b-d) only adjacent to the infected, unvaccinated nodes are infected, it follows that the vulnerability of even by 33% protected network is significantly reduced. This is quantitatively supported by the data in Table 1, from which we can conclude that even by 66% protected network can become virtually invulnerable.



a) b) c) d)

Figure 4: Infection spreading in the network (Fig. 3a), 33% nodes of which are protected (vaccinated)

Table 1

Network vulnerability depending on the number of protected nodes

Step	Percentage of protected nodes		
	0%	33%	66%
1	5	3	2
2	16	6	3
3	32	10	3
4	55	16	3

The level of losses caused to the network or multilayer network system during a certain type of negative influence can be quantified by comparing its structural and flow models during this lesion with corresponding models before the influence. Thus, the ratio of the number of nodes of MLNS structural model (1) (the dimension of matrix $\mathbf{A}^M$) during the lesion to the number of its nodes before the lesion determines the level of losses that the multilayer network suffers at the current moment as a result of this lesion. The ratio of the number of edges of MLNS structural model (1) (the number of non-zero elements of matrix $\mathbf{A}^M$) during the lesion to the number of its edges before the lesion determines the level of reduction of internal and intersystem interactions that the multilayer network is experiencing at the current moment as a result of this lesion. The ratio of the sum of elements of the matrix $\mathbf{V}^M(t)$ during the lesion to the sum of its elements before the lesion determines the level of functional damage that the multilayer system suffers at the current moment the effect of this lesion. Similarly, by comparing structural and functional models, the losses of multilayer system after the lesion are assessed. In the same way, the structural and functional losses of each layer-system of the MLNS in the process of intra- and intersystem interactions during and after damage are determined.

5. Overcoming the consequences of system lesions

No large complex system is able to protect all its elements from global targeted attacks or non-target lesions of various nature. This means that, along with organization of protection, it is no less important to develop means aimed at overcoming the consequences of system lesions. The paper [18] substantiates the need to create information models (IM) of real NSs that are important for the life of society for continuous control of their state, operation process, and improvement of work efficiency. Equally important is the role of such information models when overcoming the consequences of negative internal or external influences on NS or MLNS. Analysis of such consequences requires a holistic and complete understanding about the state of the system before, during and after the lesion. This understanding is formed on the basis of all information about the history, current state and the forecast of system behavior. Based on these considerations, we will call the information model of MLNS a data structure identical to structure of intersystem interactions, dynamic in the sense of constant expansion and replenishment, each component of which contains information about the state, operation process and interaction with the corresponding system components at the current moment, in the past and in the future, starting with the elements and ending with system at a whole. It is obvious that IM of real systems can contain extremely large amounts of data that cannot be processed "manually" in acceptable time intervals. At the same time, the operational analysis of information and the making of reasoned decisions based on it are especially important in crisis situations for every system. One of the ways to solve this problem is the formation on the base of IM the model of complex evaluation of MLNS [13], which includes models of interactive, regular and regressive evaluation of its state and operation process.

The model of MLNS interactive evaluation is built on the basis of results of continuous monitoring of its operation process, which are entered into the information model, and consists in the constant keep tracking of the interaction of intra- and interlayer flows with the elements of multilayer network system. Thus, during the analysis of Covid-19 pandemic spreading, the main tasks of this model are the selection of data about the number of newly infected people, people who have recovered and died, short-term forecasting of the necessary number of medicines, medical equipment and hospital beds, making decisions about strengthening or weakening quarantine measures, etc. The model of regular evaluation is built on the basis of information collected during a certain period of MLNS operation time, and involves a deep and thorough analysis of lesion consequences for all system elements, which were observed during this period. Regular evaluation of the consequences of Covid-19 spreading should be carried out after the end of the current pandemic wave. The main task of this model is to summarize the readiness of state and health care structures, financial and economic system of the country and its separate regions to threats that arose during the previous wave, and to prepare for minimizing the negative consequences of the next wave. The regressive model uses all data contained in the information model and collected over a sufficiently long period of time, and is intended for the search and analysis of regular and / or large-scale effects that are atypical for the behavior of system elements and were not detected and eliminated after previous interactive and

