https://doi.org/10.15407/csc.2024.02.021
UDC 004.7

I.M. OKSANYCH, PhD (Eng.), Senior Research Associate,
The Institute of Mathematical Machines and Systems Problems of the Ukraine
National Academy of Science (IMMSP NAS of Ukraine),
Glushkov ave., 42, Kyiv, 03187, Ukraine,
ORCID: https://orcid.org/0000-0002-1208-3427,
inokc2018@gmail.com

V.F. GRECHANINOV, PhD (Eng.), Head of Department,
The Institute of Mathematical Machines and Systems Problems of the Ukraine
National Academy of Science (IMMSP NAS of Ukraine),
Glushkov ave., 42, Kyiv, 03187, Ukraine,
ORCID: https://orcid.org/0000-0001-6268-3204,
vgrechaninov@gmail.com

A.V. LOPUSHANSKYI, Research Associate,
The Institute of Mathematical Machines and Systems Problems of the Ukraine
National Academy of Science (IMMSP NAS of Ukraine),
Glushkov ave., 42, Kyiv, 03187, Ukraine,
ORCID: https://orcid.org/0000-0002-4840-0236,
anatoliy.lopushanskyi@gmail.com

S.E. NOVGORODSKIJ, Senior Research Associate,
The Institute of Mathematical Machines and Systems Problems of the Ukraine
National Academy of Science (IMMSP NAS of Ukraine),
Glushkov ave., 42, Kyiv, 03187, Ukraine,
ORCID: https://orcid.org/0000-0002-6498-1819.
stanislavnovgorodskij@gmail.com

V.F. HOLOVSKYI, Senior Research Associate,
The Institute of Mathematical Machines and Systems Problems of the Ukraine
National Academy of Science (IMMSP NAS of Ukraine),
Glushkov ave., 42, Kyiv, 03187, Ukraine,
ORCID: https://orcid.org/0009-0001-4959-0940,
rusgol05@gmail.com

INTEGRATION OF DIFFERENT APPROACHES TO THE MODELING OF CRITICAL INFRASTRUCTURE

The article is devoted to solving the problem of determining the resilience of critical infrastructure systems to malicious actions of adversaries. Different modeling methods and their integration are considered. Using the example of a system of systems, including energy and transport networks, the application of methods of agent, network, economic modeling

Cite: Oksanych I.M., Grechaninov V.F., Lopushanskyi A.V, Novgorodskij S.Ye., Holovskyi V.F. Inte-gration of Different Approaches to the Modeling of Critical Infrastructure. *Control Systems and Computers*, 2024, 2, 21—34. https://doi.org/10.15407/csc.2024.02.021

and the method of system dynamics are considered, which are combined into a single structure of analysis for the development of algorithms for general decision-making support for the protection of critical infrastructure systems.

Keywords: *modeling the resilience of critical infrastructure, agent-based modeling, network modeling, and system dynamics methods.*

Introduction

Currently, the large-scale war of the Russian Federation against Ukraine, the increase in the level of terrorist threats, as well as the global trends towards the significant consequences of natural and man-made emergencies have led to the actualization of the issue of protecting systems, objects and resources that are critically important for life society, socio-economic development of the state and ensuring national security, i.e. protection of critical infrastructure (CI), which is one of the top priorities for providing national security.

The Law of Ukraine "On Critical Infrastructure" defines CI objects as infrastructure objects, systems, their parts, and their totality, which are important for the economy, national security, and defense, the malfunctioning of which can cause damage to vital national interests [1]. According to this law, CI includes objects that satisfy the most important functions and services of energy supply, water supply, transport, health care, food supply, finance, governance, and defense of the state. As noted in the Law, "The goal of state policy in the field of critical infrastructure protection is to ensure the safety of critical infrastructure facilities, prevent unauthorized interference in their functioning, forecast and prevent crises at critical infrastructure facilities". Therefore, the analysis of challenges and threats affecting the resilience of CI objects, the assessment of their security status to detect and prevent incidents, as well as the development of a set of measures to control security risks at CI objects is a primary task and problem in the state.

To solve the above-mentioned problem, the numerous CI analysis methodologies are used in the world, which make it possible to obtain estimates of its vulnerability, risks, and stability. Such assessments help in planning investments in CI, planning the continuity of its work, and making operational decisions.

Simulation modeling, agent modeling, network modeling, economic modeling, system dynamics methods, etc., as well as methodologies for modeling the interdependencies of CI systems and objects, can be included in the world's most widely used methodologies for evaluating CI systems.

Problem Setting

Analyzing different approaches to CI modeling and relying on world experience, we can conclude that each methodology has its advantages and disadvantages. These methodologies can be deterministic or probabilistic, static or dynamic, and have different assumptions, levels of detail, data requirements, properties, and scope. Therefore, it is practically impossible to assess the entire criticality of such complex objects as CI objects with one type of model. In this sense, there is a question of consideration and research of the problem of the possibility of integrating different methodologies to the modeling of risk assessment and security of CI objects into a single analysis structure for the development of algorithms for general decision-making support regarding CI protection.

Analysis of Recent Research and Publications

Today in the literature can find many works devoted to the use of different approaches to the modeling of CI systems in order to assess their resilience to threats, resistance to risks and to provide recommendations for making decisions against threats. There are both review articles describing various methods and articles describing the application of individual CI resilience assessment modeling methods to specific challenges and threats. Here is a brief description of some of them.

