UDC 621.391
DOI: 10.15587/2312-8372.2017.112495

Dorogyy Ya.

DEVELOPMENT OF THE APPROACH FOR DESIGNING, MODELLING AND RESEARCH OF CRITICAL IT INFRASTRUCTURE

Запропоновано підхід, який дозволяє розробити точні моделі компонентів критичної IT-інфраструктури та об'єднати їх на базі їхніх залежностей. Цей підхід дає інструмент для створення більш масштабних і складніших взаємозалежних моделей. Застосовуючи певні налаштування, використовуючи різні умови експлуатації, запропонований інструментарій дозволяє вивчити каскадні ефекти взаємозалежності компонентів або цілих систем, провести детальну оцінку їхньої вразливості та здійснити широке планування.

Ключові слова: *критична IT-інфраструктура, гібридний розширений відкритий автомат, рівні абстракції моделей.*

1. Introduction

To date, the creation of critical IT infrastructures is an integral part of the development of key industries that are vital for ensuring the safety and functioning of the society.

The existence of a critical IT infrastructure is closely related to the notion of a critical infrastructure – an infrastructure critical for the state, the abandonment or destruction of which can have a materially negative impact on national security.

Currently, Ukraine is only beginning to develop such global management complexes, although some industries already have developed IT infrastructure, for example, dispatching systems for transport management, energy facilities.

That is why the development of new approaches, methods and algorithms for creating, analyzing, monitoring, ensuring the quality and reliability of operation, the security of critical IT infrastructures is a very urgent problem.

2. The object of research and its technological audit

The object of research is a critical IT infrastructure.

The draft law [1] specifies that a critical IT infrastructure is a set of information and telecommunications systems of the public and private sector that ensure the functioning and security of government strategic institutions, systems and facilities (central and local government bodies, energy, transport, communications systems, banking sector, enterprises, during which activities are used and/or produced hazardous substances, etc.) and the safety of citizens (law enforcement management system and defensive sector, etc.), unauthorized intervention in the operation of which may endanger the economic, environmental, social and other types of security or harm the international image of the state. Critical infrastructures include the financial and energy sectors of the state, the food industry, medicine, manufacturing, transport, water supply, public administration and others.

A critical IT infrastructure must:

– ensure the functioning of environmentally hazardous and socially significant production and technological processes, the violation of the regular mode of which can lead to an emergency situation of anthropogenic nature;

– perform the functions of an information system, the violation (stoppage) of which may lead to negative consequences in the political, economic, social, information, environmental and other fields;

– ensure the provision of a significant amount of information services, partial or complete suspension of which can lead to significant negative consequences for national security in many sectors.

Although each critical IT infrastructure is usually seen as a separate system, all of its systems are strongly interlinked with different levels of interdependence between them. As an example, for the work of the information and telecommunications system (ITS) at the level of the declared quality of service, the uninterrupted operation of the power supply system is required, while the quality of the power supply system itself depends on the stable operation of the ITS information transmission channels. These bi-directional relationships between critical IT infrastructure systems increase their overall performance, but at the same time increase its complexity and sensitivity to various types of attacks [2, 3].

The main problem in this industry is the complete absence of ready-made solutions, methodologies, tools that are suitable for modeling, designing and researching critical IT infrastructures.

3. The aim and objectives of research

The aim of research is development of an approach to designing, modeling and researching critical IT infrastructure.

To achieve this aim, it is necessary to perform the following tasks:

1. To improve the existing mathematical apparatus of open hybrid automata for the study of critical IT infrastructures.

2. To build a simplified model of critical IT infrastructure and explore with its help the proposed approach.

4. Research of existing solutions of the problem

Modeling of interdependence of systems is a new scientific direction, which includes several innovative approaches to modeling. Existing models are analyzed in [4, 5]. Among the most popular are input-output methods, agent modeling and network approaches.

Methods of input-output are based on the V. Leontief theory of economic equality and allow to estimate the integral level of disability (percentage of failure) of infrastructures by using the dependency coefficients (Leontief coefficients). However, these coefficients are difficult to determine correctly, and therefore, as a rule, they are an approximation of a higher level, proceeding from the assumption that the interdependence of infrastructures is related to their economic interaction [6].

Agent modeling (AM) methods consider critical infrastructures as flexible adaptive systems (FAS), that is, as a complex of interacting components, the state of which can change in the learning process. AM methods use a bottom-up design strategy, and therefore various components of the IT infrastructure are represented as standalone agents with their attributes, behavior and decision rules, while the interdependencies arise between them in their interaction [7, 8].

Network approaches usually assume that each infrastructure consists of a number of network components (usually represented as nodes) that form a network, and any existing dependencies are represented as relationships between nodes belonging to different networks [9]. Using of network models to investigate critical interconnected infrastructures makes it possible to perform topological analysis quite easily (i. e., qualitatively describe the existing relationships for any set of components). The disadvantage of these models is a fairly small amount of information for conducting functional analysis. As a rule, such models make it possible to investigate only simplified hypotheses and obtain only basic characteristics of networks and completely lack the ability to investigate complex effects associated with technological aspects of their implementation [10].

There are also a number of other approaches to modeling the interdependence of critical infrastructures. For example, [11–13] presents methods based on Petri nets, stochastic activity networks and Bayesian networks.

At the moment, the approaches presented in the literature are used for various purposes, have their own strengths and weaknesses, but as such, there is no single approach to solving the problem. In addition, the difficulties associated with accessing data through their security and privacy, coupled with the fact that the structure of the critical IT infrastructure becomes more diverse and more complex, makes the problem of checking the interdependence of its components and systems a very nontrivial problem. So, there is a need for further development of approaches to research the interdependence of components, systems and entire infrastructures, and therefore the topic of work is promising.

