I. J. Computer Network and Information Security, **2022, 5, 1-10**
Published Online on October 8, 2022 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2022.05.01

Protecting Hybrid Information Transmission Network from Natural and Anthropogenic Hazards

Vadym Mukhin
National Technical University of Ukraine "Igor Sikorsky Kiev Polytechnic Institute", Kiev, Ukraine
E-mail: v.mukhin@kpi.ua

Pavlo Anakhov
National Power Company "Ukrenergo", Kyiv, Ukraine
E-mail: anahov.pv@ua.energy

Viktoriia Zhebka
State University of Telecommunications, Kiev, Ukraine
E-mail: viktoria_zhebka@ukr.net

Vladislav Kravchenko
State University of Telecommunications, Kiev, Ukraine
E-mail: vladkr58@gmail.com

Aksieniia Shtimmerman
State University of Telecommunications, Kiev, Ukraine
E-mail: shtimmerman.k@gmail.com

Valerii Zavgorodnii
State University of Infrastructure and Technologies, Kiev, Ukraine
E-mail: zavgorodniivalerii@gmail.com

Yurii Bazaka
National Technical University of Ukraine "Igor Sikorsky Kiev Polytechnic Institute", Kiev, Ukraine
E-mail: yura.bazaka@gmail.com

Received: 25 January 2022; Revised: 01 April 2022; Accepted: 08 June 2022; Published: 08 October 2022

Abstract: A hybrid network, which consists of the sections of communication lines with the transmission of signals of different physical nature on different transmission media, has been considered. Communication lines respond differently to threats, which allows to choose the line with the best performance for the transmission of information. The causal diagram of events that determine the state of the information transmission network, such as changes in emergency/accident-free time intervals, has been presented. The application scheme of the protection measures against dangerous events has been shown. To verify the measures, a matrix of their compliance with typical natural disasters has been developed and relevant examples have been given. It is suggested to evaluate the flexibility of the telecommunication network by its connectivity, characterized by the numbers of vertex and edge connectivity, the probability of connectivity. The presented scheme of the device for multi-channel information transmission in a hybrid network allows the choice for the transmission of information to the channel with the best performance. Using this device is the essence of the suggestion about increasing the flexibility of the network.

Index Terms: Connectivity of Network, Correspondence Matrix, Flexibility of Network, Network Damage.

1. Introduction

The number of natural disasters, caused by global climate change on Earth, has been recently increased all over the world (for example, [1–5]).

The environment is being changed by man consciously and, mainly, unconsciously. The distictive feature of modern times is the mass construction of potentially dangerous enterprises that pose a real threat of emergencies. This causes an unprecedented increase in the number of disasters of an unnatural nature [1,3,5-7].

Such extreme phenomena periodically occur in each of the regions of the world. The economic damage from them is measured by huge sums [3,7].

In the information society, the use, creation, dissemination, manipulation and implementation of information is an important activity. The main driving forces of society are information and communication technologies, which have led to a rapid increase in the diversity of information and, in one way or another, have changed all aspects of social organization. The growing number of disasters requires the development of recommendations to protect against them one of the main industries of modern production - telecommunications [4,8,9].

Considering the variability of the modern natural and anthropogenic environment, an important criterion for assessing the quality of the information transmission network becomes its ability to quickly adapt to the events that may carry and threaten the ability to work capacity. This ability is defined as flexibility and quick adaptation to a new environment, with minimal effort [1,5,10,11].

1.1. Motivation behind this Work

The hybrid network meets the criterion of flexibility. It consists of the sections of communication lines with the transmission of signals of different physical nature (electrical, optical) on different transmission media (free space, artificial guides). Communication lines respond differently to threats, which allows to choose the line with the best performance for the transmission of information [12,13].

The reason for increasing the motivation of this work is the existing theoretical developments on the hybrid network [13–17] and planned improvements on protection against cyber threats in the information system.

1.2. Contribution of Paper

In the form of a causal diagram, natural and anthropogenic hazards that threaten information transmission networks have been presented.

It has been offered the universal application scheme of the protection measures against dangers, the basis of which was the scheme of application of the lightning protection measures. Verification of protection measures has been performed.

The result of the universal scheme is a device recommended for multi-channel transmission of information in a hybrid network.

1.3. Related Works

The continuous study of the causes of accidents in the information transmission network is due to the interaction of changing processes. These are, firstly, natural changes in the environment, and secondly, anthropogenic changes in transmission technologies. The results of research are presented in the works of many researchers, for example, Claude de Ville de Goyet, Ricardo Zapata Marti, and Claudio Osorio (2006); M. M. Bonch-Bruevich (2012); Tolubko, V., Vyshnivskyi, V., Mukhin, V., Haidur, H., Dovzhenko, N., Ilin, O., Vasylenko, V. (2018); F. Rahman (2019); A. Gyasi-agyei (2019); V. V. Zhebka and P. V. Anakhov (2021).