The review papers [2—4] describe, characterize, and compare the currently most used approaches to CI modeling, such as: empirical, agent, network, based on the system dynamics and economic theory. Issues of interdependencies of CI systems are considered. The paper [3] highlights the problems of CI protection against the background of the use of the latest technologies such as the Internet of Things (IoT) and concludes that none of the above-mentioned approaches provides "comprehensive" threat modeling and assessment of AI resilience. The article [5] presents an overview of the approach to agent modeling in transport systems and discusses optimization problems using agent models.

In works [6—8], a study of agent approaches to CI modeling was carried out. In particular, [6] presents an agent-oriented CI model taking into account interdependencies between energy and water supply systems (Interdependent Critical Infrastructure Model — ICIM), which is intended for long-term joint planning at the national and regional levels in a specific geographic region in order to avoid shortages electricity and water.

Papers [7, 8] are devoted to the management of emergency response. In [7], a system for alerting and reporting on emergencies, built on multi-agent software architecture, is presented. The system works in real time with social media support as a decision support system for emergency management. In [8], the use of large multi-agent systems to solve emergency situations in dynamic environments with uncertainty is considered. The use of Markov, semi-Markov and partially observed Markov decision-making processes is explained.

The work [9] is devoted to the study of the physical resilience of the operation of a nuclear power plant (NPP) in the conditions of earthquakes. The NPP is presented as a system of systems described by various methods of relationships, such as a failure tree, a goal tree, a success tree, hierarchical modeling, etc. A quantitative analysis of the safe operation of the NPP is carried out, which is represented as the probability that it will not cause damage during an earthquake. The time to restore normal operation is considered an assessment of the physical resilience of the NPP. The research is conducted using the Monte Carlo method.

The works [10, 11] consider the use of network approaches to the modeling of CI resilience estimates. In particular, [10] presents a network model that uses game-theoretic modeling methods to assess the worst failures in the functioning of interdependent CI systems and determine the most effective protection measures against them. The application of network flow with a defined set of nodes and edges is shown on the example of interdependencies of gas and electric networks. A binary variable is used instead of a probabilistic estimate of the state of the node.

The paper [11] investigates the use of a network approach to CI modeling based on the topology of the water basin for the analysis of the risk of flooding of the catchment area. A multi-sector, multi-level CI network is represented by points, connectors, and polygons. Cascade effects under different flooding scenarios are considered.

In [12], two interdependent network systems are considered, each of which consists of several components (nodes) connected by connections (arcs) representing physical and/or logical connections between them. Interdependencies are modeled as links connecting the nodes of two systems and are conceptually similar to the connections of separate systems. Each node in system 1 can be interdependent with any other node in system 2. To estimate the average response of systems to cascading failures and take into account the dynamics of changes in connections between two systems, Monte Carlo simulation is performed, where interdependence connections between nodes change randomly during each test.

The works [13—15] use the system dynamics approach to modeling interdependencies of CIs.

The article [13] investigates a dynamic model for assessing the risks of failures in combined complex infrastructure systems. A model of a coupled dynamic complex system based on cellular automata is considered. Failures in connected and unconnected systems are compared. It is concluded that connected systems are more susceptible to large-scale failures, and a failure in one system can cause a similar failure in another.

Research [14] is devoted to solve the problem of survivability of a complex dynamic system in realistic operating modes. The energy network of Scandinavia and the influence of its topology parameters on the stability of operation are considered and investigated.

The work [15] is devoted to the study of the system dynamics approach and presents the CRISADMIN project, funded by the European Commission for Critical Infrastructure Protection (CIPS), which aims to develop a decision support system (DSS) based on a system dynamic model of critical infrastructures. The model of system dynamics allows for a deep understanding of the interdependencies between CIs, as well as possible impacts in case of critical events on the socio-economic context.

The Object of Research and the Purpose of the Article

During the bombing of the territory of an independent state by an aggressor, in addition to the population, all critical infrastructure objects of both large cities and small towns and villages suffer. However, energy facilities that produce, transmit and supply electricity to the population (thermal power plants, transformer substations, etc.) receive the greatest damage. Transport also suffers. The subway, trolleybuses stop, railway junctions are damaged, model cars burn, bridges collapse. There is a lot of destruction and casualties among the population. Rescue services, firefighters, medics, and energy teams are involved in restoring life in places of such damage.

The purpose of the article is to build a model of integration of various approaches to CI modeling for a comprehensive analysis of the possibilities of its protection and recovery.

The object of research of the article is the system of CI systems, which consists of systems of energy, transport and liquidation of the consequences of emergencies.

According to the results of the literature analysis, it can be said that the agent, network, economic approaches and the approach based on system dynamics are currently the most used. Therefore, the application of such approaches is considered in the article.

Using the Agent Modeling Approach

In order to analyze the damage structure and restore the operation of the entire AI that is exposed to an aggressor's attacks, its model can be conveniently represented as a system of separate systems that are represented by heterogeneous agents and combined into one connected decision support system (DSS).

Fig. 1 shows the multi-agent model of the system of individual systems of the critical infrastructure of the CIMM (CI multi-agent model), which allows us to present the CI as a set of agents that have their roles (the names are shown in Fig. 1) and perform functions corresponding to these roles. This representation allows for a more detailed and transparent review of the tasks and behavior of decision-making agents (DMs) and to develop appropriate algorithms to support these decision-making (DSs).

Let's consider the structure of the model in more detail.