5. Methods of research

Let critical IT infrastructure C be represented as a set of systems and components Ω. Then, let's present our Ω in the form of extended open cellular automata (EOCA) [14]:

$$\Omega = (D, S, S_0, I, O, Z, L, G, T, \tau, F, SP, P, R, V),$$

where D – a finite set of discrete states of the system (components) of a critical IT infrastructure Ω. The set is divided into the following sets: D_{sf} – set of safe states, D_{cr} – set of critical states, and D_t – set of terminal states; S – a finite set of continuous states of the system (components) of a critical IT infrastructure Ω. The set is divided into the following sets: S_{sf} – set of safe states, S_{cr} – set of critical states, and S_t – set of terminal states; $S_0 \subseteq S \times D$ – a finite set of initial states $s_0 \in S_{sf}$, $d_0 \in D_{sf}$; $I = \Xi \cup \Psi$ – a finite set of inputs, which is divided into: Ξ – set of internal inputs (within one component), Ψ – set of external inputs (between component inputs); O – a finite set of output states.

Notation $(s,d) \in S \times D$ describes the change in the state of a component Ω that has:

- initial state $S_0 \subseteq S \times D$;
- dynamics of changes in states, described by a vector $\phi : S \times D \times I \to R^n$;
- output function $\varphi : S \times D \times I \to O$;
- set of allowed states and inputs $Z \to 2^{S \times I}$;
- $L \subseteq D \times D$ – a finite set of transition marks, including a special symbol †;
- set of conditions $G : L \to 2^{S \times I}$ that initiate the transition between discrete states;
- the reset ratio $T : L \times S \times S$, which resets the input value $s \in S$ before each transition;
- τ – time manager;
- F – distribution of interventions in the operation of components;
- SP – set of specifications;
- P – set of policies;
- R – set of security requirements;
- V – set of vulnerabilities.

The transition is deterministic and occurs under the condition G in the case when, $l \in L \setminus \{†\}$ or probabilistic, in the case when $l = †$. The state value in this case is formed randomly according to the distribution F.

Interactive participants in this model are:

- components (telecommunication, industrial, etc.);
- systems;
- infrastructures;
- operators of critical IT infrastructure systems;
- opponents;
- environment.

Their operation logic is described by sets of specifications SP, policies P and security requirements R.

The environment controls the temporal and spatial aspects of all events in the model and dispatches all changes in states according to τ, using distributions F for this. Distribution provides the ability to create strategies for the failure of available components and is used to solve the problems of simultaneous occurrence of events in critical IT infrastructure and processing.

It is very convenient to represent such model in the form of a directed graph (Fig. 1). Each vertex of such graph represents a discrete state $d \in D$. The edges of a directed graph represent discrete transitions between states. For example, an edge $(d_1, d_2) \in L$ starts at the vertex $d_1 \in D$ and ends at the vertex $d_2 \in D$. Each transition occurs when the condition $G(d_1, d_2)$ is met or accidentally if $L(d_1, d_2) = †$. The ratio T is reset at the end of the transition, when the value of the continuous state changes.

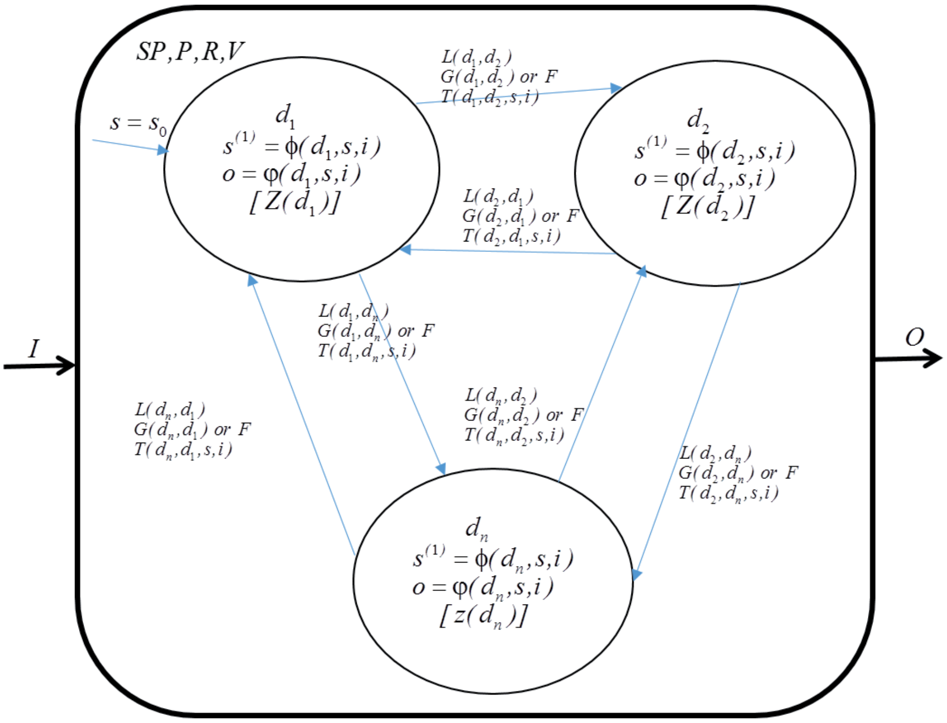

Fig. 1. The model in the form of a directed graph

The simple path (EOCA triggering) consists of a sequence of intervals τ of continuous evolution, which are changed by discrete transitions. The execution begins with some initial state $(d_0,s_0)\in S_0$. The model remains in a discrete state d_i while the continuous state $s_i\in S$ and/or the input value $i\in I$ have valid values Z. At the same time, the output value $o\in O$ is defined as $\varphi(s_i,d_i,i)$. If $s_i\in S$ and/or the input value $i\in I$ reaches the transition condition $G(d_i,d_j)$, then the state change occurs instantaneously, and the value of the continuous state is determined by the ratio T.

Each critical IT infrastructure can be represented as a composition of various EOCAs. Fig. 2 shows the composition of two EOCAs.

ITS EOCA consists of a composition of two elements:

– network operation center;

– network.

Let's describe the model of the network operations center in EOCA terms. The model contains 5 discrete states:

– «Normal» – the state of the normal operation of the network operation center (NOC);

– «Uninterruptible power supply» – the NOC operation state on uninterruptible power supplies in case of absence of current in the electrical network;

– «Cooling errors» – the NOC operation state on in the event of accidents in the cooling system of the equipment;

– «Critical» – the NOC operation state in the event of simultaneous failure of power and cooling systems;

– «Accident» – the NOC operation state, in which further work is impossible due to a failure that occurred.