In order to establish unified technical requirements in the field of network operation, generalize existing research and operational experience, standards and recommendations have been created, in particular, State standard of Ukraine 2860 (1994); IEC 62508 (2010); State Classifier of Ukraine 019 (2010); State standard of Ukraine 3899 (2013).

According to the causes of the dangers the following measures are being developed. These include protection of communication cables from pests according to Recommendation ITU-T L.46 (2000); precautions for the protection of underground linear cable structures in accordance with Recommendation ITU-T L.92 (2012).

P. Anakhov, A. Makarenko, V. Zhebka, V. Vasylenko and M. Stepanov (2020) developed a universal application scheme for the hazard protection measures.

Based on this scheme, V. V. Zhebka (2021) developed a flexible device for multichannel information transmission in a hybrid network, which allows to choose the line with the best performance for the transmission of information.

1.4. Aim of the Article

The aim of the article is to develop a flexible network of information transmission protected from the dangers of natural and anthropogenic nature.

To achieve this goal it is necessary to solve the following tasks:

- to systematize the causes of accidents;
- to develop a scheme for the application of the protection measures;
- to verify protection measures;
- to develop recommendations for network protection.

2. Methodology

2.1. Systematization of the Accident Causes

In Fig.1 in the form of a causal diagram (Ishikawa diagram) the events, determining the state of the network - changes in emergency/accident-free time intervals, are presented.

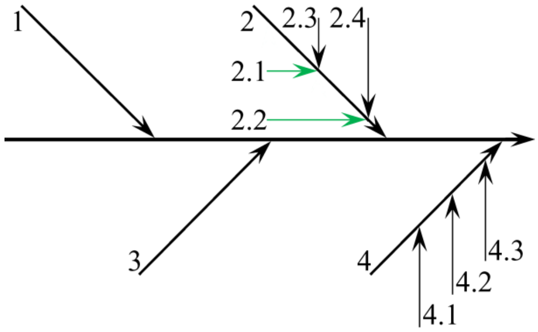


Fig.1. Diagram of events, determining the state of the information transmission network (modified from [17])

The list of the events, determining the state of the telecommunications network is presented in table 1.

Table 1. Events, determining the state of the information transmission network

Event	Explanation
1. Accident caused by a failure caused by aging and/or wear processes occurring inside the object [12]	- aging – a natural process of irreversible change in the properties of materials during storage, transportation and operation of products [13]; - wear – a special type of the products destruction due to their mechanical friction against each other or the action of electric current [13]
2. Human-operator activity (human factor)	
2.1. Accident-free operation due to error-free actions in the work of a human-operator, which allow to avoid an accident or eliminate it [15]	Positive human impact as a result of the actions taken or not, which led to the prevention, detection and elimination of failures of the components of ITS (Information Telecommunication System) [15]
2.2. Trouble-free operation due to automation of human-operator actions, including the applying of artificial intelligence	
2.3. Accident caused by erroneous actions of a human-operator [15]	Negative human impact as a result of actions taken or not, which led to the failure of the components of ITS [15]
2.4. Accident when automating the actions of a human-operator, performing erroneous actions that do not allow to avoid the accident or eliminate it, as well as provoke an accident	
3. Accident caused by external hazards of a natural nature [6,18,19]	Damages related to dangerous geophysical, geological, meteorological or hydrological phenomena, soil or subsoil degradation, fire in natural ecological systems, changes in the state of the air basin, infectious diseases and poisoning of people, infectious diseases of domestic animals, mass death of wild animals, damage to crops plant diseases and pests, etc. [18]
4. External events of anthropogenic nature:	
4.1. Accident caused by man-made damages [6,18,19]	Damages as a result of a traffic accident (catastrophe), fire, explosion, accident with the release (threat of release) of dangerous chemical, radioactive and biologically dangerous substances, sudden destruction of buildings; accidents in electric power systems, life support systems, telecommunication systems, on treatment facilities, in systems of oil and gas industrial complex, hydrodynamic accidents, etc. [18]; - conditions when the number of service requests exceeds the established capabilities of the fixed network area [20]
4.2. Accident caused by social damages [6,18,19]	Damages caused by illegal acts of terroristic and unconstitutional orientation, or related to the disappearance (theft) of weapons and dangerous substances, accidents with people, etc. [18]
4.3. Accident caused by military damages [6,18,19]	Damages caused by the conventional weapons or weapons of mass destruction employment, during which secondary factors of defeat occur [18]

2.2. Scheme of the Protection Measures Application

The scheme of the protection measures application against dangerous events of natural and anthropogenic nature is shown in Fig.2.

The proposed scheme is designed to develop a blueprint for action to prevent natural and anthropogenic hazards. Short-term hazard forecasting is performed to alert the public and collect data. The data are used in the long-term forecasting. It is used in assessing risks and their acceptable levels, to declare the safety of facilities, make decisions on their location and operation, develop measures to prevent accidents and prepare for response. The list of protection measures includes:

- application of the resistant to certain hazards materials and structures;
- interception of danger, which involves shielding the object or its most vulnerable and responsible elements from danger, or shielding danger from the object, as well as counteracting the danger;
- application of the elements of flexibility of the information transmission network, which consist in reconfiguration of systems for ensuring efficiency (power supply, ventilation and air conditioning, fire alarm, fire extinguishing, notification, etc.);
- reconfiguration of the transmission network.

