Cyber attacks cascading effects simulation for Ukraine power grid

Oleksii Novikov [1], Georgy Vedmedenko [1], Iryna Stopochkina [1], and Mykola Ilin [1]

[1] *National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Peremogy ave., 37, Kyiv, 03056, Ukraine*

Abstract

The paper substantiates mathematical models that can be computationally suitable for cascade effects modeling in the networks of critical infrastructure objects. An interpretation of SIS and Motter-Lai models in the case of damage caused by cyberattacks in networks of critical infrastructure in the field of the energy sector is considered. The improvements have been made to the Motter-Lai algorithm. This improvement allows us to take into account the volatile nature of attack success, which depends particularly on the cyber security level of critical infrastructure objects and cyber security awareness of the staff. Data on the structure of the energy network of Ukraine and data on a successful attack that caused wide failures (2015, Ivano-Frankivsk region, Ukraine) were used. The load parameters of network nodes were calculated. The conclusions about the nature of the dynamics of the network connectivity coefficient depending on the overload factor were made. The parameters of the models were adjusted using the known data about Ivano-Frankivsk cyberattack history. The software was developed using Python NetworkX. An experiment showed the suitability of the selected models for predicting cascade blackouts caused by cyberattacks. Also, it was shown that the attack has a main impact at the first stage of its development, then the growth of the damaged nodes number became less active. The developed software can be used for the prediction of infrastructure behavior under cascading effects.

Keywords

Complex networks, critical infrastructure, cybersecurity attacks, cascade effect, SIS model, Motter-Lai model.

1. Introduction

The applied relevance of the problem is determined by the need to predict situations caused by cyber attacks in the networks of critical energy infrastructure. For this purpose, it is expedient to determine indicators of network resistance to the harmful influences.

A computer simulation may be a good solution for numerical assessment of criteria for assigning objects to critical infrastructure [1] (in particular, the severity of possible negative consequences of disruptions; duration of elimination of consequences, and further negative impact on other sectors) and for calculation of relevant network indicators. This paper substantiates the use of models that allow modeling and assessing the effects of harmful effects on energy facilities, and predict the duration of the elimination of the consequences and the extent of negative impacts, using the results of theoretical and applied research infrastructures of other countries [2-5]. The algorithm, which works on the basis of the Motter-Lai (M-L) model, has been improved, which makes it possible to take into account the probabilistic nature of object failures caused by malicious interference. The software was developed, a computational experiment was performed on the example of the energy network of Ukraine.

XXI International Scientific and Practical Conference "Information Technologies and Security" (ITS-2021), December 9, 2021, Kyiv, Ukraine
EMAIL: o.novikov@kpi.ua(O.Novikov); hopotion@gmail.com(G.Vedmedenko); irst-ipt@lll.kpi.ua (I.Stopochkina); m.ilin@kpi.ua (M.Ilin)
ORCID: 0000-0001-5988-3352(O.Novikov); 0000-0002-4759-9183(G.Vedmedenko); 0000-0002-0346-0390(I.Stopochkina); 0000-0002-1065-6500 (M.Ilin)


2. Relation of critical infrastructure and networks

Any actual country infrastructure consists of networks of different type (heterogenous) objects, some of which, may play an important role in the overall structure of the system, compared to others. The order in which the infrastructure is classified as critical depends on the specifics of the subject area of this structure, its geographical location, the number of objects (network nodes) for which the structure is the supplier of a resource, and so on.

One of the most important areas of critical infrastructure research is the modeling and study of failures and critical situations. With the continuous improvement of information technology, the problem of possible cyber attacks aimed at these structures is very relevant, respectively, deserves great attention to modeling such situations, developing principles of counteraction to them, researching the network's propensity to attack, and more. It is possible to use methods of complex networks investigation to solve these problems.

2.1. Critical infrastructure of Ukraine

Critical infrastructure is a part of the state infrastructure, which is a set of physical or virtual systems and tools important to the state in the sense that their failure or destruction can lead to detrimental consequences in the field of defense, economy, health, and security of the nation.

Critical objects are those that can have the most negative impact on the economy, a key resource, or the entire infrastructure.

The sectors of critical infrastructure of Ukraine include [1] fuel and energy sector with subsectors of electricity, oil industry, gas industry, nuclear energy; information sector with subsectors of information technologies, telecommunications; sector of life support systems (subsector - utilities); sector of the food industry and agro-industrial complex; health sector; financial sector; transport and postal sector (aviation and industry, road and urban transport, rail transport, sea and river transport, postal services); industry sector (chemical industry, metallurgy industry, defense industry, space industry); civil protection of the population and territories; ecological safety.

There are four categories of criticality, which include critical infrastructure.

The first category is especially important objects of national importance, significant impact on other critical infrastructure and disruption of which will lead to a crisis of national importance. Electricity grid facilities fall into this category because large-scale power grid critical situations typically affect a large percentage of the population.

The second category is vital objects, the dysfunction of which will lead to a crisis situation of regional importance.

The third category is important objects, the dysfunction of which will lead to a crisis situation of local significance.

The fourth category is the necessary objects, the dysfunction of which will lead to a crisis situation of local significance.

The criticality category of a critical infrastructure object is determined based on the analysis of the level of the negative impact that a person, society, environment, economy, national security, and defense capabilities of a country may suffer due to disruption or cessation of infrastructure functions [1].