The model has the following inputs (Fig. 3):

– i_{ps}^{NOC} – NOC power;

– i_{cl}^{NOC} – NOC cooling;

– f_{tech}^{NOC} – availability of technical failures in the NOC.

The occurrence of technical failures is controlled by the distribution F or the system itself.

The transition from the «Normal» state to other states occurs under the following conditions:

– if there is a technical failure $f_{tech}^{NOC}=1$;

– if the level of power supply has fallen below the level of the NOC requirements $i_{ps}^{NOC}<R_0$;

– if the level of coolant supply has fallen below the level of the NOC requirements $i_{cl}^{NOC}<R_0$.

As the time managers in the system are the values of continuous states s_{ups} and s_{cl}. In the case of a power failure, an uninterruptible power system can support the NOC operation $s_{ups}=T_{ups}$.

In the case of a failure of the cooling system, the NOC operation is maintained for some time, equal to $s_{cl}=T_{cl}$.

The model also has three outputs:

– NOC operation state z_{NOC} (z_{NOC} takes 2 values: 1 – NOC performs its functions, 0 – accident in the NOC);

– NOC demand for power supply r_{ups};

– NOC demand for cooling r_{cl}.

Let's consider the following model – the network operation model, which is a variant of the model from [15]. The model has three discrete operating states (Fig. 4):

– «Normal» – the network operates in normal mode;

– «Data transmission failure» – failure of one or more data transmission channels;

– «Accident» – the network has completely refused.

The network model has the following inputs:

– i_l^{NET} – the network operates in normal mode, if there are no failures of data transmission channels, that is $i_l^{NET}=0$;

– i_{noc}^{NET} – the network operates in the normal mode, if the NOC also operates in the normal mode, that is $i_{noc}^{NET}=1$;

– i_{ps}^{NET} – input receives data from the power supply system;

– i_{cl}^{NET} – input receives data from the cooling system;

– i_{pct}^{NET} – input receives data on the number of incoming packets that enter the network.