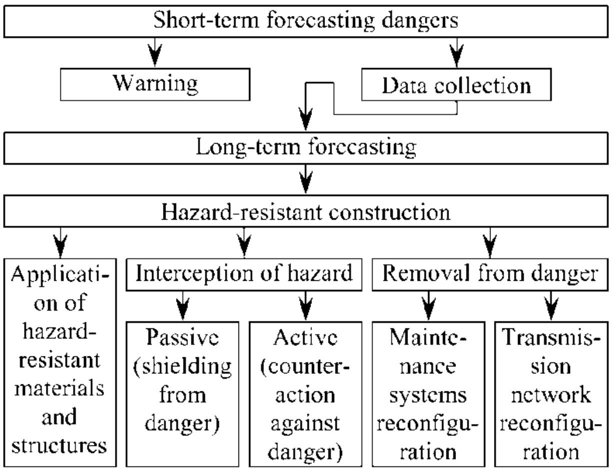


Fig.2. Scheme of application of protection measures against dangers (modified from [17])

3. Verification of Protection Measures

To verify network protection measures, a matrix of compliance of network protection measures with typical natural disasters has been developed (see Table 2).

Table 2. Matrix of compliance of information transmission network protection measures with typical natural disasters

Protection measure [17]	Natural disasters[1] [21]						
	1	2	3	4	5	6	7
1. Short-term forecasting	a_{11}	a_{12}	a_{13}	a_{14}	a_{15}	a_{16}	a_{17}
2. Warning	a_{21}	a_{22}	a_{23}	a_{24}	a_{25}	a_{26}	a_{27}
3. Application of stable materials and structures	a_{31}	a_{32}	a_{33}	a_{34}	a_{35}	a_{36}	a_{37}
4. Passive interception of danger	a_{41}	a_{42}	a_{43}	a_{44}	a_{45}	a_{46}	a_{47}
5. Active interception of danger	a_{51}	a_{52}	a_{53}	a_{54}	a_{55}	a_{56}	a_{57}
6. Reconfiguration of power, ventilation and air conditioning systems	a_{61}	a_{62}	a_{63}	a_{64}	a_{65}	a_{66}	a_{67}
7. Transmission network reconfiguration	a_{71}	a_{72}	a_{73}	a_{74}	a_{75}	a_{76}	a_{77}

[1]1 – Earthquakes, 2 – Tsunami, storm surges, 3 – Flash floods/floods, 4 – Forest fires, 5 – Hurricanes/tornadoes/typhoons/wind storms, 6 – Landslides, 7 – Severe cold, snow, ice or heat, 8 – Lightning.

Typical natural disasters are presented according to the list from ITU-T L.92 Recommendation for facilities located outside the premises for cable entry and placement of linear equipment (for outside plant facilities) [21].

Table 3 shows some examples of the application of the protection measures against natural disasters, in accordance with the elements of the matrix from table 2.

4. Recommendations for Network Protection

Fig.3 shows a diagram of a flexible device for implementing multi-channel information transmission in a hybrid network, which allows choosing the best performance channel for transmitting information.

Lettering in Fig.3: e_{ij} – communication lines (channels) between stations and network nodes; i_f, $i_f = \overline{1, n_f}$, i_t, $i_t = \overline{1, n_t}$, i_ε, $i_\varepsilon = \overline{1, n_\varepsilon}$, i_m, $i_m = \overline{1, n_m}$ – channel identifiers of frequency multiplexing systems with frequency f, with time t channel divisions, with channel divisions according to the physical nature of signals ε, with channel divisions by transmission media m, respectively; n_f, n_t, n_ε, n_m – the number of channels n of multiplexing systems with frequency f, time t channel divisions, with channel division by the physical nature of the signals ε, and by the transmission media m, respectively.

Table 3. Examples of the application of the protection measures against natural disasters