Due to the fact that leaders of the Russian Federation very often threatens to use weapons of mass destruction against the population of the European continent, and in addition to this, other countries strive to increase their nuclear potential, NATO issued a document concerning its policy in the field of defense from chemical, biological, radiological and nuclear (CBRN) weapons [17]. According to this document, NATO's main policy principles and commitments are to prevent, protect and recover the lives of the population, territories and NATO forces after the use of CBRN. Therefore, agents whose role is to prevent, protect and recover CIs after terrorist attacks should be part of the CIs system of systems model.

As a result, the set of agents of the CIMM model has the form:

$$A_{CIMM} = \{A_{CA}, A_{En}, A_{Tr}, A_{Er}, A_{Contr}, A_{Prev}, A_{Prot}, A_{Rec}\},$$

where

A_{CIMM} — set of agents of the CIMM model,
A_{CA} — situational awareness Agent (SA),
A_{En} — energy Agents,
A_{Tr} — transport Agents,
A_{Er} — emergency response Agents,
A_{Contr} — CI resilience control Agent,
A_{Prev} — emergency prevention Agent,
A_{Prot} — CI protection Agent,
A_{Rec} — CI recovery Agent.

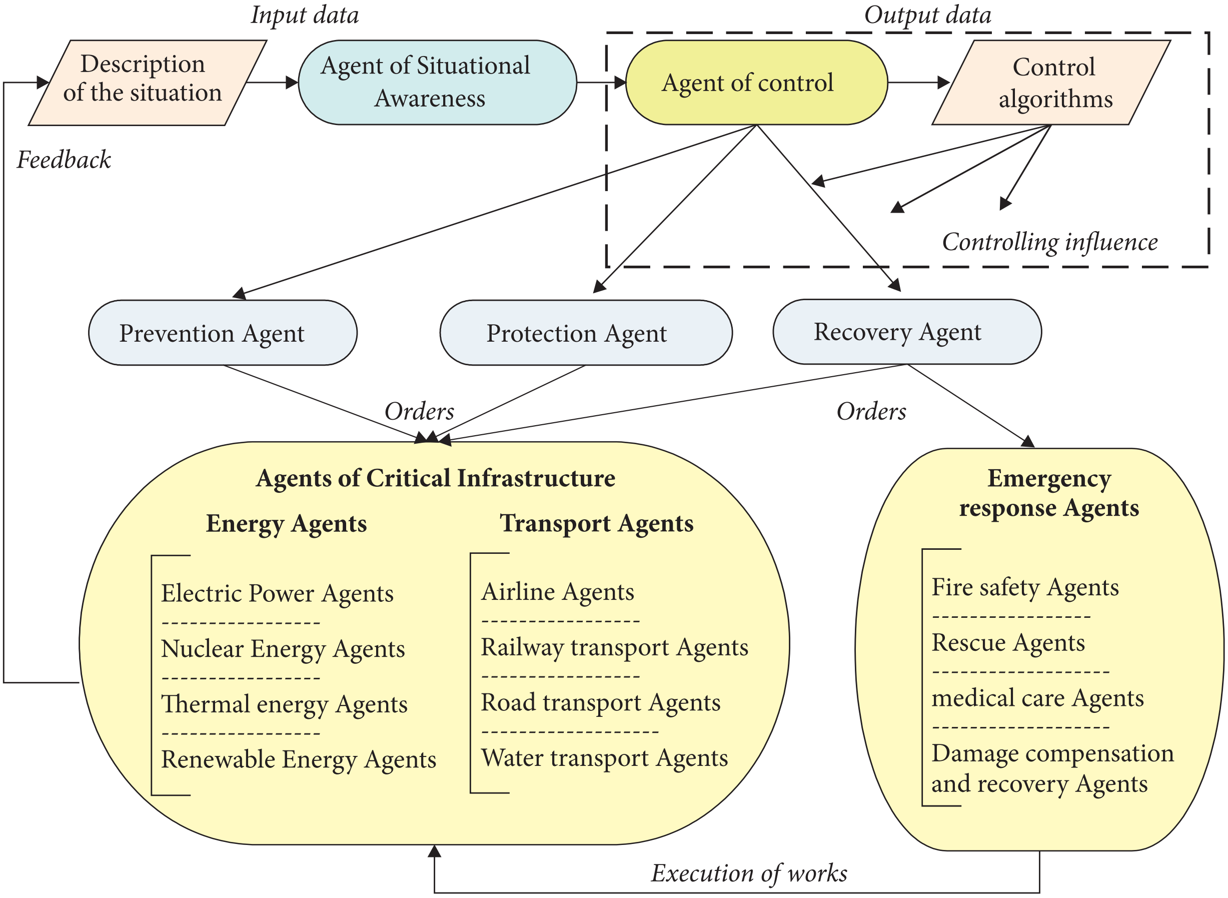

Fig. 1. Multi-agent model of the system of individual CI systems (CIMM)

Model input data. The input data of the CIMM are data about the emergency that is about to happen or has already happened at CI objects and the state of the CI: messages coming from various sources, including from the Internet of Things (IoT); intelligence data; media and social network data; data from various sensors, etc. These data are sent to A_{SA}.

The functions of A_{SA} consist of verification, aggregation and intellectual analysis of input data, the result of which is the formation of the operational situation as a function of time and the forecast of its development. Also here, preliminary modeling of emergency development options should be carried out, including using the approaches and methods described in this article.