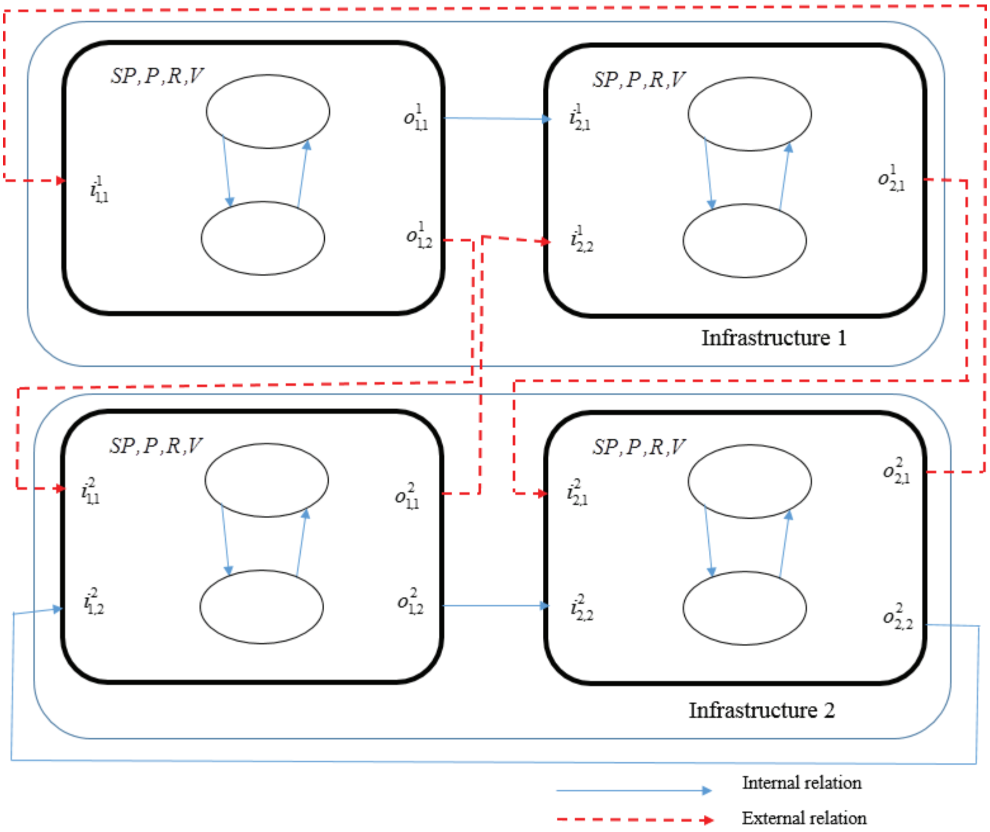

Fig. 2. The composition of automata

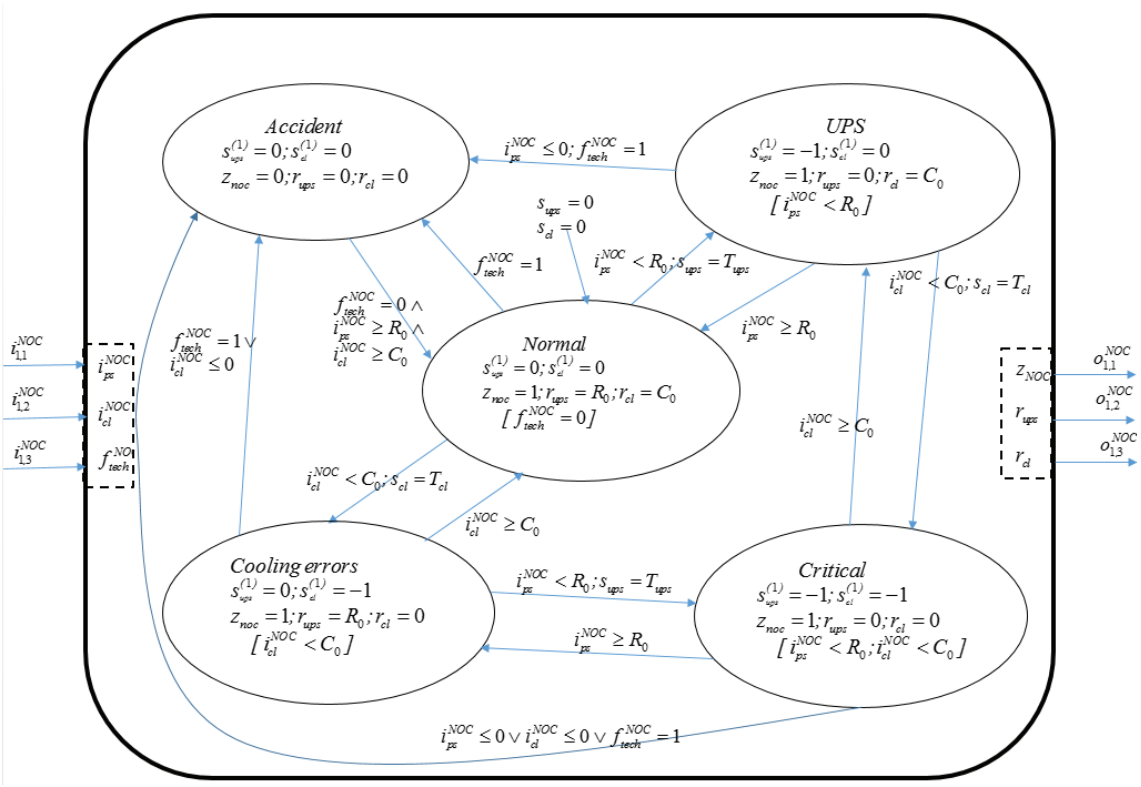
$Accident$
$s^{(1)}_{ups}=0; s^{(1)}_{cl}=0$
$z_{noc}=0; r_{ups}=0; r_{cl}=0$
$i^{NOC}_{ps}\le 0; f^{NOC}_{tech}=1$
UPS
$s^{(1)}_{ups}=-1; s^{(1)}_{cl}=0$
$z_{noc}=1; r_{ups}=0; r_{cl}=C_0$
$[\,i^{NOC}_{ps}<R_0\,]$
$s_{ups}=0$
$s_{cl}=0$
$f^{NOC}_{tech}=1$
$i^{NOC}_{ps}<R_0; s_{ups}=T_{ups}$
$i^{NOC}_{cl}<C_0; s_{cl}=T_{cl}$
$f^{NOC}_{tech}=0\wedge$
$i^{NOC}_{ps}\ge R_0\wedge$
$i^{NOC}_{cl}\ge C_0$
$f^{NOC}_{tech}=1\vee$
$i^{NOC}_{cl}\le 0$
$i^{NOC}_{ps}\ge R_0$
$Normal$
$s^{(1)}_{ups}=0; s^{(1)}_{cl}=0$
$z_{noc}=1; r_{ups}=R_0; r_{cl}=C_0$
$[\,f^{NOC}_{tech}=0\,]$
$i^{NOC}_{1,1}$
$i^{NOC}_{1,2}$
$i^{NOC}_{1,3}$
i^{NOC}_{ps}
i^{NOC}_{cl}
f^{NO}_{tech}
z_{NOC}
r_{ups}
r_{cl}
$o^{NOC}_{1,1}$
$o^{NOC}_{1,2}$
$o^{NOC}_{1,3}$
$i^{NOC}_{cl}\ge C_0$
$i^{NOC}_{cl}<C_0; s_{cl}=T_{cl}$
$i^{NOC}_{cl}\ge C_0$
$Cooling\ errors$
$s^{(1)}_{ups}=0; s^{(1)}_{cl}=-1$
$z_{noc}=1; r_{ups}=R_0; r_{cl}=0$
$[\,i^{NOC}_{cl}<C_0\,]$
$i^{NOC}_{ps}<R_0; s_{ups}=T_{ups}$
$i^{NOC}_{ps}\ge R_0$
$Critical$
$s^{(1)}_{ups}=-1; s^{(1)}_{cl}=-1$
$z_{noc}=1; r_{ups}=0; r_{cl}=0$
$[\,i^{NOC}_{ps}<R_0; i^{NOC}_{cl}<C_0\,]$
$i^{NOC}_{ps}\le 0\vee i^{NOC}_{cl}\le 0\vee f^{NOC}_{tech}=1$