However, it should be noted that there are critical infrastructure facilities that are particularly important but may be subject to a number of cyber attacks. Exploring the effects of these attacks, especially with regard to the cascading effect, is important for planning countermeasures and understanding the vulnerabilities of relevant critical infrastructure.

2.2. Cascading effects in networks

An important phenomenon in networks during critical situations caused by external disturbances is the phenomenon of cascading damage in the network when damage or disabling of a single object or several nodes of the network leads to the fact that successively (or implicitly) connected with the affected node objects also lose their ability to work. The process can be repetitive from node to node, and in this case, if the network is sufficiently vulnerable to interference and external disturbances, the cascade effect can contribute to a very large total damage to the network and, consequently, lead to a global crisis.

There are still many examples of the cascade effect in existing known network-like structures: sudden epidemiological situation dissemination in a short period of time (a week or even a few days, depending on the topology of the network and the nature of the disease); the dissemination of some important information over the Internet. The most important and interesting for us example of the cascade effect, which will be studied in this paper, is the gradual disconnection of individual infrastructures or sets of infrastructures from the general network of the country due to the sudden failure of network nodes. This type of cascade shutdown is actually very dangerous for the country, because, for the most critical situations, when significant network infrastructures are damaged, the speed of the cascade effect can be very fast or even increase over time. Respectively, to prevent negative effects it is necessary to perform fast actions. The speed of the possible cascade effect in networks is determined by the general condition and topology of the network at the time of damage, the significance of the first damaged nodes, the nature of the external disturbance that led to the critical situation, and so on.

It should also be noted that the nature of the reason for disconnection of the infrastructure network of the country can be different - damage can occur due to direct exposure to external factors (natural conditions, cataclysms), or probably the most common type of disturbance, malicious interference, and cyber attacks on certain information structures of these networks, which leads to their actual disconnection or damage. Currently, the malicious type of disturbance is more important and dangerous, because, compared to natural disturbances, attacks on infrastructure, planned by hackers are usually difficult to predict and, accordingly, to prevent them.

A well-known example of a natural cascade effect is the famous blackout in Italy [4], which took place in 2003 and, in addition to Italy itself, also had an effect on neighboring countries such as Switzerland, France, Austria, and Slovenia. As a result of natural phenomena, the main power transmission line between Italy and Switzerland was destroyed, which led to a sudden overload of voltage at the respective stations of both countries. Even attempts at mitigation measures, which were soon carried out by staff at the relevant infrastructure facilities, did not yield significant results, and over time the next power line was cut off, which in turn led to cascading power outages in Switzerland. According to the disconnection, the transmission lines connecting the Italian infrastructures with those in France were also congested, causing a gradual next wave of disconnections.

A smaller but at the same time equally important example of cascading outages was the blackout in Ukraine in 2010 [7], caused by a planned cyber attack on a set of individual infrastructure objects of the country.

Thus, the problem of cascading outages in the country's infrastructure networks plays a very important role in the study of possible critical situations of a global nature. Such situations usually cause very great damage to the country, so their research, as well as research into methods of combating these injuries, is of considerable interest to this day.

This paper deals with a simulation of cascade effects for the power supply grid of Ukraine because at the moment appropriate works were not found among the existing in open access.

3. Models for cascading effects in networks of objects

Modeling of cascade effects, prediction of the corresponding consequences, and calculation of concomitant indicators were performed by a number of researchers.

In the article [6] the Motter-Lai model of the cascade process of blackouts in the critical infrastructure network was proposed. The model uses topological facilities of investigated network and allows to simulate blackout process taking into account a possibility of an impact on all set of network nodes, but not only on adjacent. The main idea of the model is the investigation of the resulting connectivity of the network at the finish of the cascade blackout process.

In the article [8] the question of assessment and cascading failures effects mitigation was considered. The authors propose the method of risk assessment, which takes into account dependencies between infrastructures.

In the article [9] the authors investigate the cyber attacks cascading effects on Secure water treatment plant and Water Distribution system. They take into account an interdependency of critical infrastructure subsectors and objects. They propose an attacker and attack models and give invariants of normal processes for these objects, and anomaly deviations. Authors use program tools for attack modeling and experimental study of the cascading effects.

The algebraic approach for cascading and interactional effects imitational modeling is given in [10].

The cascading effects in different network topology complex systems were investigated in [11]. The authors use a graph-based approach and give the ratios of important indexes, the set of models were compared (in particular, Watt's model, tree-based analytical approach, Newman model, and others). It was grounded, that SIR-like epidemiological models can be used for cascade effects simulation in different networks.

In paper [12] the questions of robustness against failures and attacks were discussed. The focus is made on statistical mechanics for network dynamics, which requires to have a lot of data to investigate the network evolution.

In paper [13] the topological structure and robustness of the electric power grid were investigated. Some metrics were introduced for the assessment of effectiveness and resilience. The calculation of these metrics can be used for obtaining input parameters for other models.

In [14] the structural vulnerability of the North American Power Grid was discussed. Authors say that the network is robust for most kinds of perturbations.

In [15] authors present a new model for dynamics of failure cascade spread. The model takes into account delays of interaction between nodes. Also, the authors consider the question of damage mitigation, which is the advantage of the work.

The paper [16] deals with artificially created networks, in particular, ER random graphs and scale-free networks. The authors consider the random node removals strategy and study an example of Internet network.