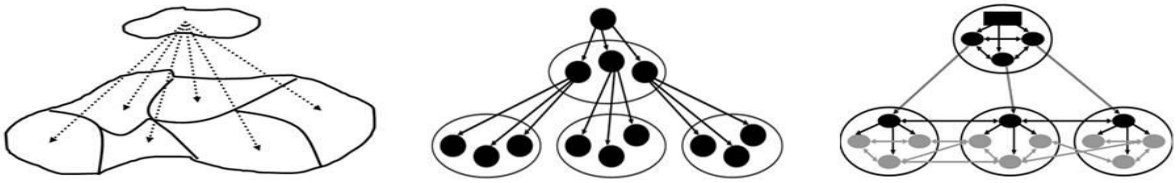
regular evaluations. The main task of this model is to identify threats before they become widespread and turn into a real system lesion. The regressive model is advisable to use to establish a real picture of morbidity and mortality from Covid-19. The search criterion in this case is a positive result of PCR or ELISA testing. However, since about 80% of infected people suffer from this disease without any symptoms and do not consult doctors, and not all citizens are tested, the real picture of coronavirus spreading has not yet been established. That is, despite the presence of clear search criteria, it is possible to form an objective conclusion about the real state of the system only on the basis of indirect data. An important task of this model is also to determine and forecast possible remote consequences of this damage (complications, effects of vaccination, deterioration of the condition of people with chronic diseases and so on). In each of the above evaluation models, interrelated methods of local analysis of the state, operation quality and interaction of MLNS elements are used adapted to the implementation of specified goals of every model; methods of aggregated evaluation, aimed at building generalized conclusions regarding separate subsystems or layers of MLNS; and methods of prognostic assessment of the behavior of evaluations of multilayer system components in the short-, medium- and longterm perspective. In particular, if in the models of interactive and regular evaluation these methods determine the negative impact of lesion on the basis of quantitative measure of the departure of characteristics of elements beyond the limits of established standards, then in the regressive model – effects not detected during continuous monitoring or regular investigations of system elements, massively distributed in space and / or time. The events of recent years testify to the importance of objective versatile evaluation of the system state and its readiness to overcome various types of threats. The overestimation of the health care systems capabilities of even the most developed countries has led to the late creation of vaccines against Covid-19 and millions of victims among the world's population. The overestimation of military power of the russian army and the underestimation of defense capabilities of Ukraine caused the late supply of weapons and prolongation of russian-ukrainian war.

The main advantage of evaluation models compared to IM of multilayer systems is orders of magnitude smaller amounts of data, which are much easier to analyze and allow us to quickly localize the most affected elements of MLNS, that is, it is an effective means to overcome the problem of quantitative complexity of system research. At the same time, the identity of structures the evaluation models and IM of multilayer system allows us quite simply to move from the evaluation of element to the analysis of all available data about it, which are contained in the relevant component of information model. Since the majority of actually existing MLNS are comprehensive, that is, multipurpose and multifunctional formations, their lesions and the consequences of these lesions can be comprehensive in nature. It is the model of complex evaluation of MLNS, which combines various types of system studies, methods of intellectual data processing and interconnected approaches to the analysis of results allows us to create an adequate picture of system behavior and make appropriate operational decisions to eliminate the identified threats.

6. On the effective implementation of approaches to system protection and overcoming the consequences of lesions

The vast majority of real complex network systems can be represented in the form of hierarchies of ordering, subordination, influence or their combination (Fig. 5a)-b)) [18]. Such representation contributes to a better understanding of the principles of the NS structure formation and processes that take place in it, and simplifies decision-making support procedures. Complex hierarchical network structures (Fig. 5c) and systems (CHNS) obtained as a result of such hierarchization are characterized by a large number objects of different types (elements, subsystems of various levels of hierarchy), and by the peculiarities of action of negative internal and external influences. At the same time, the information and evaluation models of such systems are better structured and understandable for decision-maker. The study of the state and process of functioning of such systems requires operational processing and analysis of significant volumes of quickly and continuously arrived input data of various origins. Naturally, actions to protect complex network systems must be carried out in real time to minimize the consequences of lesion regardless of its type. For this purpose, it is advisable to use not only modern research methods, but also high-performance computing devices [21] and high-

speed telecommunication technologies (radio, optical, and other electromagnetic systems). The most modern supercomputers are clusters, in which, in addition to powerful processors, a high-performance communication environment is used to connect computing nodes. Most often, such environment is built on the basis of 100 Gigabit Ethernet, InfiniBand, Intel Omni-Path, Tofu interconnect D, Slingshot-10/11 technologies, Aries interconnect, Broadcom, etc. In the latest telecommunication technologies, fiber optic cables replace the usual communication lines in most new generation networks. In addition, significant volumes of information are transmitted using mobile communications, in particular the 4G standard, which is the most common in vast majority countries of the world. The 5G standard is already being implemented, the full transition to which is planned by 2035, and the foundations of the 6G standard are being developed.



a) b) c)

Figure 5: Fragments hierarchy of ordering (a), hierarchy of subordination (b), and hierarchical network structure (c)

Since the information models of real hierarchical network systems are characterized by huge amounts of data that cannot be processed "manually" in an acceptable time, we have developed a general approach to the effective implementation of above-described complex evaluation methods based on large-block parallelization of its components. In addition, effective parallel algorithms for information processing within each of the selected blocks have been built for local, interactive, prognostic, and aggregated evaluation of the CHNS's components of different hierarchical levels.