Matrix element	Examples of the application of the protection measures
$a_{11} - a_{17}$	- environmental monitoring (organization of early disaster detection systems) [21]; - monitoring of telecommunications (receiving and processing information about the state of the object, phenomena and processes directly at the installation site of the object) [21]
$a_{21} - a_{27}$	- threat alert [21]; - collection of the statistical data for processing long-term forecasts [22]; - physical-geographical zoning of territories for detection of climatic conditions of operation [23]
a_{31}, a_{36}	- increasing the sustaining capacity of the structures by increasing the size of the load-bearing elements and strength of the materials, as well as a number of design measures [24]; - application of materials, structures and structural schemes that provide the lowest values of seismic loads (light materials, seismic insulation, other systems of dynamic regulation of seismic load) [24]
a_{32}, a_{33}	- application of the waterproof partitions in cable sewers [21]; - laying communication cables in the gas pipelines, holding cables under excess pressure [21]
a_{34}	- application of the non-combustible or flame retardant materials [21]
a_{35}	- laying thin cables in a bundle wound on an optical cable, which is intended for suspension on the supports of overhead communication lines, catenary and auto-blocking of railways, power lines, lighting poles, between buildings and structures or on a dielectric cable [25]
a_{38}	- using materials resistant to thermal and dynamic influences, pulse overvoltages [26]; - using lightning-resistant cables with high sheath conductivity (aluminum) and high electrical insulation strength [27]; - to protect information from transmission errors, noise-tolerant coding with error detection, with error correction is used [28]
a_{41}	- shielding of the seismic waves by a layer of loose rock [29,30]; - using rubber gland seals for penetration into duct lines [21]; - taking measures to ensure the tightness of the hatch cover to the neck of the cable well [21]; - using flexible joints in gas pipelines to hold cables under excess pressure [21]
a_{42}	To protect against the destructive impact of the wave the following can be applied: - construction of shore protection sea walls, shafts and dams [31]; - forest plantations on the shores, which will dissipate the energy of the waves, reduce the width of the floodplain, detain floating objects (logs, small vessels, debris), which can significantly increase the destruction of rattlesnakes [31]; For flood protection – as for the high water protection (a_{43})
a_{43}	- construction of the protective structures [32]; - protection of the metal structures from corrosion by insulating coatings [33]; - installation of the watertight partitions in the cable sewers [21]; - sealing the ends of plastic pipes with a waterproof filler in hatches/mines of the underground infrastructure [21]
a_{44}	Using fire protection (insulation with clean strips of earth) [21]
a_{45}	- installation of the additional structures for compensation of wind loads (vertical struts, rope extensions) [21]; - reinforcement of the supports by steel wires (at an expected wind speed of more than 40 m/s) [21]; - using fastening between supports [21]; - increasing the maximum allowable tensile load due to cable clamps [25]
a_{46}	- installation of the retaining structures between external objects and steep landslide slopes [21]; - increasing the stability of the landslide slopes [21]
a_{48}	lightning protection system consisting of lightning arrester (lightning arrester, current arrester), grounding, equipotential bonding system (PAS), surge protection devices [34,35]
a_{51}	- excitation of weak seismicity by artificial sources in order to unload tectonic stress [36]; - installation of the oscillation damping systems [21]; - reducing the magnitude of inertial seismic loads on structures by adjusting their dynamic characteristics during the oscillating process, and controlling the mechanism of the structures deformation during the earthquakes. Adjustment of dynamic parameters is carried out in order to avoid a resonant increase in oscillation amplitudes or to reduce resonant effects [24]
a_{52}	- suppression of the long sea waves in the port approach channel, by determining the natural frequency of the channel, which depends on its morphometric characteristics, and further changes in the geometric dimensions of the channel [37], channel depth [38], to prevent resonance between incident wave and natural oscillations reservoirs
a_{53}	- providing surface water runoff [32]; - using drainage pumps in cable ducts [21]
a_{54}	Start a counter-fire to extinguish the fire [21]
a_{55}	connection of artificial dampers for protection of cables against vibration [21]
a_{56}	"Exchange" of the landslide into a series of smaller landslides, which is performed by dismemberment of the landslide by explosions in the wells into separate blocks. During an earthquake or "undercut" of the slope, the blocks of the array will move separately down the landslide surface with a smaller mass compared to the whole array [39]
a_{57}	Ventilation and air conditioning systems are used to maintain microclimate conditions that provide optimal operating conditions for technical facilities [40]
$a_{61} - a_{67}$	- duplication of the power sources and power supply cables [21]; - using reserve generating capacity due to diesel generators, autonomous wind and solar power plants [9,41]; - in some cases, backup equipment is used to increase the reliability of the technological air conditioning system of communication centers [40]
$a_{71} - a_{77}$	- reconfiguration of the telecommunication hardware outfit [4]; - adherence to the condition of spatial separation of the main and backup communication lines [16,21,42]; - adherence to the condition of separation of the main and backup communication lines by the nature of the transmitted signal [16,21,42]

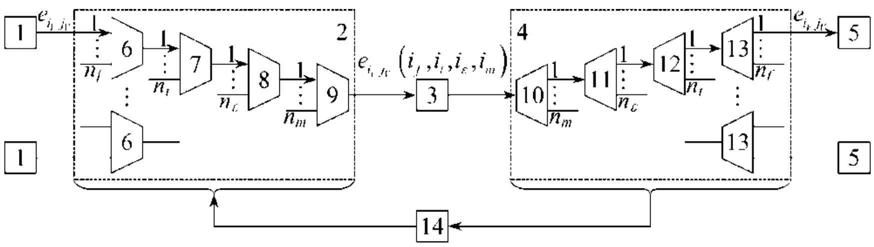


Fig.3. Block diagram of a device for multi-channel information transmission on a section of the information transmission network, in simplex mode [15]