The functions of A_{En} and A_{Tr} include ensuring the necessary needs of society, respectively, in energy capacities and in passenger and cargo transportation.

The function of A_{Prev} includes political decisions at the state level and decisions on prevention policies at the level of individual CI objects, the main ideas of which are building up the potential of countering the enemy and investments in CI security. It is also advisable to take into account the testing of protection systems and personnel training.

The function of A_{Prot} includes ensuring the safety and stable functioning of CI objects: physical protection; cyber defense; ensuring sustainable work based on risk analysis and assessment; organizational resilience; anti-crisis management.

The functions of A_{Rec} include, in addition to eliminating the consequences of emergency situations, also functions to restore the needs for resources that were damaged or destroyed as a result of the emergency (providing the population with electricity and transport).

Model output data. On the basis of SA data, the control agent A_{Prev} produces decision-making support algorithms and, based on them, forms controlling influences on agents of prevention, protection and recovery in order to ensure the safe and normal operation of CI objects to meet society's needs for electricity and transport. Controlling influences are the output data of the model.

The control influence on the recovery of services in electricity and transport consists in the redistribution by the recovery agent A_{Rec} of the production of services between the corresponding agents A_{En} and A_{Tr}.

When the availability of certain types of transport becomes impossible, the load falls on those types that remain available. In this case, the control agent A_{Contr} carries out fixation and regulation by redistributing the load to individual types of transport.

In the case of electricity, when it is impossible to satisfy the population and industry in the required capacity as a result of damage or destruction of one type of supply, another comes to his aid. In this case, the control agent A_{Contr} carries out the dispatching of capacity redistribution between the agents A_{En}, taking into account the demand forecast.

Multi-agent CIMM model (Fig. 1) makes it possible to carry out both a top-down and bottom-up analysis of the CI system.

The advantages of the agent approach lie in the possibility of representing the decision maker and the main participants in the system as heterogeneous agents with their own connections and actions. The method makes it possible to simulate "what if" scenarios (as described above) and evaluate the effectiveness of various management strategies. Agent-based modeling can be integrated with other modeling methods for more complete analysis.

Disadvantages of the agent approach are a modeling the behavior of agents and the configuration of systems depends on the assumptions made by the developer.

Using the System Dynamics Approach

System dynamics (SD) approaches make it possible to model the dynamic and evolutionary behavior of CI components and systems, interdependent CIs, as they assess the impact of various factors on the evolution of these systems over time. SD methods can also use cause-and-effect diagrams and stock-and-flow diagrams that describe the flow of information and products through CI systems.

SD-based approaches capture important causes and effects in disruptive scenarios, the impact of political and technical factors. They make it possible to reflect the evolution of the system in the long term and provide investment recommendations. These approaches can be used to compare alternative strategies for the protection of CIs and promote consensus among stakeholders in decision-making.

System dynamics approaches take into account:

1) Presence of time-varying values;

2) Variability based on causal relationships;

3) Feedback loops containing the main cause-and-effect actions of a closed system.

The SD approach can be used to forecast the evolution of all CI components and systems (features of the territory, time of critical event, environmental factors, types of participating entities, etc.) from the occurrence of an emergency to its implementation.

In the CIMM model (Fig. 1), considered in the article, the SD approach consists of the following stages:

- collection of data by the A_{SA} agent about emergency situations in time (possibility of occurrence, occurrence itself, spread);
- analysis of data by agent A_{SA} and determination of importance $SA(t)$:
- modeling of the further deployment of the emergency over time (including relationships between CI components and systems and cascading effects) and the development of DS algorithms by the A_{Contr} agent;
- formation by the agent A_{Contr} of recommending control influences on the agents A_{Prev}, A_{Prot},

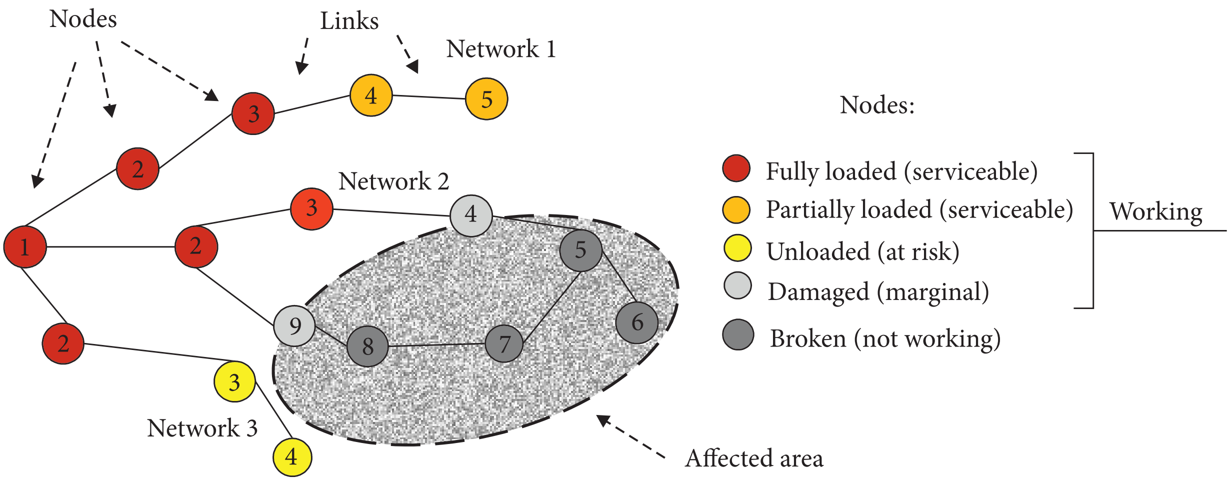

Fig. 2. An example of a conditional network topology

A_{Rec} (who act as DM) in accordance with the developed DS algorithms;