Fig. 3. The model of the operation of the network operation center

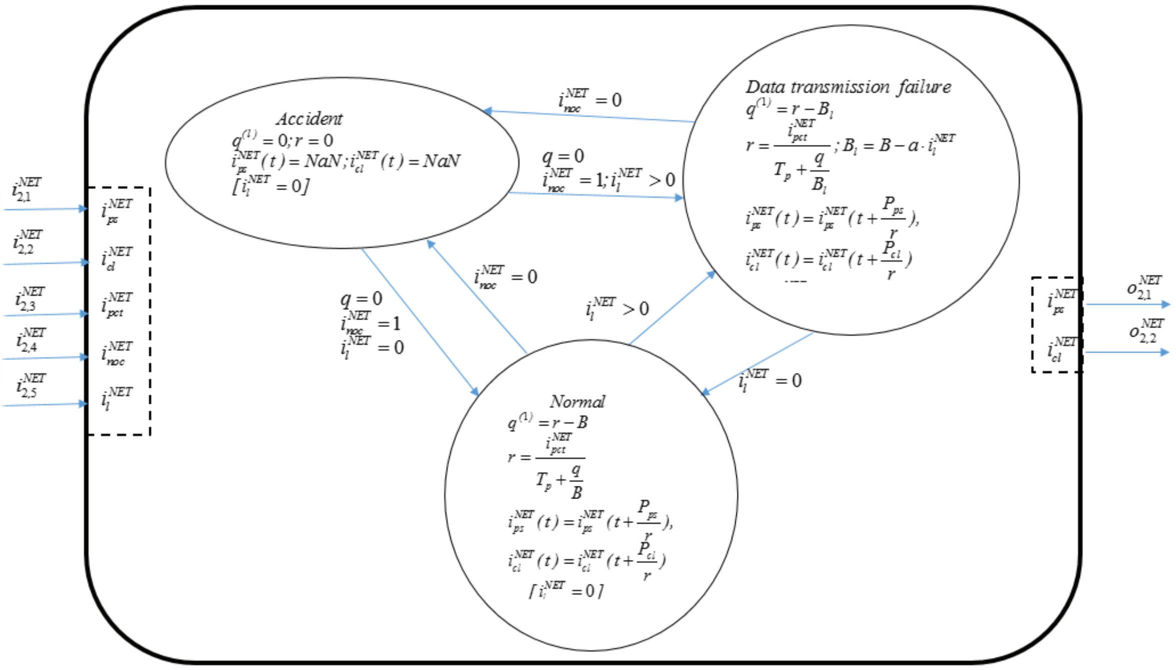
$i_{2,1}^{NET}$
$i_{2,2}^{NET}$
$i_{2,3}^{NET}$
$i_{2,4}^{NET}$
$i_{2,5}^{NET}$
i_{ps}^{NET}
i_{cl}^{NET}
i_{pct}^{NET}
i_{noc}^{NET}
i_{l}^{NET}
Accident
$q^{(1)}=0; r=0$
$i_{ps}^{NET}(t)=NaN; i_{cl}^{NET}(t)=NaN$
$[i_l^{NET}=0]$
$i_{noc}^{NET}=0$
$q=0$
$i_{noc}^{NET}=1; i_l^{NET}>0$
Data transmission failure
$q^{(1)}=r-B_l$
$r=\frac{i_{pct}^{NET}}{T_p+\frac{q}{B_l}}; B_l=B-a\cdot i_l^{NET}$
$i_{ps}^{NET}(t)=i_{ps}^{NET}(t+\frac{P_{ps}}{r}),$
$i_{cl}^{NET}(t)=i_{cl}^{NET}(t+\frac{P_{cl}}{r})$
$i_{noc}^{NET}=0$
$q=0$
$i_{noc}^{NET}=1$
$i_l^{NET}=0$
$i_l^{NET}>0$
$i_l^{NET}=0$
Normal
$q^{(1)}=r-B$
$r=\frac{i_{pct}^{NET}}{T_p+\frac{q}{B}}$
$i_{ps}^{NET}(t)=i_{ps}^{NET}(t+\frac{P_{ps}}{r}),$
$i_{cl}^{NET}(t)=i_{cl}^{NET}(t+\frac{P_{cl}}{r})$
$[i_l^{NET}=0]$
i_{ps}^{NET}
i_{cl}^{NET}
$o_{2,1}^{NET}$
$o_{2,2}^{NET}$

Fig. 4. Network operation model

While the network is operating in normal mode, the data transmission rate is calculated by the formula:

$$r=\frac{i_{pct}^{NET}}{T_p+\frac{q}{B}}, \qquad (1)$$

where i_{ps}^{NET} – the number of packets entering the network; T_p – propagation delay; q – the queue size; B – network bandwidth in pack/s.

According to [14], the queue size q is described by the following equation of dynamics:

$$q^{(1)}=r-B. \qquad (2)$$

Data from the power supply and cooling systems are fed into the system with a delay:

$$i_{ps}^{NET}(t)=i_{ps}^{NET}\left(t+\frac{P_{ps}}{r}\right),$$
$$i_{cl}^{NET}(t)=i_{cl}^{NET}\left(t+\frac{P_{cl}}{r}\right), \qquad (3)$$

where P_{ps}, P_{cl} – the number of packets coming from a particular system.

Thus, the more network traffic, the greater the propagation delay. In the case of a failure of data transmission channels, the network capacity is reduced by the formula:

$$B_l=B-a\cdot i_l^{NET}, \qquad (4)$$

where a – the number of refused data transmission channels.

In the case when the NOC is in an inoperative state, that is $i_{noc}^{NET}=0$, the transition to the «Accident» state occurs and at all outputs of the system have the value NaN.

6. Research results

To simulate NOC, a model is built in the Simulink/Stateflow package (Fig. 5). This model is very simplistic, but sufficient to demonstrate the proposed approach for the design and study of complex interconnected systems with the EOCA help.

The state diagram of the NOC model in StateFlow looks like this (Fig. 6).

The following values of parameters are set for the model:

– $T_{ups}=20$ s – the time that NOC can operate using uninterruptible power supplies;

– $T_{cl}=10$ s – the time that NOC can operate without a cooling system;

– $R_0=3000$ W·h – the minimum level of electricity required for the NOC operation;

– $C_0=2000$ BTU/hour – the minimum level of cooling power required for the NOC operation.