Analyzing the advantages and disadvantages of the models, listed before, we can conclude, that a sufficient number of proposed models use an extensive set of parameters, that have a great impact on the results of the simulation. So, to have adequate results, we need to have the possibility to identify all these parameters and values for a concrete attack situation. But it is not possible to perform in the most number of cases because of uncertainty and fuzzy features of existing attacks on power grid objects and lack of observations. Because of these reasons we have decided to use such models that operate with parameters that are possible to be obtained in practical cases, so we have chosen a Motter-Lai model and SIS model from SIR-like models family.

3.1. Mathematical models that were used

Let M is investigated network. For the network nodes, we can obtain the values centrality measures using the formula:

$$B(i) = \sum_{st} \frac{\sigma_{st}(i)}{\sigma_{st}}, \quad (1)$$

where i is the current network node, $\sigma_{st}(i)$ is the number of the shortest paths between s and t nodes, that pass through the selected node i, $\sigma_{st}(i)$ is the general number of shortest paths between nodes s and t in the whole network. For each network node we introduce the boundary load factor of the node:

$$c_i = (1 + \alpha)b_i, \quad (2)$$

where b_i is the calculated load factor of the node in the network (Betweenness centrality, BC), and value $\alpha \geq 0$ is the coefficient of stability of the node, which plays the role of an indicator of the allowable overload of the i node.

The algorithm of cascade shutdowns of Motter-Lai is presented in the following form:

1. Delete the attacked node or set of network nodes, and the corresponding connections, recalculate b, and obtain $b`$.

2. Check the overload condition on all nodes: $b` > c$? If true then delete the node. If no nodes are deleted then go to step 4.

3. Return to step 1.

4. Get a modified network $M`$ as a result of damage. Calculate G – coefficient of final network connectivity after cascade effect:

$$G = \frac{N_{after}}{N}, \quad (3)$$

where N is the general number of nodes in M, and N_{after} is the number of nodes in the most connected component of the resulting graph $M`$.

Epidemiological models have a large number of possible uses, and one of them may be the modeling of the country's electricity grid. It is possible to describe such a system in terms of these models, namely, using the SIS model. Because we are interested in how much the original network can be damaged, we assume that the disabled nodes can no longer be restored, and thus can no longer return to work in one experiment. However, it is possible that if the system is degraded for a longer period of time, there may be situations in which the network continues to be damaged, but some of its nodes are restored and returned to working order.

Based on the above considerations, it was decided that the SIS model and M-L model will be used for the study, which also allows to compare the results of these models and identify possible agreement between them.

SIS model is a modification of the well-known epidemiology SIR model. This model differs from the previous one in that instead of three states (susceptible, infectious, recovered) there are only two states (susceptible, infectious). Such a model has been proposed to describe situations in which, in principle, an object cannot receive "immunity" (this is typical for most APT attacks on critical infrastructure objects). The model equation is:

$$\begin{cases} \frac{ds}{dt} = -\frac{\beta s_i}{N} + \gamma i; \\ \frac{di}{dt} = \frac{\beta s_i}{N} - \gamma i, \end{cases} \quad (4)$$

where variables s and i point to a number of objects in “susceptible” and “infected” states accordingly, and β shows the speed of attack propagation or attack effect cascade propagation, and γ parameter shows the recovery speed for a typical object (node).

The total number of objects remains the same throughout the experiment. An alternative simulation model for this investigation can be a cellular automate, however, for large volumes of the data, the computational complexity of its work algorithm can be an obstacle.

3.2. Implementation of models

When modeling such critical situations that take place in real life, it is also necessary to take into account external factors that can in some way contribute to a particular behavior of the model in different situations. For the studied situation, we deal with large and complex systems as the country's power supply grid. There may be a large number of additional factors of various nature: the general condition of the station equipment, its quality, nature of external disturbances (cyber attacks or natural disasters), staff status and critical situation readiness, the human factor, etc.

For the SIS epidemiological model, the possible factors are determined by the specific choice of the coefficients β and γ, but for the simulation model M-L it is not possible to specify such an impact on the network.

Based on these considerations, several adjustments and modifications were made to the simulation model to improve the accuracy of the experiment and increase its generality: in addition to the allowable overload factor α, the probabilistic nature of the object shutdown was exceeded. Thus, we have the opportunity to improve the experiment by adjusting the probability value. For example, during an attack, realizing that staff was not prepared for this, and there is an external force from the attacker, which contributes to the deterioration of the situation in real time, we can assume that the value of the shutdown probability for this case will be close to one.

So, we propose to implement the modification into the classic algorithm: removal is carried out with a certain probability,

$$P = f\,(security\ status, staff\ readiness, attack\ type) \tag{5}$$

That means that if the node will be seriously damaged depending on some factors, that have to be assessed by the expert method. Value P may be determined as some average for all nodes, or for each node individually.

4. Cyberattack on the electricity network of Ukraine in 2015

On December 23, 2015, the Ukrainian regional electricity distribution company (Kyivoblenerho, Ivano-Frankivsk region) announced the disconnection of services to consumers. The cyberattack affected additional parts of the distribution network and forced operators to switch to manual mode. The failure was due to an attack that allowed attackers to remotely control the SCADA system [7]. The attack was carried out on three independent regions of the country with a short period of time between them: Ivano-Frankivsk, Kyiv and Kyiv region and Chernivtsi region were affected. The attack resulted in several power outages in different parts of the country, causing a large number of consumers to lose electricity in various areas. This situation is used to build software models (in particular, the selection of constants), and verify their adequacy.