- formation of additional recommendations to agents A_{Prev}, A_{Prot}, A_{Rec} and orders to agents A_{En}, A_{Tr} to continue overcoming the consequences of the emergency;
- collection of data on the progress of emergency situations and the state of CI systems in the sense of the ability to meet the corresponding needs of A_{En}, A_{Tr} agents (feedback);
- refinement of $SA(t)$ by agent A_{SA};
- refinement of DS algorithms by agent A_{Contr};
- formation of additional recommendations to agents APrev, AProt, ARec and orders to agents AEn, ATr to continue overcoming the consequences of the emergency.

The described algorithm is repeated over time until the consequences are completely eliminated and the CI operation is restored.

The model based on system dynamics of CIMM represents a top-down analysis of the system of CI systems.

The main advantages of the approach based on system dynamics are, of course, the ability to analyze the evolution of CI systems and the effectiveness of methods for countering threats.

Disadvantages of the approach based on system dynamics include the fact that it describes the behavior of CIs at the system level and does not analyze, for example, the topology of components. Therefore, it should be combined with other modeling methods.

Using the Network Modeling Approach

CI systems of electricity and transport, which are distributed over large geographical areas, can be represented as network systems, where nodes represent their various components, and edges simulate physical or relational connections between the components of these systems. Such network systems are described by their topologies and flows. The threat resilience of such CI systems can be analyzed by first modeling failures of individual CI components and systems, and then by modeling cascading effects both within and between CIs at the system level of interdependent CI systems.

In the network modeling of CI resilience based on their topologies, such indicators of individual CIs are used as the number of working or damaged network nodes, the loss of communication between them, the duration of their unavailability, the number of lost customers, which is reflected in the form of losses that exceed possible values. Topology-based methods capture the topological features of individual CI systems, identify their critical components, and provide suggestions for increasing their resilience.

Flow-based methods consider services (flows) that are created and transmitted by individual CI systems. Each node is represented as a node of supply or demand for services, and a link as the capacity of their delivery. Such a representation makes it possible to perform flow dispatching, that is, to redirect the load from one link to another in the network, or to redistribute the load to other nodes when a node fails.

Fig. 2 shows an example of the topology of a conditional aggregate CI network, which can be applied to both power grids and transport networks. In the case of a power grid, nodes characterize individual components of CI, and links are connections between them in the form of transmission power. In the case of a transport network, nodes model individual stations, and links model the passenger or cargo flow between them.

In the CIMM model (Fig. 1), dispatching of electricity power flows and passenger and cargo flows is performed by the management agent A_{Contr}. For the topology shown in Fig. 2, the load that was on damaged (4, 9) and completely destroyed (5—8) nodes of Network 2 is redirected to partially loaded (4, 5) nodes of Network 1 and to unloaded (3, 4) nodes of Networks 3. Since 6 nodes were loaded before the damage and only 4 after redistribution of flows, we can state the loss of a part of the capacity in the general service supply network.

Binary and probabilistic assessments of node states can be used for failure calculations. These estimates are determined by experts based on historical data or their personal professional opinion. In the network modeling of CI systems, the binary and multiple states of nodes are considered.

A binary state characterizes a node as either working or not working. This binary state distinguishes nodes that have failed or are completely damaged from nodes that can still work. This representation of the state of the network allows us to quickly determine the situation that is developing — whether it is safe or dangerous, to determine the approach of a dangerous critical situation and to take the necessary measures. However, such a model can also give false results.

On the contrary, models of the multiple state of nodes allow to get a more accurate approximation to reality, because they model different states (for example, serviceable, marginal and risk state) (Fig. 2), but they require knowledge or calculation of the probabilities of occurrence of these states.

Risk analysis. For probabilistic risk analysis, the Monte Carlo method is often used for probabilistic assessments of impacts on systems, the simulation of which allows us to estimate the probability of CI systems transitioning into a dangerous state after external influences. Markov, semi-Markov processes, interval analysis, and Bayesian networks can also be used to study probabilistic values of quantities. Probability estimates, which are inputs to such methods, are usually determined by experts based on historical data or their personal opinion.

However, for risks that are difficult or even impossible to predict (for example, due to the lack of statistical historical data on the event), probabilistic assessment cannot be applied. Furthermore, for deliberate threats posed by an intelligent, targeted terrorist, probabilities may not be suitable for modeling adversary behavior, and probabilistic terrorism risk assessment may even lead to erroneous results. To identify the worst failures in terrorist attacks, it can be assumed that a hypothetical intelligent adversary (aggressor) has perfect knowledge and is able to use unlimited resources to deliberately damage CI.

In such a case, it is appropriate to consider failures as simultaneous losses of one or more components of the CI system and evaluate its performance in the worst cases. When using binary evaluation, if a network component (node or link) is completely lost, then the state variable that describes it is equal to “0”, otherwise, when the component is still working, it is equal to “1”.