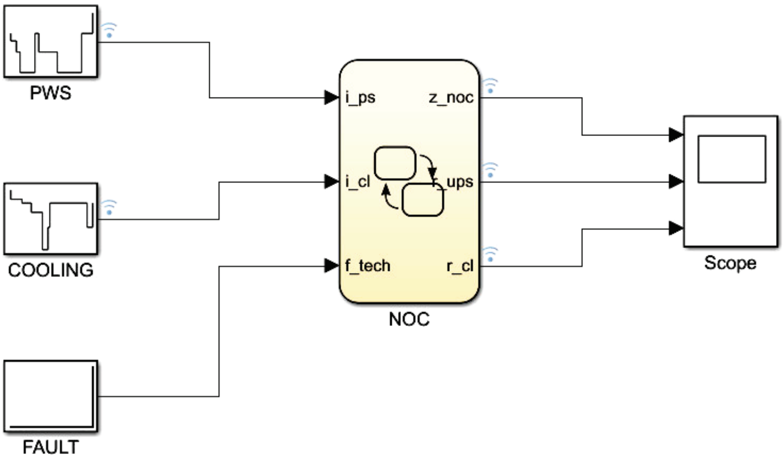

Fig. 5. Model of the network operation center in Simulink

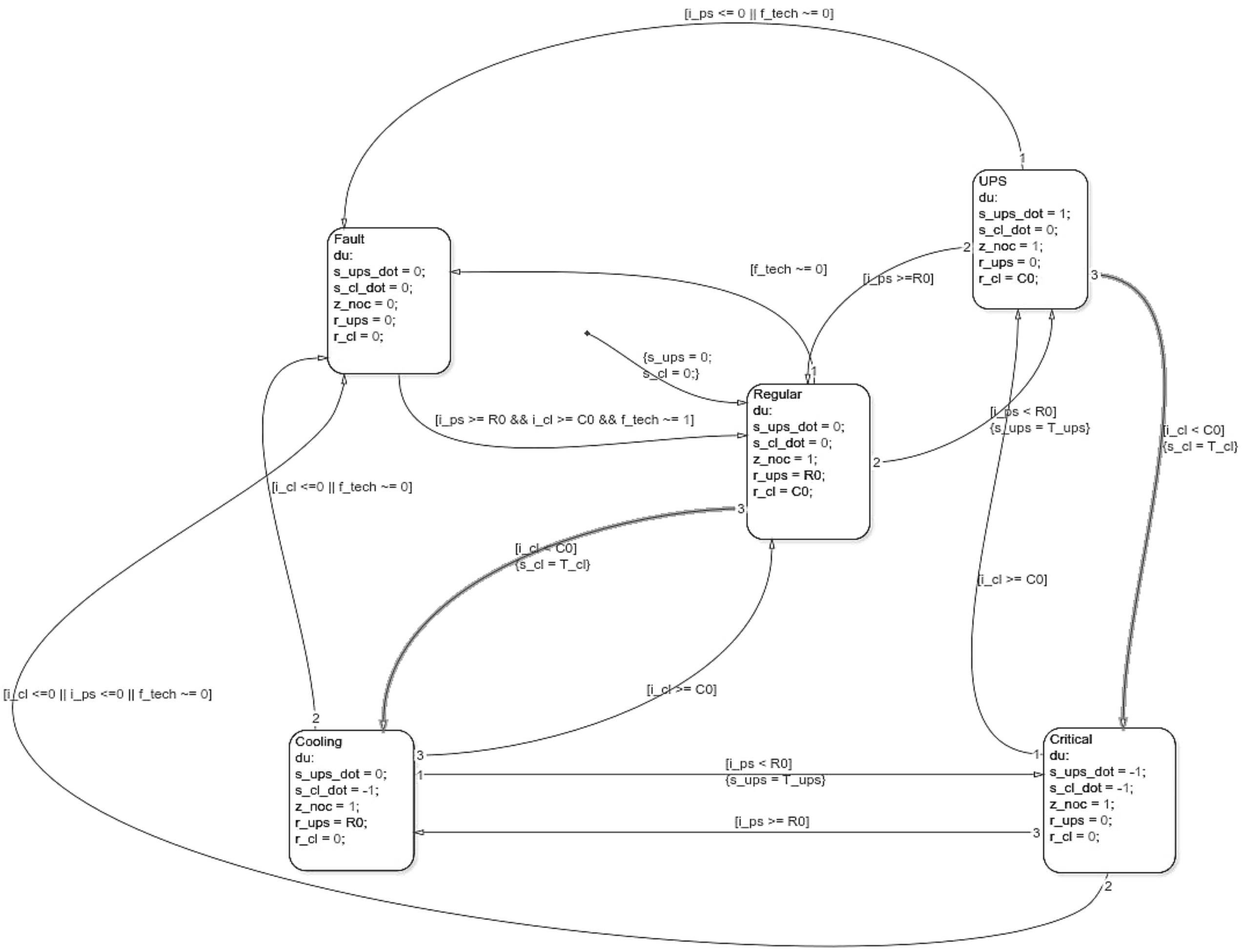

Fig. 6. Model of the network operation center in Stateflow

The time diagrams show the values of the parameters that are fed to the inputs of the constructed model (Fig. 7–9).

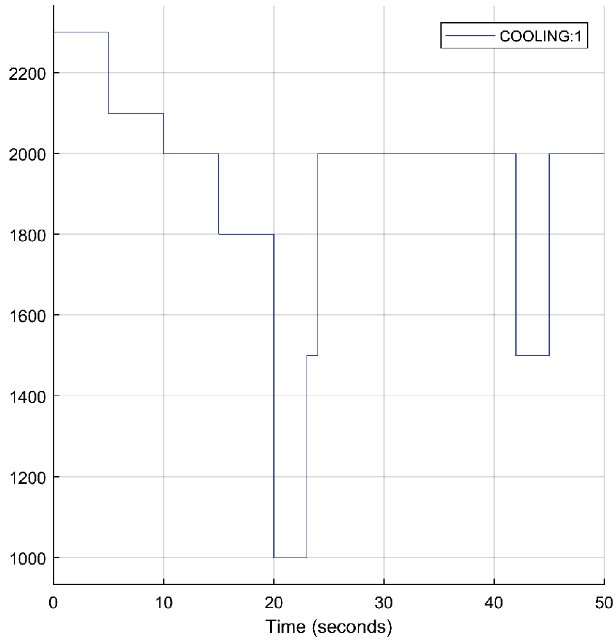

Fig. 7. The cooling capacity diagram at the input of the network operation center

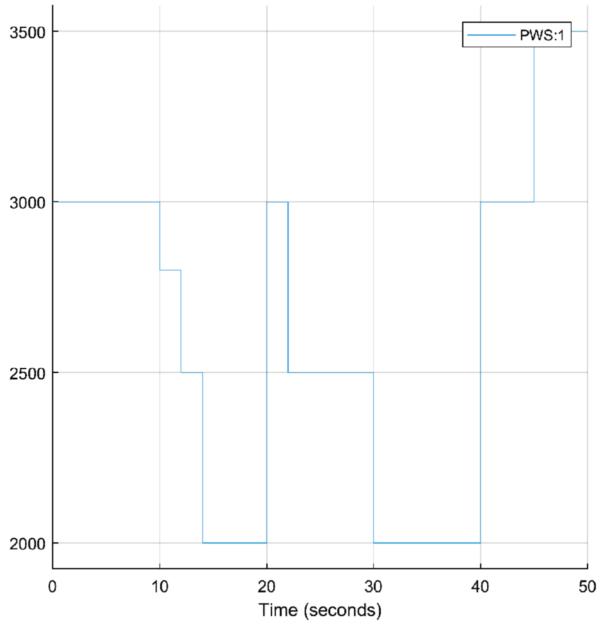

Fig. 8. The electricity availability diagram at the input of the network operation center

The time diagrams of the outputs of the NOC model are shown in Fig. 10.