The device for multichannel transmission of information on the network includes an information source 1, transmitter switch 2, communication line 3, the resources of which are sets of transmission media, signals of different physical nature, frequency bands and signal time intervals, receiver switch 4, user server 5, channel condition monitoring selector and transmission channel selection 14. The transmitter switch 2 comprises flexible multiplexers 6, which provide information with channel separation by n_f units ($n_f \geq 1$) by frequency, flexible multiplexers 7, which provide information with channel separation by n_t units ($n_t \geq 1$) by time, flexible multiplexers 8, which provide transmission of information with channel separation by the number of n_ε units ($n_\varepsilon \geq 1$) by the physical nature of the signal, flexible multiplexers 9, which provide transmission of information with channel separation by the number of n_m units ($n_m \geq 1$) by media. The switch of the receiver 4 includes flexible demultiplexers 10, 11, 12, 13, which provide reception of information with the division of channels by media, the physical nature of the signal, time and frequency, respectively.

The device for multichannel information transmission is implemented as follows. The information signal on the channel (communication line) e_{ij} from the information source 1 is fed to the transmitter switch 2. In the switch 2 by successive transformations in the multiplexers 6-9 the information signal is assigned a unique resource for independent transmission over the communication line 3: in the flexible multiplexers 6, 7, 8, 9 signal is assigned the frequency resource i_f, time resource i_t, resource belonging to to the set of signals of different physical nature i_ε, the environmental resource i_m, respectively. The information signal transmitted from the switch transmitter 2, using the hybrid communication line 3, on the channel $e_{ij}(i_f,i_t,i_\varepsilon,i_m)$, is received by the switch of the receiver 4. In the switch 4 by successive inverse transformations in demultiplexers 10-13 the information signal is converted in the format $e_{i'j'}$, acceptable for transmission to the switch of the receiver 5. The selector for monitoring the state of the channels and the selection of the transmission channels 14 monitors the status of resources in the receiver 4, which, when transmitted over the communication line 3, are subject to destabilizing factors, and generates commands to exclude network resources in the transmitter 2 that do not meet the accepted requirements for the quality of signal transmission and the inclusion of network resources in the switch transmitter 2, which meet the accepted requirements for the quality of signal transmission.

5. Discussion

According to [42,43], the flexibility of a network information system can be explained as adaptability, evolution and reusability.

According to research [44], network flexibility explained as adaptability, adjustability, cognitivity, configurabiliti, dynamism, intelligence, programmability, scalability, customizability.

There is a suggestion to evaluate the flexibility of the network to some extent by the ability to handle new requests. The flexibility φ of a system S, depends on its current state, as the fraction of new requests that can be supported from a given set and sequence of the new requests, within a given time threshold T [45]:

$$\varphi_T(S) = \frac{servicing\ the\ number\ of\ new\ requests\ during\ a\ certain\ time\ interval\ T}{number\ of\ new\ requests} \tag{1}$$

It should be noted that this definition corresponds to the reliability of the transmission system "coefficient of availability k_A" for a period of time T. It is calculated as the ratio of time, during which the system was under operating conditions, to the specified interval T, which takes into account the duration of downtime [46]:

$$k_A = \frac{t_r}{t_r + t_m} \tag{2}$$

where t_r – operating time between failures; t_m – recovery time.

To increase flexibility, a network on a chip using a centralized controller with two separate networks on a single platform is being proposed [42].

Integration of different networks is ensured. Wireless Access Points provide enhanced flexibility for network deployment by allowing dynamic (3-D) positioning of the nodes or even optimized trajectory planning for different objective functions. In addition to the aerial and terrestrial networks, the integration of space (satellite) and undersea networks is another aspect of the flexible hybrid networks [47].

Network resources are stations and nodes of dimension *n*, which are the set of vertices of the graph of the information transmission network $\upsilon_i \in V$, and the communication channels between them, which are described by the set of edges $e_{ij} \in E$. The network topology is given by the graph $G(V,E)$ described by the adjacency matrix [44]:

$$A = \left\| a_{ij} \right\|, \; i, j = \overline{1,n}, \; a_{ij} = \begin{cases} 1, \forall e_{ij} \in E; \\ 0, \forall e_{ij} \notin E. \end{cases} \tag{3}$$

In this case, the flexibility of the information transmission network can be described by the formula [44]:

$$\left\{ \begin{aligned} & \chi(G) \geq 2; \\ & \lambda(G) \geq 2; \\ & P_{ij}(t) \geq P_{ij}^{normalized}; i \neq j; i, j = \overline{1,n} \end{aligned} \right\} \tag{4}$$

where $\chi(G)$ – number of vertex connectivity (the smallest number of vertices, the removal of which together with the incident edges leads to an incoherent or single-vertex graph); $\lambda(G)$ – number of the edge connectivity (the smallest number of edges, the removal of which leads to an incoherent graph); $P_{ij}(t)$ – the probability of connectedness (the probability that the message from node *i* to node *j* will be transmitted in a time, which is not exceeding *t*).