In flow simulation, each link in the network has a corresponding capacity corresponding to the maximum amount of flow that can pass through it, and each node has a bandwidth and a necessary demand for its normal operation. In such a case, the resilience to a destructive event of a CI network (power grid or transport network) can be represented by the level of its productivity immediately after the event, quantified by the normalized total level of satisfied demand:

$$R_k = \frac{\sum_{n \in N} D_n}{\sum_{n \in N} \hat{D}_n}, \qquad (1)$$

where R_k — resilience of the k network to destruction (the part (percentage) of satisfaction the needs of consumers in power produced by the CI system);

n — node from the set of nodes N of the network k;

D_n — satisfied demand at the node n;

$\hat{D}_n$ — required demand at the node n.

Using the example of the topology of the conditional aggregate network considered above (Fig. 2), it can be noted that in the event of its damage, the stability of Network 2 (R_2) will be significantly reduced due to the lack of satisfied demand in its damaged and destroyed nodes

$$(D_4 = 0;\ D_9 = 0;\ D_5 < \hat{D}_5;$$
$$D_6 < \hat{D}_6;\ D_7 < \hat{D}_7;\ D_8 < \hat{D}_8).$$

Consideration of interdependencies. CI systems, as a rule, are distributed over large geographical areas, are complex collections of interacting subsystems that have an internal dynamic structure and make up a single whole. More importantly, different CIs do not operate in isolation from each other — transport networks often use complex control and information systems, electricity generation requires fuel, and so on. CI systems are physically, geographically, cyber- and logically dependent and interdependent.

For a set of CI networks, their total resilience R to a destructive event can be represented by the weighted sum of the resistance of each of them:

$$R = \Sigma W_k R_k,\ (k \in K), \qquad (2)$$

where W_k — weight coefficient of resilience of the k network (determined by an expert);

R_k — resilience of the k network, which is calculated according to formula (1);

K — the number of networks in total.

The value R in this case characterizes the combined resilience, which determines the share (percentage) of the satisfaction of consumers' need for power produced by interdependent CI systems.

In the case of the topology of the conditional aggregate network (Fig. 2), its aggregate resilience will be reduced by the value of the resilience of Network 2.

The decision-making model for protecting the resilience R of CI networks in this case can be presented in the form of a triple "defense-attack-recovery" (3).

$$\max_{a \in A} \min_{t \in T} \max_{s \in S(a,T)} R, \qquad (3)$$

where

a is a protective investments in the resilience R of CI networks from the set of investments A;

t — resilience threats R from the set of threats T;

s — decisions to restore the operation of CI networks from a set of possible decision options S (a, t) taking into account threats t and investments a to counter them.

The algorithm of the model consists of 3 tasks: 1) the task of protection is to maximize the resilience of CI to possible actions of an attacker; 2) the attacker's task is to minimize CI resilience; 3) the task of recovery is to maximize the resilience of CI after the actions of the attacker.

Consider the operation of the triple algorithm (3) on the example of the CIMM model.

1) Solving the problem of protecting the resilience of R networks against potential actions of an attacker.

At the stage of planning the resilience protection R of the set of energy and transport networks, the control agent A_{Contr} based on the data received from the situational awareness agent A_{SA} makes investment decisions to strengthen weak nodes in interdependent CIs in order to *maximize* the performance of the networks in the worst case of an attack. It is assumed that the protected node should become invulnerable to damage, that is, it should work even under the attack of an attacker. A_{Contr} uses controlling influences and orders agents of prevention of A_{Prev} and protection of A_{Prot} in order to strengthen the resilience of networks.

2) The goal of the attacker's attack is to harm the CI systems in the R network.

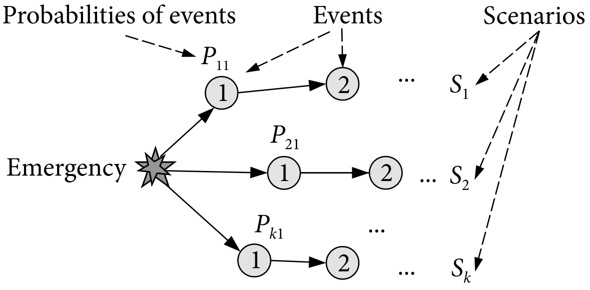

Fig. 3. Oriented graph of emergency scenarios reflecting cascading effects

The attacker chooses the weakest nodes for attack in order to *minimize* the resilience of network nodes.

3) Solving the problem of restoring stable operation of networks after damage to CI systems by an attacker.

In order to mitigate the loss of resilience of CI systems caused by an attacker's attack and to maximize CI performance, the recovery agent A_{Rec} under the control of A_{Contr} carries out repeated (relative to the original) dispatching of network flows, which depends on the investment decisions that were made at the first stage (expressed in the state of protection of the nodes) and the attacker's decisions.

Consideration of cascading effects. Complex interrelationships between different CI systems create new vulnerabilities, and a failure in one of them can propagate and cause failures in connected ones, leading to cascading effects that can affect areas located very far from the emergency zone. For example, the destruction of a certain energy structure can cause disruptions in the operation of industry, in providing the population with communal and information services, in the operation of electric transport; the destruction of the transport structure can lead to disruptions in the supply of necessary goods to the population, industry, and energy structures.

The unfolding of cascading effects is conveniently represented and explored using graph theory. This approach uses graphs consisting of nodes and arcs to describe the relationships between individual CI components or interconnected CIs in a network.

Fig. 3 shows an oriented graph of possible scenarios for the deployment of an imaginary emergency situation at the CI object, that are simulating cascading effects, and the calculation of their probabilities.