The results of interactive and prognostic evaluation are especially important for overcoming the consequences of system lesions. For this purpose, parallel algorithms for forecasting both the evaluations themselves and the behavior of characteristics of CHNS components under study are proposed. The interactive evaluation procedure is formally divided into five steps [22], at each of which a given number of evaluations of a certain level of generalization is calculated in parallel, starting from local ones and ending with averaged evaluation of the fourth level of generalization. The corresponding parallel algorithm is specified using the primitives *fork*, *join* (branching, merging) by the following algorithmic construction:

$$\begin{aligned} &fork\,(h_1^0, h_2^0, ..., h_{l_0}^0)\ join, \\ &fork\,(h_1^1, h_2^1, ..., h_{l_1}^1)\ join, \\ &fork\,(h_1^2, h_2^2, ..., h_{l_2}^2)\ join, \\ &fork\,(h_1^3, h_2^3, ..., h_{l_3}^3)\ join, \\ &h^4, \end{aligned} \qquad (2)$$

where $h_{i'}^0,\ i'=\overline{1,l_0}$; $h_{j'}^1,\ j'=\overline{1,l_1}$; $h_{k'}^2,\ k'=\overline{1,l_2}$; $h_{l'}^3,\ l'=\overline{1,l_3}$, are the parallel branches, in which local evaluations and evaluations of the first, second, and third levels of generalization are calculated, respectively; h^4 is a fragment in which the evaluation of fourth level of generalization is calculated. It was established that the acceleration of parallel algorithm (2) is quite significant. Note that the above algorithmic construction does not take into account any limitations on the amount of computing resources. We also propose a parallel evaluation algorithm that takes into account such constraints and show that its speedup is close to its optimal value. The constructed parallel algorithms for interactive and prognostic evaluation of complex hierarchical network systems are oriented to implementation on modern computing devices – clusters with multi-core processors and in high-performance environments that generally reflect the structure of studied systems. Since interactive

evaluation is based on the results of continuous monitoring of CHNS components, it, together with prognostic evaluation, based on the implementation of corresponding parallel algorithms on high-performance hardware, allows us to timely detect the potential threats, reduce their impact on the system, and prompt plan the material costs to eliminate the consequences of possible lesions. In real systems, in most cases, negative trends in their functioning are revealed between the current and the next regular evaluation. Such evaluation is important for improving the system operation and modernizing its separate components, but it does not allow us to respond in a timely manner on a number of unexpected external or internal influences that may lead to irreversible consequences in the work of both separate elements and CHNS as a whole. It should also be noted here that modern technical means of quality selection, measurement, identification and transmission of information are used in almost real time to obtain significant volumes of various types of continuous monitoring data and this pace should be maintained during further processing such data using parallel evaluation algorithms.

7. Conclusions

In 2020-2023, humanity faced two global challenges. The Covid-19 pandemic is a vivid example of a system-wide non-target lesion. The russian-ukrainian war and reverse comprehensive sanctions against aggressor are the examples of targeted attacks. The negative consequences of these lesions (threat of the world food, energy, financial crisis and beginning of the third world war) affected almost all countries of the world. Humanity proved to be unprepared for such challenges, but the problems of global warming, climate disasters and large-scale droughts remain. Over the past half century, about 67% of known plant and animal species have disappeared [23], and over the past 20 years, the costs of combating climate disasters have increased 8 times [24]. So far, scientists know more than 20 viruses of dangerous infectious diseases, the mutations of which can lead to the spread of pandemics, much more catastrophic than Covid-19 [25], the threat of global military conflicts is increasing, etc. This confirms the relevance of studying the features of group and system-wide lesions of various types and developing methods of protection against them for many real systems. Non-target negative impacts or targeted attacks on separate network system or intersystem interactions may be aimed at destabilizing their structure and/or the operation process and arise as a result of action of both internal and external sources. Understanding the structural and functional importance of system elements allows us to choose objects that require priority protection or most contribute to the spread of lesions. The development of scenarios for the protection or blocking of such objects and the practical implementation of these scenarios, timely neutralization of the sources or causes of lesions allows us to significantly reduce the damage that these lesions can cause both to separate MCs and to the MLNS of which they are a part. Complex evaluation of consequences of negative impact on the system or the process of intersystem interactions and determining the sequence of actions that can be used to overcome these consequences and return them to unaffected state is equally important step to ensure normal life activities. All these tasks can be successfully solved by developing and applying modern information and high-speed telecommunication technologies, as well as the use of high-performance computing tools, and their results will be implemented for more effective protection of complex network, hierarchical network and multilayer network systems from targeted attacks and non-target lesions of various types.