6. Conclusion and Future Scope

The hybrid network, which consists of the sections of communication lines with the transmission of signals of different physical nature on different transmission media, has been considered. Communication lines respond differently to threats, which allows you to choose the line with the best performance to transmit information.

The causes of the accidents in the information transmission network have been systematized. The causal diagram of the events that determine the state of the network – changes in emergency/accident-free time intervals has been presented. An explanation of these events has been provided.

The scheme of application of measures of protection against dangerous events has been shown, as a method of the network research.

To verify the protection measures against dangerous events, a matrix of compliance of measures with typical natural disasters has been developed. Relevant examples have been given.

The scheme of the device device for implementing multi-channel information transmission in a hybrid network, which allows choosing the best performance channel for transmitting information has been presented. A suggestion to increase the flexibility of the network, which is to use this device, has been made.

It is suggested to assess the flexibility of the telecommunications network by its connectivity.

In the future research work, we intend to investigate and systematize software anthropogenic hazards, and develop a modified scheme of measures to protect the network of information transmission from cyber threats.

References

[1] Klügel, M., He, Mu, Kellerer, W., Babarczi, P. A Mathematical Measure for Flexibility in Communication Networks. In 2019 IFIP Networking Conference (IFIP Networking). DOI: 10.23919/IFIPNetworking.2019.8816855.
[2] Banholzer, S., Kossin, J., Donner, S. The Impact of Climate Change on Natural Disasters. In Zommers, Z., Singh, A. (Eds.) Reducing Disaster: Early Warning Systems for Climate Change. Springer, 2014, 21–49.
[3] Halkos, G., Managi, S., Tzeremes, N. G. The effect of natural and man-made disasters on countries' production efficiency. Journal of Economic Structures (J. Econ. Struct), 2015, Vol. 4, 10 p. DOI 10.1186/s40008-015-0019-2.
[4] ITU-D Study Group 2. Question 6/2: ICT and climate change. Final Report. Geneva: ITU, 2017. 64 p.
[5] Babarczi, P., Klügel, M., Alba, A. M., He, A., Zerwas, J. Kalmbach, P., Blenk, A., Kellerer W. A mathematical framework for measuring network flexibility. Computer Communications (Comput. Commun.), 2020, Vol. 164, 13–24. DOI: 10.1016/j.comcom.2020.09.014.
[6] Rahman, F. Save the world versus man-made disaster: A cultural perspective. IOP Conference Series: Earth and Environmental Science, 2019, Vol. 235, 012071, 10 p.
[7] Hossam Abdel Rahman Mohamed, "A Proposed Model for IT Disaster Recovery Plan", International Journal of Modern Education and Computer Science, vol.6, no.4, pp.57-67, 2014.
[8] Safonov, G. V. Dangerous consequences of global climate change. Russian Regional Environmental Centre, Global Opportunity Fund, World Wildlife Fund of Russia, 2006, 20 p. (in Russian).
[9] Weather and Climate Services in Europe and Central Asia. A Regional Review. World Bank Working Paper No. 151.