As a result of the occurrence of an emergency, it is possible to deploy k scenarios of the development of the situation (S_1, S_2, ..., S_κ), each of which, in turn, can consist of i events.

The probability of the deployment of each scenario can be determined using the theorem of multiplication of probabilities that are independent in the aggregate:

$$P_{S_k} = 1 - \prod (1 - P_{k_i}), \ (i \in S_k), \qquad (4)$$

where

P_{S_k} — the probability of the scenario S_k unfolding;

P_{k_i} — the probability of the occurrence of the i event in the scenario S_k, $k \in K$;

K — the set of possible deployment emergency scenarios.

A mathematical model for assessing the threat of cascading effects for various scenarios for the development of events in the zone affected by the CI object allows us to obtain a set of data for the DSS and the subsequent response of the decision maker to the unfolding of an emergency.

The advantages of the network modeling approach is the ability to analyze the resilience of a CI by modeling failures and cascading effects, first at the level of components (nodes) within a CI, and then between CIs at the system level, that is, bottom-up modeling.

The disadvantages of the network modeling approaches include the fact that they do not provide complete information about CI systems, for example, about the characteristics of flows in real CIs.

Use of Economic Modeling Methods

Economic modeling is the construction of economic (budgetary) models of the behavior of individual CI components and systems in their response to vulnerabilities. The most common economic model for analyzing the interdependencies of CI systems is the input-output model.

The input-output model (Leontief inter-industry balance model) is an economic and mathematical balance model of all purchases, sales and various services between sectors of the economy, based on technological connections of production, representing the inter-industry balance of the economy, when each sector of the economy consumes goods in its production process and services from other industries. Thus, disruption of production in one industry leads to disruption of production in other industries, creating a cascading effect.

To establish mutual unequivocal correspondence between the products of different CIs (for example, electricity generation measured in kilowatt-hours, gas in cubic meters, coal in tons, etc.), the model uses single value indicators — the set price of products. This refers to the physical interdependence of CI systems representing different sectors of the economy. According to Leontief's model, for two interrelated sectors of the economy the following equation is valid:

$$x_i = \Sigma_j a_{ij} x_j + c_i, \qquad (5)$$

where

x_i — total output (costs) of industry products *i*;

a_{ij} — the ratio of the costs of industry *i* to the costs of industry *j* in units of the total production demand for the products of the industry *i* on the products of industry *j*;

c_i — the total volume of production (costs) of the industry *i* intended for final consumption by end consumers (without investments and exports).

It follows from formula (4) that in the case of physical inoperability of industry *j* caused by malicious attacks on it, the output of the industry *i* is reduced due to their interdependence.

In the case of the CIMM model (Fig. 1), if the industry *j* is electric power industry, then the industry *i* is electric transport, which consumes electricity; if industry *j* is transport, then industry *i* is energy systems that require transport for their operation (nuclear, thermal energy).

The model makes it possible to take into account the disruption of one or more CIs and to estimate the ripple economic effects measured by the failure of CIs. In general, input-output models for assessing the failure of individual CIs allow analyze how violations spread between interconnected CIs and how to implement effective measures to mitigate their consequences. Such an assessment makes it possible to analyze the resilience of a system of interconnected CIs or a separate CI and carry out its replacement.

The advantages of the economic modeling approach are its usefulness for analyzing interdependencies at the macroeconomic or sectoral level after natural disasters, malicious attacks or random events.

Disadvantages of the economic modeling approach include its inability to analyze the interdependence between CIs at the component level.

Conclusion

The paper examines various approaches to modeling critical infrastructure and its resilience to enemy threats. In particular, methods of agent modeling, network modeling, system dynamics, and economic modeling are considered. Their advantages and disadvantages are determined. It is noted that each method separately from the others is not effective for a full assessment of the resilience of CI systems to threats.

A multi-agent CI model is proposed, which takes into account the systems of energy, transport and liquidation of the consequences of emergency events. The roles and functions of agents are described.

Using the example of the proposed multi-agent model, the use of system dynamics, network and economic modeling methods is shown. An algorithm for assessing the resilience of a CI network in network modeling based on flows with consideration of interdependencies is given. The calculation of the probabilities of cascading effects is shown. The application of the input-output economic modeling method is described, which makes it possible to estimate material losses caused by the failure of CI systems and their impact on other sectors of the economy.

As a result of the conducted research, we can come to the conclusion that CI systems and their networks are complex dynamic systems with many connections and interdependencies. Each of the considered modeling methods has its own advantages and disadvantages and cannot fully describe the resilience and risks of CIs. However, the integration of these modeling methods into one system makes it possible to carry out a comprehensive analysis of CI resilience and identify weak nodes in order to make investments to increase their resilience.

The results of the work can be useful when building a prototype of a simulation complex for assessing the resilience of CI networks and systems to the threats using various simulation methods.