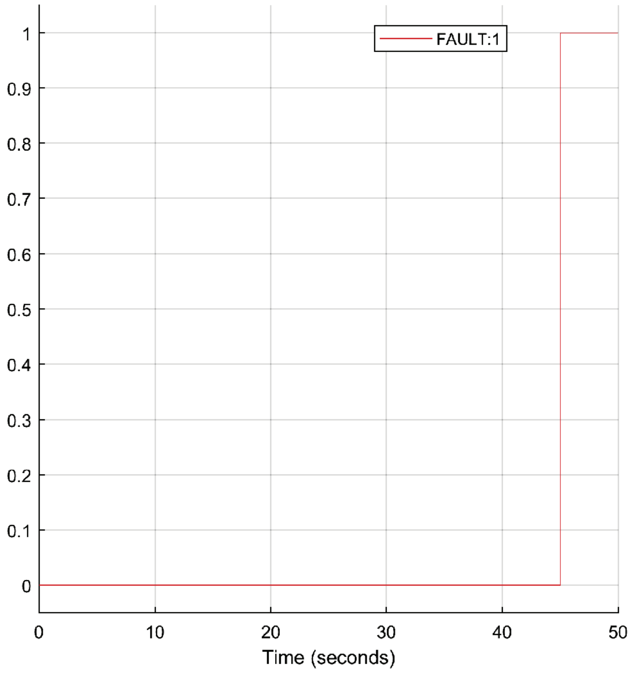

Fig. 9. Distribution diagram of the occurrence of technical failures at the input of the network operation center

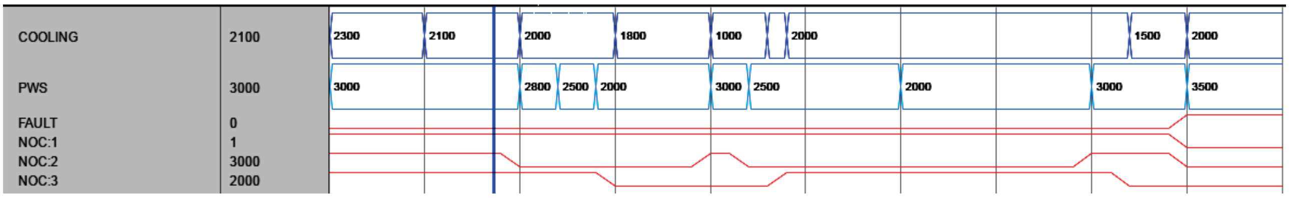

Fig. 10. The time diagrams of the outputs

The diagram in Fig. 10 indicates that the NOC operates in a given mode, passes the corresponding states depending on the input parameters coming from other subsystems of the model.

7. SWOT analysis of research results

Strengths. When working with critical IT infrastructures, scalability is one of the problems faced by all methods that are used to model interdependence. The proposed approach is both modular and scalable in the sense that it has sufficient flexibility in selection and use of both high-precision and simple models for critical IT infrastructure. Modularity is achieved through the use of composition elements, whereas scalability is presented in two forms: scalability in building the model (topology and functionality) of the critical IT infrastructure and scalability in terms of the processing power required to run the models. From the point of view of modeling, the proposed approach allows creating model compositions that can be further used as top-level components, which in turn can be used to create components of an even higher level and the like. Thus, the approach allows to accumulate a portfolio of components for multiple use. For example, an electrical substation can be represented as a set of several generators. Thus, it is possible to build a model of a single generator, and then reuse it to create a model of an electrical substation. And if add uninterruptible power supplies to this set of, it is possible to obtain the model of the electrical infrastructure as part of a more complex critical IT infrastructure. From the point of view of the necessary computational power for the launch of the model, the approach provides the same possibility of forming the necessary level of abstraction.

The approach is based on the use of extended open hybrid automata (EOHA) and provides all the necessary tools for building, planning, researching, managing, evaluating, etc. critical IT infrastructures.

Weaknesses. At this stage of the approach development, the only weakness is the availability of very simplified models of subsystems and critical IT infrastructure components.

Opportunities. In the future, it is planned to use the proposed approach for developing models with different levels of abstraction for various components and subsystems of the critical IT infrastructure, with the ultimate aim of creating a library of models that will allow them to be selected and easily used for various studies. Also, the future aim is investigation of the ways of generating scenarios for constructing compositions in order to create large and super-large models.

The proposed approach and modeling library for Simulink/Stateflow will allow researchers to model any relationships between systems, components of critical IT infrastructure.

Threats. It is now difficult to predict the negative risks of the developed approach. But it is possible to say for sure that no additional costs are necessary will be for developer of critical IT infrastructure that will use the proposed approach and the library of models developed in the future.

8. Conclusions

1. Existing mathematical apparatus of open hybrid automata for the purpose of researching critical IT infrastructures is improved. Additional elements are added to the usual open hybrid automaton, which significantly expand its functionality. Many transition markers $L \subseteq D \times D$ allow the creation of marked transitive systems of components and systems of critical IT infrastructure for further investigation of them for the reach and safety of states. The distribution F allows to add a probabilistic character in the behavior of the elements, and the sets SP, P, R, V – provide the components and systems of the critical IT infrastructure with quality characteristics.

2. The simplified models of some critical IT infrastructure components are constructed and investigated using them to use the proposed approach. This approach allows to create patterns of models based on interdependence, existing between them, combining them into more complex models, and thus, to form the following levels of model abstraction. The operability of the proposed approach is tested for simple models – several models are created in the Matlab package, their work is studied, and the expected results are obtained.