4.1. Initial data processing

To investigate the cyberattack effect, the map of the electricity grid of Ukraine, which was obtained from the official site of the Ministry of Energy, was used (Fig.1).

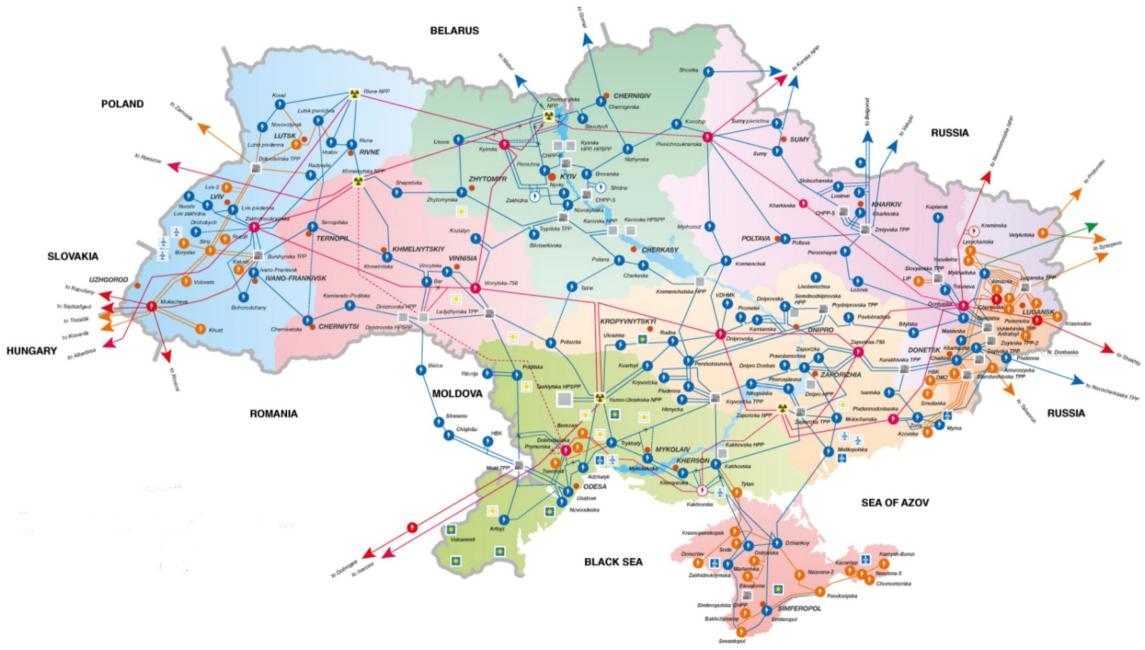

Figure 1: Integrated power system of Ukraine with the main objects

The analysis and processing of initial data for their preparation for use in a specific software implementation were carried out:

1. Nodes that do not affect the overall structure and integrity of the network, such as the Livoberezhnaya distribution station in the Dnipro region, have been ignored - it is easy to see that these nodes have no connections to other nodes in the network, or at least the connections are not listed in the map. We suggest that this node does not affect the results of the study.
2. We have ignored those connections between nodes which: a) do not currently exist (connections are in the planning stage, but in fact, they do not exist yet), or b) are duplicating edges (for the number of connections between nodes greater than one). Multiple edges also do not affect the study, because we are interested in the actual connectivity of individual nodes.
3. It was decided that the network is presented by an undirected, unweighted graph.

After the final formalization of the source data, a software implementation of the described network was created. The map was marked, a matrix of network adjacencies was generated, and, using a software package for working with Gephi 0.9.2 graph models, the final software interpretation of the source network was created (Fig.2).