Washington, D.C., 2008, 79 p.
[10] Ospina, A. V., Faulkner, D., Dickerson, K., Bueti, C. Resilient pathways: the adaptation of the ICT sector to climate change. Geneva: ITU, 2014, 62 p.
[11] Khaled, Z. EL, Mcheick, H. Case studies of communications systems during harsh environments: A review of approaches, weaknesses, and limitations to improve quality of service. International Journal of Distributed Sensor Networks (IJDSN), 2019, Vol. 15 (2), 22 p. DOI: 10.1177/1550147719829960.
[12] Hu, Zh., Mukhin, V. Ye., Kornaga, Ya. I., Herasymenko, O. Y. Resource Management in a Distributed Computer System with Allowance for the Level of Trust to Computational Components. Cybernetics and Systems Analysis (Cybern. Syst. Anal), 2017, 53(2), pp. 312–322. DOI: 10.1007/s10559-017-9931-9.
[13] Mukhin, V., Kuchuk, N., Kosenko, N., Artiukh, A., Yelizyeva, A., Maleyeva, O., Kuchuk, H., Kosenko, V. Decomposition Method for Synthesizing the Computer System Architecture. In ICCSEEA 2019 Advances in Computer Science for Engineering and Education II. Advances in Intelligent Systems and Computing, vol 938. Springer, Cham. DOI: 10.1007/978-3-030-16621-2_27.
[14] Zhenbing Hu, Vadym Mukhin, Yaroslav Kornaga, Yaroslav Lavrenko, Oksana Herasymenko, "Distributed Computer System Resources Control Mechanism Based on Network-Centric Approach", International Journal of Intelligent Systems and Applications, Vol.9, No.7, pp.41-51, 2017.
[15] Zhebka, V. V. Patent of Ukraine №147713. Device for multichannel information transmission.
[16] Anakhov, P., Zhebka, V., Grynkevych, G., Makarenko, A. Protection of telecommunication network from natural hazards of global warming. Eastern-Europian Journal of Enterprise Technologies (EasternEuropean J. Enterp. Technol.), 2020, No. 3/10, 26–37. DOI: 10.15587/1729-4061.2020.206692.
[17] Zhebka, V. V., Anakhov, P. V. Monitoring the Sustainability of Information and Telecommunication System and Elaboration of Measures to Protect from Dangers. Metrology and instruments, 2021, No. 1(87), 23–29. (in Ukrainian). DOI: 10.33955/2307-2180(1)2021.23-29.
[18] Abdolhossein Fathi, Keihaneh Kia, "A Centralized Controller as an Approach in Designing NoC", International Journal of Modern Education and Computer Science, Vol.9, No.1, pp.60-67, 2017.
[19] Saida Boukhedouma, Mourad Oussalah, Zaia Alimazighi, Dalila Tamzalit, "Service Based Cooperation Patterns to Support Flexible Inter-Organizational Workflows", International Journal of Information Technology and Computer Science, vol.6, no.4, pp.1-18, 2014.
[20] Recommendation ITU-R P.1817-1 (02/2012). Propagation data required for the design of terrestrial free-space optical links.
[21] DSTU (State standard of Ukraine) 2860-94. Reliability of equipment. Terms and definitions.
[22] Gyasi-agyei A. Telecommunications Engineering: Principles And Practice. Singapore: World Scientific Publishing Company, 2019, 760 p.
[23] DSTU (State standard of Ukraine) 3899:2013. Design and ergonomics. Terms and definitions.
[24] IEC 62508:2010. Guidance on human aspects of dependability.
[25] DK (State Classifier of Ukraine) 019:2010. Emergency classifier (Order No. 457 on 11 October, 2010 of State Committee of Ukraine for Technical Regulation and Consumer Policy).
[26] Goyet, C. de V. de, Marti, R. Z., Osorio, C. Natural Disaster Mitigation and Relief. In: Jamison, D. T., Breman, J. G., Measham, A. R., Alleyne, G., Claeson, M., Evans, D. B., Jha, P., Mills, A., Musgrove, P. (Eds.), Disease Control Priorities in Developing Countries. 2nd edition. Washington (DC): The International Bank for Reconstruction and Development / The World Bank. New York: Oxford University Press, 2006, 1147–1162.
[27] Bonch-Bruevich, M. M. Research and development of load redistribution algorithms in cellular communication systems of the GSM standard. PhD abastract. Moscow, Technical university of communications and informatics, 2012, 24 p. (in Russian).
[28] Recommendation ITU-T L.92 (10/2012). Series L: construction, installation and protection of cables and other elements of outside plant. Disaster management for outside plant facilities.
[29] Stjebljuk, M. I. Civil Defense and Civil Protection. Kyiv: Znannia-pres, 2007, 487 p. (in Ukrainian).
[30] ITU-T Recommendation M.34 (11/88). Performance monitoring on international transmission systems and equipment.
[31] Folorunsho Olaiya,Adesesan Barnabas Adeyemo,"Application of Data Mining Techniques in Weather Prediction and Climate Change Studies", International Journal of Information Engineering and Electronic Business, vol.4, no.1, pp.51-59, 2012.
[32] GOST (Interstate standard) 15150-69. Design for various climatic conditions.
[33] Chigrinskaya, L. S. Seismic resistance of buildings and structures. Angarsk: State Technical Academy, 2009, 107 p. (in Russian).
[34] Gaskevich, E., Chizhanov, S., Petrenko, I. Drop-cable in private sector: model for calculating wind loads taking into account impact from trees. First mile, 2017, No. 7, 16–24. (in Russian). DOI: 10.22184/2070-8963.2017.68.7.16.24.
[35] Gunjaev, G. M., Chursova, L. V., Raskutin, A. E., Gunjaeva, A. G. Lightning resistance of modern polymer composites. Aviation materials and technologies, 2012, No. 2, 36–43. (in Russian).
[36] Kozak, M. M. Linear communication structures. Vinnytsia: Higher Vocational School, 2009, 317 p. (in Ukrainian).
[37] Majdanjuk, V. P. Encryption and protection of information. Vinnytsia: National Technical University, 2009, 164 p. (in Ukrainian).
[38] Alagoz, B. B., Alagoz, S. Towards Earthquake Shields: A Numerical Investigation of Earthquake Shielding with Seismic Crystals. Open Journal of Acoustics, 2011, Vol. 1(3), 63–69. doi:10.4236/oja.2011.13008.
[39] Zaalishvili, V. B., Krantsfeld, J. L. Geophysical basis of engineering earthquake protection of responsible construction objects. Geology and geophysics of the South of Russia, 2014, No. 1, 39–50. (in Russian).
[40] Vorobyov, Yu. L., Akimov, V. A., Sokolov, Yu. I. Tsunami: prevention and protection. Moscow: Russian Emergency Situations Ministry, 2006, 264 p. (in Russian).
[41] DBN (State building norms of Ukraine) B.1.1-25-2009. Engineering protection of territories and buildings from flooding and inundation.
[42] Mukhin, V., Loutskii, H., Barabash, O., Kornaga, Ya., Steshyn, V. Models for Analysis and Prognostication of the Indicators of the Distributed Computer Systems' Characteristics. International Review on Computers and Software (IRECOS), 2015, 10(12),