8. References

[1] Y. Sawada, M. Bhattacharyay, and T. Kotera, Aggregate impacts of natural and man-made disasters: A quantitative comparison, International Journal of Development and Conflict 9(1) (2019) 43-73.

[2] A. Rose, Economic resilience to natural and man-made disasters: Multidisciplinary origins and contextual dimensions, Environmental Hazards 7(4) (2007) 383-398.

[3] S. Iyer et all, Attack robustness and centrality of complex networks, PLoS ONE 8(4) (2013) e59613.

[4] P. Holme et al, Attack vulnerability of complex networks, Physical review E: Statistical, nonlinear, and soft matter physics 65(5-2) (2002) 056109.
[5] W.R. Scott and G.F. Davis, Organizations and organizing: Rational, natural and open systems perspectives. New York: Taylor & Francis Group, 2015.
[6] R. Albert, H. Jeong, A.-L. Barab´asi, Error and attack tolerance of complex networks, Nature 406 (2000) 378–382. doi: 10.1038/35019019.
[7] Main indicators of the activity of banks.URL: https://index.minfin.com.ua/ua/banks/stat/
[8] Everything about the cyber attack on Ukraine on February 15th: banks and law enforcement agencies were damaged. URL: https://24tv.ua/use-pro-kiberataku-ukrayinu-15-lyutogo-postrazhdali-golovni-novini_n1868773
[9] 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. doi: 10.1016/j.physa.2014.06.079.
[10] S. Wandelt et al, A comparative analysis of approaches to network-dismantling, Scientific Reports 8(1) (2018) 13513. doi: 10.1038/s41598-018-31902-8.
[11] L. Glenn, Understanding the influence of all nodes in a network, Science Reports 5 (2015) 8665. doi: 10.1038/srep08665.
[12] S. Boccaletti et al, The structure and dynamics of multilayer networks, Physics Reports 544(1) (2014) 1-122. doi: 10.1016/j.physrep.2014.07.001.
[13] D. O. Polishchuk, O. D. Polishchuk, M. S. Yadzhak, Complex deterministic evaluation of complex hierarchically-network systems. I. Methods description, System Research and Information Technologies 1 (2015) 21-31.
[14] 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. doi: 10.20535/SRIT.2308-8893.2018.2.05.
[15] A.-L. Barabasi, The architecture of complexity, IEEE Control Systems Magazine 27(4) (2007) 33-42.
[16] 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. doi: 10.1007/s11067-014-9274-2.
[17] M. Berlingerio et al, Multidimensional networks: foundations of structural analysis, World Wide Web 16 (2013) 567–593. doi: 10.1007/s11280-012-0190-4.
[18] O. Polishchuk, M. Yadzhak, Network structures and systems: III. Hierarchies and networks, System Research and Information Technologies 4 (2018) 82-95. doi: 10.20535/SRIT.2308-8893.2018.4.07
[19] Q. Nguyen et al, Conditional attack strategy for real-world complex networks, Physica A: Statistical Mechanics and its Applications 530 (2019) 12156. doi: 10.1016/j.physa.2019.121561.
[20] O. Polishchuk, Vulnerability of complex network structures and systems, Cybernetics and Systems Analysis 56(2) (2020) 312-321. doi: 10.1007/s10559-020-00247-4.
[21] The list Top500 URL: www.top500.org.
[22] O. Polishchuk, M. Yadzhak, Network structures and systems: IV. Parallel processing of continuous monitoring results, System Research and Information Technologies 2 (2019) 105-114. doi: 10.20535/SRIT.2308-8893.2019.2.09.
[23] Almost 70% of animal populations wiped out since 1970. URL: https://www.theguardian.com/environment/2022/oct/13/almost-70-of-animal-populations-wiped-out-since-1970-report-reveals-aoe
[24] 800% increase in UN appeal needs for extreme weather-related emergencies over last 20 years – new Oxfam research. URL: https://www.oxfam.org/en/press-releases/800-increase-un-appeal-needs-extreme-weather-related-emergencies-over-last-20-years
[25] W.-T. He et al, Virome characterization of game animals in China reveals a spectrum of emerging pathogens, Cell 185(7) (2022) 1117-1129. doi: 10.1016/j.cell.2022.02.014.