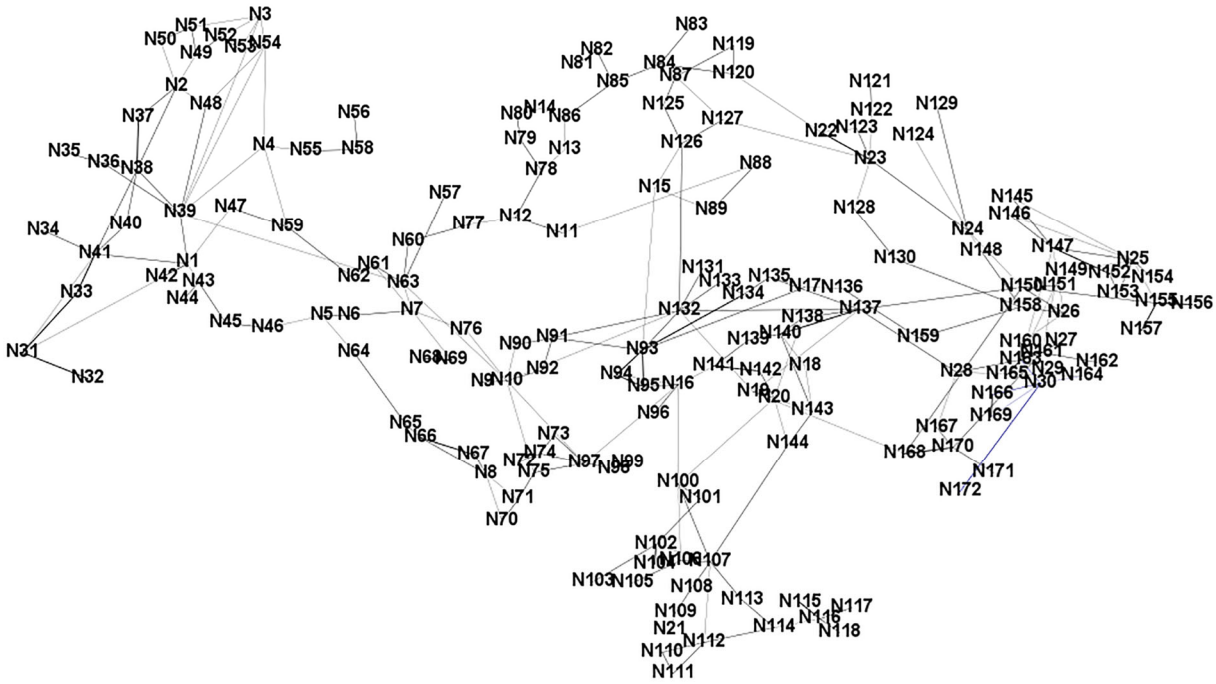

Figure 2: Graph of the Ukraine power grid made with Gephi software.

In the power industry, generators are those infrastructure objects that are suppliers of electricity (for example, nuclear power plants, thermal power plants, etc.). Distributors are those infrastructure objects that do not generate electricity - they do not supply energy by themselves, but are a link in the transfer of resources.

Based on these definitions, a network of 30 generators and 142 distributors was obtained (we have a total of 172 nodes).

The following approach was developed and used for the Motter-Lai simulation model: 1) the load factors (BC) were calculated for all network nodes. The software package NetworkX Python for obtaining the factors of the network was used. The nodes for the following steps were selected based on the obtained factor values (the most important values are shown in Table 1); 2) the distribution of nodes by regions was performed for identifying node classes that possibly were shutdowned first in a given area; 3) after the classification of nodes for these areas and the calculation of the values of the coefficients BC, in each area were selected those nodes whose BC values are the largest.

Table 1
Nodes classification and load factor values (normalized on the segment [0, 1] and non-normalized)

Ivano-Frankivsk (I-F)			Kyiv			Chernivtsi		
Node	BC	Normalized	Node	BC	Normalized	Node	BC	Normalized
1	1216.4	0.083	12	1019.6	0.070	5	372.7	0.026
40	0	0	13	373.9	0.026	6	471.2	0.032
41	692.8	0.048	14	57.3	0.004	45	71.7	0.005
42	0	0	57	0	0	46	54.7	0.004
43	381.7	0.026	77	1046.4	0.072			
44	0	0	78	791.1	0.054			
			79	171.8	0.012			
			80	61.1	0.004			
			81	0	0			
			86	444.9	0.031			

A set of the most important nodes has been identified: for Ivano-Frankivsk region – node 1, Burshtyn thermal power plant; for Kyiv and Kyiv region – node 77, Bila Tserkva distribution station; for Chernivtsi region – node 6, Dniester hydroelectric power plant. The initial number of successfully attacked nodes is 3, and the number of «susceptible» nodes is 169.

For SIS epidemiology model possible options in the development of the attack are determined by the specific choice of coefficients β and γ, however, for the imitational M-L model there is no possibility to determine such impact on a network, therefore, adjustments were made: in addition to the coefficient of acceptable overload α the probability of disconnection of the object in case of exceeding the threshold was also introduced. For example, during an attack, in the case of untrained personnel, and low-security level of the object, it can be assumed that the value of the probability of shutdown, in this case, will be close to 1. Taking into account the introduced adjustments, a software implementation was developed.

4.2. The results of simulation of cyber attack cascading effects

Based on the processed initial data, the behavior of the network at different parameter values was investigated. Regarding the M-L model, there were cases when the number of deleted nodes increases and the network connectivity parameter G decreases with increasing overload parameter α (Fig. 2). This behavior is associated with the so-called "islanding" effect [4].

Having built both models, we use the processed initial data and investigate the behavior of the network at different values of parameters (Table 2).

From the table of results we see that in some cases, as the parameter of congestion of the node α increases, the number of deleted nodes increases, and the parameter of network connectivity G decreases. For some sets of parameters in the network, it is possible that it is divided into several separate subgraphs ("islands"), not related to each other. The stages of the evolution of the network, obtained on the basis of the adjusted algorithm, are shown in Fig. 4.

Epidemiological model of SIS is given by a pair of differential equations (4) and in the general case does not take into account the relationship between nodes. To simulate this cyber attack we have to set initial conditions for solving the system: the number of "damaged" will be 3 and the number of "favorable" - 169.

The results of the SIS model for this critical situation are shown in Table 3 and generalized in Fig.5.

Table 2
Results of the M-L model for this critical situation

P	α	# of nodes	G	P	α	# of nodes	G
	0.05	23	0.698		0.05	36	0.25
	0.10	21	0.75		0.10	38	0.599
0.50	0.15	31	0.628	0.65	0.15	33	0.674
	0.20	34	0.598		0.20	21	0.738
	0.25	15	0.726		0.25	36	0.599
	0.05	31	0.645		0.05	47	0.221
	0.10	25	0.738		0.10	26	0.645
0.55	0.15	36	0.575	0.70	0.15	35	0.599
	0.20	31	0.622		0.20	21	0.715
	0.25	33	0.605		0.25	33	0.616
	0.05	38	0.319		0.05	46	0.221
	0.10	32	0.581		0.10	43	0.558
0.60	0.15	24	0.744	0.75	0.15	35	0.639
	0.20	34	0.628		0.20	31	0.645
	0.25	29	0.605		0.25	29	0.669