pp. 1216–1224. DOI: 10.15866/irecos.v10i12.8023.
[43] Mukhin, V., Volokyta, A., Heriatovych, Y., Rehida, P. Method for efficiency increasing of distributed classification of the images based on the proactive parallel computing approach. Advances in Electrical and Computer Engineering (AECE), 2018, 18(2), pp. 117–122. DOI: 10.4316/AECE.2018.02015.
[44] Strakhov, V. N., Savin, M. G. Reduction of seismic hazard: missed opportunities. Geophysical journal, 2013, Vol. 35(1), 4–11. (in Russian).
[45] Analysis of modern foreign and domestic experience in installing lightning protection systems for electrical networks. Kyiv: Research and Design Center for the Development of the United Energy System of Ukraine, 2018, 74 p. (in Ukrainian).
[46] IEC 62305-1:2010. Protection against lightning – Part 1: General principles.
[47] Recommendations for the simultaneous protection of communication cables from corrosion, lightning strikes and electromagnetic influences. Moscow: Radio and communication, 1983, 12 p. (in Russian).

Authors' Profiles

Vadym Mukhin: Professor of department of the mathematical methods of system analysis of National Technical University of Ukraine "Kiev Polytechnic Institute", Doct. of Sc.

Born on November 1, 1971. M. Sc. (1994), PhD (1997), Doct. of Sc. (2015) from the National Technical University of Ukraine "Kiev Polytechnic Institute"; Professor (2015).

Major interests: the security of distributed computer systems and risk analysis; design of the information security systems; mechanisms for the adaptive security control in distributed computing systems; the security policy development for the computer systems and networks.

Pavlo Anakhov: Senior engineer of Department of infrastructure systems at National Power Company "Ukrenergo", Kyiv, Ukraine.

Born on May 26, 1961. M. Eng. (1991) from O. S. Popov Odessa National Academy of Telecommunications, M. Sc. (2007) from graduate school of National Academy of Sciences of Ukraine.

Major interest: research of IT networks; monitoring and improving the sustainability of the information and telecommunications systems; limnology, oceanology and hydroelectric power; development of measures to protect against hazards.

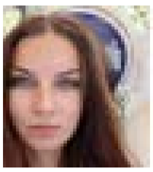
Viktoriia Zhebka: Professor of Software Engineering, State University of Telecommunications. Doctor of Engineering. Specialist (2012), Candidate of Technical Sciences (2015), Doctor of Technical Sciences (2021) from the State University of Telecommunications; Associate Professor (2019).

Main interest: research of IT networks; monitoring and improving the sustainability of information and telecommunications systems; development of measures for protection against dangers; machine learning.

Vladislav Kravchenko: Director of the Educational and Scientific Institute of Telecommunications of the State University of Telecommunications. Candidate of Technical Sciences, Associate Professor.

Born on June 22, 1993. Master of Science (2015), Candidate of Technical Sciences (2018) from the State University of Telecommunications, Associate Professor (2021).

Major interest: mobile communication systems, 4th and 5th generation networks, Internet of Things, video information systems.



Aksieniia Shtimmerman: Teather of the System analysis Department in the State University of Telecommunications, Kyiv, Ukraine.

Born on December 11, 1978, MS (2001) from Odessa State Academy of Refregerations, MS (2010) from Odessa I.I. Mechnikov National University of Ukraine.

Major interest: research of technology and concepts of Brain-Computer Interface, artifical intelligence, optimization signal processing, decides the algorithms with the objective of proper control BCIs.

Valerii Zavgorodnii: Head of Department of the Information Technologies and Design of the State University of Infrastructure and Technologies, Ukraine, Kiev, Doct. of Sc.

Born on May 25, 1982. PhD (2013), Assoc. Prof. (2015) of Department of Systems Software, Doct. of Sc. (2020) from the State University of Telecommunications.

Major interests: information technologies, databases, decision support systems, introduction of Information and communication technology in the educational process.

Yurii Bazaka: Senior lecturer of Department of Information Systems and Technologies of the National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", PhD.

Born on Apr 24, 1992. PhD (2021) from West Ukrainian National University;

Major interests: software testing, automation testing, testing of distributed systems, automation tests of microservices

How to cite this paper: Vadym Mukhin, Pavlo Anakhov, Viktoriia Zhebka, Vladislav Kravchenko, Aksieniia Shtimmerman, Valerii Zavgorodnii, Yurii Bazaka, "Protecting Hybrid Information Transmission Network from Natural and Anthropogenic Hazards", International Journal of Computer Network and Information Security(IJCNIS), Vol.14, No.5, pp.1-10, 2022. DOI:10.5815/ijcnis.2022.05.01