References

1. Pro vnesennia zmin do deiakykh zakoniv Ukrainy shchodo zabezpechennia kibernetychnoi bezpeky Ukrainy [Electronic resource]: Draft Law No. 11125 from August 31, 2012 // Official web portal of the Verkhovna Rada of Ukraine. – Available at: \www/URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?id=&pf3511=44208
2. Rinaldi, S. M. Identifying, understanding, and analyzing critical infrastructure interdependencies [Text] / S. M. Rinaldi, J. P. Peerenboom, T. K. Kelly // IEEE Control Systems Magazine. – 2001. – Vol. 21, No. 6. – P. 11–25. doi:10.1109/37.969131
3. Ouyang, M. Review on modeling and simulation of interdependent critical infrastructure systems [Text] / M. Ouyang // Reliability Engineering & System Safety. – 2014. – Vol. 121. – P. 43–60. doi:10.1016/j.ress.2013.06.040
4. Satumtira, G. Synthesis of Modeling and Simulation Methods on Critical Infrastructure Interdependencies Research [Text] / G. Satumtira, L. Duenas-Osorio // Sustainable and Resilient Critical Infrastructure Systems. – Berlin, Heidelberg: Springer, 2010. – P. 1–51. doi:10.1007/978-3-642-11405-2_1
5. Hasan, S. Modeling infrastructure system interdependencies and socioeconomic impacts of failure in extreme events: emerging R&D challenges [Text] / S. Hasan, G. Foliente // Natural Hazards. – 2015. – Vol. 78, No. 3. – P. 2143–2168. doi:10.1007/s11069-015-1814-7
6. Oliva, G. Fuzzy dynamic input–output inoperability model [Text] / G. Oliva, S. Panzieri, R. Setola // International Journal of Critical Infrastructure Protection. – 2011. – Vol. 4, No. 3–4. – P. 165–175. doi:10.1016/j.ijcip.2011.09.003
7. Kaegi, M. Analyzing maintenance strategies by agent-based simulations: A feasibility study [Text] / M. Kaegi, R. Mock, W. Kroger // Reliability Engineering & System Safety. – 2009. – Vol. 94, No. 9. – P. 1416–1421. doi:10.1016/j.ress.2009.02.002
8. Rolik, A. I. Kontseptsiia upravleniia korporativnoi IT-infrastrukturoi [Text] / A. I. Rolik // Visnyk NTUU «KPI». Informatics, operation and computer science. – 2012. – Vol. 56. – P. 31–55.
9. Svendsen, N. K. Graph Models of Critical Infrastructure Interdependencies [Text] / N. K. Svendsen, S. D. Wolthusen // Inter-Domain Management. – Berlin, Heidelberg: Springer, 2007. – P. 208–211. doi:10.1007/978-3-540-72986-0_27
10. Wang, S. Vulnerability analysis of interdependent infrastructure systems under edge attack strategies [Text] / S. Wang, L. Hong, M. Ouyang, J. Zhang, X. Chen // Safety Science. – 2013. – Vol. 51, No. 1. – P. 328–337. doi:10.1016/j.ssci.2012.07.003
11. Gursesli, O. Modeling infrastructure interdependencies using Petri nets [Text] / O. Gursesli, A. A. Desrochers // SMC'03 Conference Proceedings. 2003 IEEE International Conference on Systems, Man and Cybernetics. Conference Theme – System Security and Assurance (Cat. No.03CH37483). – IEEE, 2003. – P. 1506–1512. doi:10.1109/icsmc.2003.1244625
12. Beccuti, M. Quantification of dependencies between electrical and information infrastructures [Text] / M. Beccuti, G. Franceschinis, S. Donatelli, S. Chiaradonna, F. Di Giandomenico, P. Lollini, G. Dondossola, F. Garrone // International Journal of Critical Infrastructure Protection. – 2012. – Vol. 5, No. 1. – P. 14–27. doi:10.1016/j.ijcip.2012.01.003
13. Di Giorgio, A. A Bayesian Network-Based Approach to the Critical Infrastructure Interdependencies Analysis [Text] / A. Di Giorgio, F. Liberati // IEEE Systems Journal. – 2012. – Vol. 6, No. 3. – P. 510–519. doi:10.1109/jsyst.2012.2190695
14. Dorogyy, Ya. Yu. TS-sumisna arkhitektura krytychnoi IT-infrastruktury [Text] / Ya. Yu. Dorogyy // Visnyk NTUU «KPI». Informatics, operation and computer science. – 2016. – Vol. 65.
15. Lee, J. Modeling Communication Networks With Hybrid Systems [Text] / J. Lee, S. Bohacek, J. P. Hespanha, K. Obraczka // IEEE/ACM Transactions on Networking. – 2007. – Vol. 15, No. 3. – P. 630–643. doi:10.1109/tnet.2007.893090

РАЗРАБОТКА ПОДХОДА К ПРОЕКТИРОВАНИЮ, МОДЕЛИРОВАНИЮ И ИССЛЕДОВАНИЮ КРИТИЧЕСКОЙ ИТ-ИНФРАСТРУКТУРЫ

Предложен подход, который позволяет разработать точные модели компонентов критической ИТ-инфраструктуры и объединить их на базе их зависимостей. Этот подход дает инструмент для создания более масштабных и сложных взаимосвязанных моделей. Применяя определенные настройки, используя различные условия эксплуатации, предложенный инструментарий позволяет изучить каскадные эффекты взаимозависимости компонентов или целых систем, провести детальную оценку их уязвимости и осуществить широкое планирование.

Ключевые слова: критическая ИТ-инфраструктура, гибридный расширенный открытый автомат, уровни абстракции моделей.

Dorogyy Yaroslaw, *PhD, Associate Professor, Department of Automation and Control in Technical Systems, National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute», Ukraine, e-mail: cisco.rna@gmail.com, ORCID: http://orcid.org/0000-0003-3848-9852*