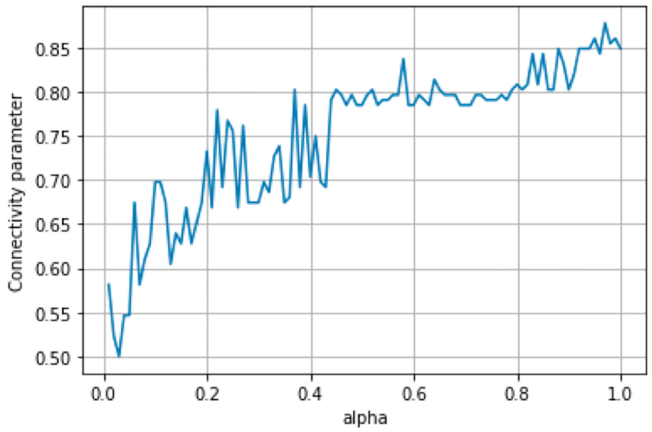

Figure 3: An example of network connectivity G dynamics ($0 < \alpha < 1, \Delta\alpha = 0.01$)

From the Table 3, for this model, we see that in general the results obtained from it are different, but for satisfactory parameter values, we have a certain analogy. This is due to the choice of parameters, which, again, depends on the nature of the network.

Table 3
Results of the SIS model for various parameters values

β	γ	# of nodes	β	γ	# of nodes
0.45	0.30	57	0.50	0.30	85
	0.35	38		0.35	71
	0.40	18		0.40	57
0.55	0.30	78	0.65	0.30	92
	0.35	62		0.35	79
	0.40	46		0.40	66
0.60	0.30	85	0.70	0.30	98
	0.35	71		0.35	85
	0.40	57		0.40	73

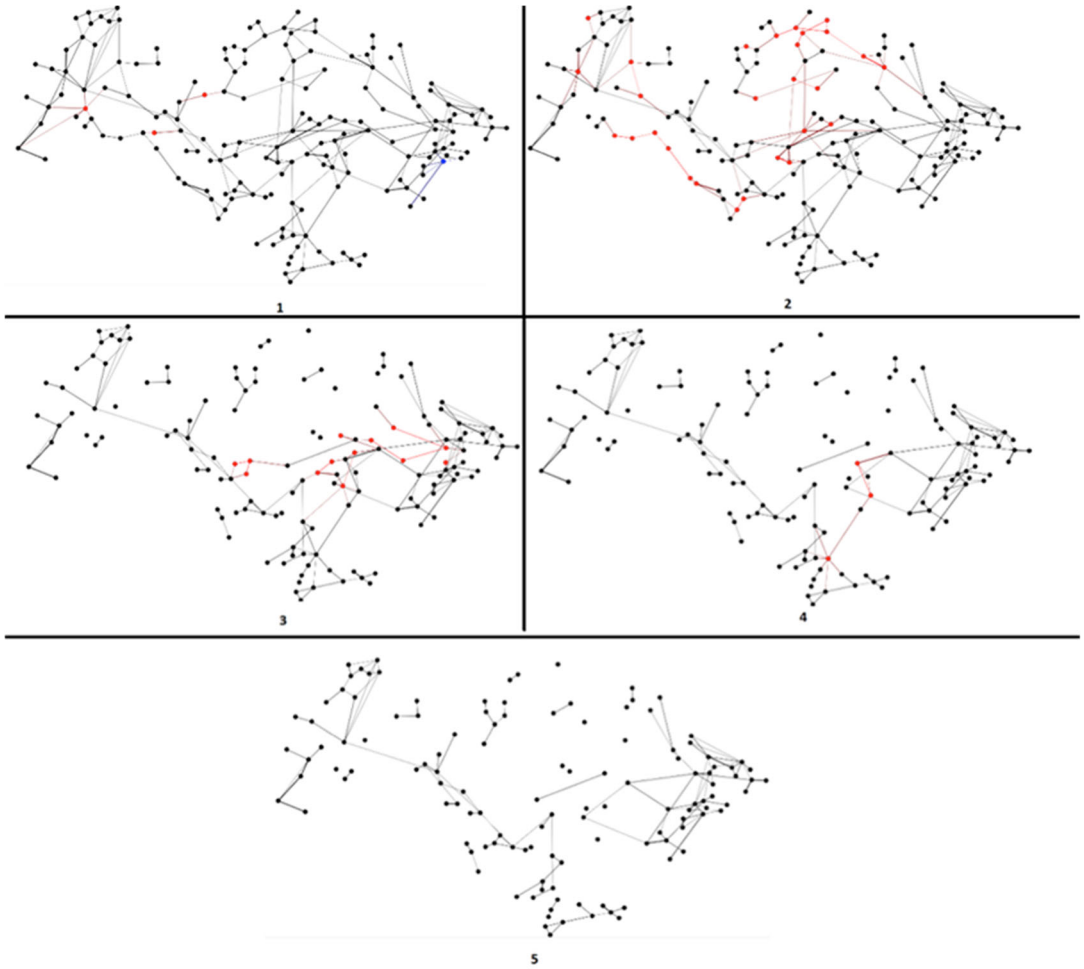

Figure 4: Evolution of the network in time based on the M-L algorithm ($\alpha = 0.05, \mathrm{P} = 0.75$), steps 1-5.

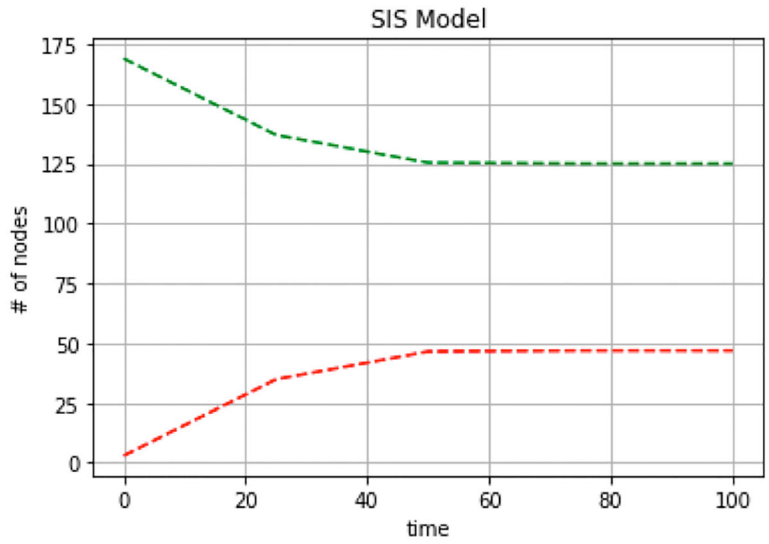

Figure 5: Number of active (declining curve) and disabled (growing curve) nodes in the SIS model ($\beta = 0.55, \gamma = 0.40$)

4.3. Critical nodes damaging effect

After performing the computational experiment and results analysis it was found that both models were suitable to predict an evolution of real situations in general. This gives reason to believe that the obtained software implementation can be used for further research in other critical infrastructures.

Consider node number 10, Mykolaiv region. According to the table of centrality coefficients of nodes (BC coefficients), this node is the busiest node of the entire network, and therefore, the most critical node in the infrastructure. This is still obvious - as can be seen from the map of initial data (Fig. 1), the selected node for the network in some sense combines two large clusters of nodes in the western and eastern parts of the country. It follows that this node is important for the network in terms of its connectivity, so its characteristics research is of great interest.

So, using the built models we suppose selected node was attacked, and then we have the following results (Table 4).

Table 4

Results of the M-L model when removing the #10 node

P	α	# of nodes	G	P	α	# of nodes	G
	0.05	34	0.302		0.05	41	0.233
	0.10	20	0.483		0.10	28	0.535
0.50	0.15	23	0.343	0.60	0.15	26	0.343
	0.20	23	0.355		0.20	25	0.477
	0.25	23	0.372		0.25	22	0.343
	0.05	34	0.319		0.05	34	0.297
	0.10	28	0.308		0.10	25	0.343
0.55	0.15	21	0.372	0.65	0.15	23	0.343
	0.20	21	0.552		0.20	24	0.500
	0.25	23	0.360		0.25	29	0.331
	0.05	38	0.273		0.05	36	0.262
0.70	0.10	33	0.319	0.75	0.10	36	0.308
	0.15	36	0.326		0.15	35	0.349
	0.20	30	0.337		0.20	27	0.331
	0.25	32	0.326		0.25	29	0.337

Analyzing the results obtained using the simulation model, we see that on average the total number of damaged nodes does not differ much from the previous example, although the initial parameter values are different. It follows that this node is actually very important for the network because its removing leads to significant damage to the network. Together with the islanding effect, such cases as for parameters $P = 0.60$ and $\alpha = 0.05$ are allowed, when we receive damage of about 20 percent of the whole network.

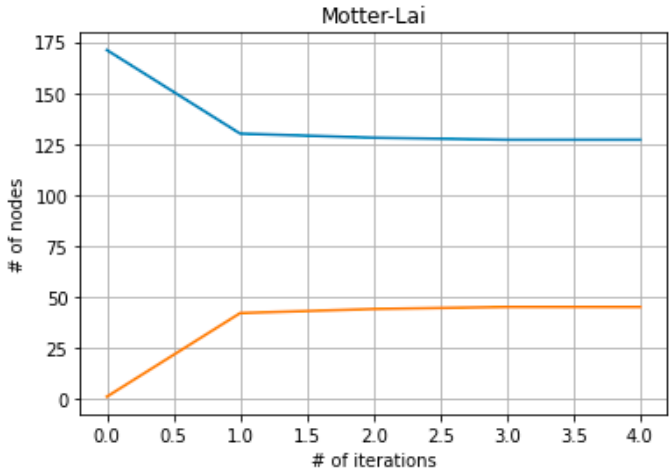

Figure 5: Evolution of the number of operational and disabled nodes ($P = 0.60, \alpha = 0.05$)

In addition, Fig. 5 clearly shows that a significant amount of damage in the network occurs after the removal of a critical node, i.e. after the first iteration. The number of damaged nodes in subsequent iterations is quite small, so the effect of the next cascading damage is not very large. This is due to the fact that the abrupt removal of a critical node in the network suddenly recalculates the load of all remaining nodes, which leads to the simultaneous failure of many adjacent, and not only, structures. The further situation becomes more stable.

Using the SIS epidemiological model, we mean the following - since the model does not work with every certain network node but only with their number and the corresponding required coefficients, we believe that the value of the "infection" rate should be higher than usual. The appropriate results are shown in Table 5.

Table 5
Results of the SIS model for one critical node

β	γ	# of nodes	β	γ	# of nodes
0.60	0.40	57	0.70	0.40	73
	0.45	42		0.45	61
	0.50	29		0.50	49
0.65	0.40	66	0.75	0.40	80
	0.45	52		0.45	68
	0.50	39		0.50	57

5. Conclusions

The selected models make it possible to effectively predict the behavior of the network when implementing harmful effects that lead to the failure of the energy supply object, and the subsequent cascading effect of failure in the network. The models agree well with the forecast results and real cyberattack data, which gives grounds to consider them suitable for an approximate estimate of the number of damaged nodes in the network.

The M-L model allows us to evaluate the results from the standpoint of simulation modeling of the behavior of objects in the network. The model allows taking into account such factors as the value of the allowable overload of the object and the probabilistic nature of disconnections.

The SIS model makes it possible to estimate the number of active and the number of non-functioning nodes in the network. The experiment showed that the vast majority of failures of child nodes occurs in the first time period after the failure of a critical node. Then the effect of failures becomes more stable, which gives reason to believe that with the loss of control over the node in the first hours of the accident,

in the next steps the cascade effect does not depend so much on the speed of recovery actions. The topology of the Ukraine power grid network shows significant robustness for damaging even critical nodes. Amplification of the object's features that affect the probability of disabling a node may improve the situation also.

Further research can be related to the analysis of networks of critical infrastructure from the standpoint of negative impacts in the supply chain, which occur when economic and other non-technical relations are disrupted.

6. References

[1] Cabinet of Ministers of Ukraine. Resolution No. 1109 — Some Issues of Critical Infrastructure Objects, October 9, 2020 [in Ukrainian]. URL: https://zakon.rada.gov.ua/laws/show/1109-2020-п#Text.

[2] P. Chopade and M. Bikdash, Critical infrastructure interdependency modeling: Using graph models to assess the vulnerability of smart power grid and SCADA networks, 8th International Conference & Expo on Emerging Technologies for a Smarter World, 2011, pp. 1-6. doi: 10.1109/CEWIT.2011.6135885.

[3] B. A. Carreras, D. E. Newman, I. Dobson, Thresholds and Complex Dynamics of Interdependent Cascading Infrastructure Systems. To appear as Chapter 5, pp. 95-114, in G. D'Agostino and A. Scala (eds.), Networks of Networks: The Last Frontier of Complexity, Springer Switzerland 2014. doi: 10.1007/978-3-319-03518-5_5.

[4] E. Zio, G. Sansavini, Modeling failure cascades in critical infrastructures withphysically-characterized components and interdependencies, ESREL 2010 Annual Conference, 2010, pp.652 - 661. URL: https://www.researchgate.net/publication/281156637_Modeling_failure_cascades_in_critical_infrastructures_with_physically-characterized_components_and_interdependencies.

[5] A. Blokus-Roszkowska, P. Dziula, Safety Analysis of Interdependent Critical Infrastructure Networks: December, 2019, TransNav the International Journal on Marine Navigation and Safety of Sea Transportation, 13(4): 781-787. doi: 10.12716/1001.13.04.10.

[6] E. A. Motter, Y.-C. Lai, Cascade-based attacks on complex networks, Phys. Rev. E 66, 065102(R). doi: 10.1103/PhysRevE.66.065102.

[7] R. M. Lee, M. J. Assante, T. Conway, Analysis of the Cyber Attack on the Ukrainian Power Grid, March 2016. URL: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

[8] P. Kotzanikolaou, M. Theoharidou, D. Gritzalis, Cascading Effects of Common-Cause Failures on Critical Infrastructures, 2013. doi: 10.1007/978-3-642-45330-4_12.

[9] V. Palleti, S. Adepu, V. Mishra et al., Cascading effects of cyber-attacks on interconnected critical infrastructure, Cybersecurity 4, 8 (2021). doi:10.1186/s42400-021-00071-z

[10] Elie M. Adam, Munther A. Dahleh, On the mathematical structure of cascade effects and emergent phenomena, 2019. doi: 10.48550/arXiv.1911.10376.

[11] A. W. Hackett, Cascade dynamics on complex networks, Ph.D. Thesis, University of Limerick, 2011. URL: https://pdodds.w3.uvm.edu/teaching/courses/2009-08UVM-300/docs/others/2011/hackett2011b.pdf.

[12] R. Albert, A.L. Barabasi, Statistical mechanics of complex networks, 2002. Rev. Mod. Phys., Vol. 74, pp.47–97. doi: 10.1103/RevModPhys.74.47

[13] S. Arianos, E. Bompard, A. Carbone, F. Xue, Power grid vulnerability: A complex network approach, Chaos 19, 013119 (2009). https://doi.org/10.1063/1.3077229.

[14] R. Albert, I. Albert, G.L. Nakarado, Structural vulnerability of the North American power grid, 2004, Phys. Rev. E 69, 025103(R). doi:10.1103/PhysRevE.69.025103.

[15] K. Peters, L. Buzna, D. Helbing et al., Modelling of cascading effects and efficient response to disaster spreading in complex networks, Int. J. Critical Infrastructures, Vol. 4, No. 1-2. doi: 10.1504/IJCIS.2008.016091.

[16] P. Crucitti, V. Latora and M. Marchiori, A model for cascading failures in complex networks, 2004, Phys. Rev. E 69, 045104(R). doi: 10.1103/PhysRevE.69.045104.