REFERENCES

1. The Law of Ukraine "On critical infrastructure" at 16.11.2021 no 1882-IX. Update date: 15.06.2022. [online]. Available at: <https://zakon.rada.gov.ua/laws/show/1882-20#Text> [Accessed 01 Feb. 2024]
2. Quyang, M. (2014). "Review on modeling and simulation of interdependent critical infrastructure systems", *Reliability Engineering & System Safety*, 121, pp. 43—60. DOI: http://dx.doi.org/10.1016/j.ress.2013.06.040.
3. Ani, U.P.D., Watson, J.D.Mck., Nurse J.R.C., Cook A., Maple, C. (2019). "A review of critical infrastructure protection approaches: improving security through responsiveness to the dynamic modelling landscape". *Conference: Living in the Internet of Things* (IoT 2019). London, UK, 2019, pp.1—15. DOI: https://doi.org/10.1049/cp.2019.0131.
4. Oliva, G., Panzieri, S., Setola, R. (2012). "Modeling and simulation of critical infrastructures". *WIT Transactions on State of the Art in Science and Engineering*, Vol 54, WIT Press. DOI: https://doi.org/10.2495/978-1-84564-562-5/03.
5. Huang, J., Cui, Y., Zhang, L., Tong, W., Shi, Y., Liu, Z. (2022). "An Overview of Agent-Based Models for Transport Simulation and Analysis". *Journal of Advanced Transportation,* Vol. 2022. https://doi.org/10.1155/2022/1252534.
6. Thompson, J.R., Frezza, D., Necioglu, B., Cohen, M., Hoffman, K., Rosfjord, K. (2019). "Interdependent Critical Infrastructure Model (ICIM): An agent-based model of power and water infrastructure". *International Journal of Critical Infrastructure Protection*, 24, pp. 144–165. http://dx.doi.org/10.1016/j.ress.2013.06.040.
7. Sako, D.J.S, Igiri, C.G., Bennet, E.O., Deedam, F.B. (2024). "ESARS: A Situation-Aware Multi-Agent System for Real-Time Emergency Response Management". *European Journal of Information Technologies and Computer Science,* 4 (1), pp. 1—8. DOI: https://doi.org/10.24018/compute.2024.4.1.83.
8. Mukhopadhyay, A., Vazirizade, S.M. "Multi Agent Systems for Emergency Response". [online]. Available at: <https://ayanmukhopadhyay.github.io/files/talks/MultiAgentEmergency.pdf> [Accessed 01 Feb. 2024]
9. Ferrario, E. (2014). "System-of-systems modeling and simulation for the risk analysis of industrial installations and critical infrastructures". *Engineering Sciences* [*physics*]. Ecole Centrale Paris, English. NNT: 2014ECAP-0046ff. https://theses.hal.science/tel-01127194/.
10. Fang, Y., Zio, E. (2019). "Game-Theoretic Decision Making for the Resilience of Interdependent Infrastructures Exposed to Disruptions". In: Gritzalis, D., Theocharidou, M., Stergiopoulos, G. (eds) *Critical Infrastructure Security and Resilience. Advanced Sciences and Technologies for Security Applications*. Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-00024-0_6.
11. Schotten, R., Bachmann, D. (2023). "Critical infrastructure network modelling for flood risk analyses: Approach and proof of concept in Accra, Ghana". *Journal of Flood Risk Managemen*. DOI: https://doi.org/10.1111/jfr3.12913.
12. Zio, E., Sansavini, G. (2011). "Modeling Interdependent Network Systems for Identifying Cascade-Safe Operating Margins". *IEEE Transactions on Reliability*, 60 (1), pp. 94—101. DOI: https://doi.org/10.1109/TR.2010.2104211.
13. Newman, D.E., Nkei, B., Carreras, B. A., Dobson, I., Lynch, V.E., & Gradney, P. (2005). "Risk assessment in complex interacting infrastructure systems". *Proceedings of the 38th Annual Hawaii International Conference on ystem Sciences*, Big Island, HI, USA, 2005, 63 p. DOI: https://doi.org/10.1109/HICSS.2005.524.
14. Hellmann, F., Schultz, P., Grabow, C., Heitzig, J., & Kurths, J. (2015). "Survivability: A unifiying concept for the transient resilience of deterministic dynamical systems". *arXiv*. DOI: https://doi.org/10.48550/arXiv.\1506.01257.
15. Armenia, S., Cardazzone, A., Carlini, C , Assogna, P., D'Alessandro, C. N., Limone, E., Brein, E. (2014). "A system dynamics approach to critical infrastructures interdependency analysis: the experience of the Crisadmin project. *In Proceedings of the 32nd International Conference of the System Dynamics Society*.

16. Rodrigue, J-P., Ducruet, C. The Geography of Transport System. 2.1 — The Geography of Transportation Networks. [online]. Available at: <https://www.fh777.org/index-31.html> [Accessed 01 Feb. 2024]
17. NATO's Chemical, Biological, Radiological and Nuclear (CBRN) Defence Policy. [online]. Available at: <https://www.nato.int/cps/en/natohq/official_texts_197768.htm> [Accessed 05 July 2023]

Received 01.05.2024

ЛІТЕРАТУРА

1. Закон України "Про критичну інфраструктуру" від 16.11.2021 №1882-IX. Дата оновлення: 15.06.2022. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text.
2. Quyang M. Review on modeling and simulation of interdependent critical infrastructure systems. Reliability Engineering & System Safety. 121 (2014). pp. 43—60. https://doi.org/10.1016/j.ress.2013.06.040.
3. Ani U.P.D., Watson J.D. Mck., Nurse J.R.C., Cook A., Maple C. A review of critical infrastructure protection approaches: improving security through responsiveness to the dynamic modelling landscape. Conference: Living in the Internet of Things (IoT 2019). Volume: 2019. DOI: https://doi.org/10.1049/cp.2019.0131.
4. Oliva G., Panzieri S., Setola R. Modeling and simulation of critical infrastructures. WIT Transactions on State of the Art in Science and Engineering. Vol 54. WIT Press, 2012. DOI: https://doi.org/10.2495/978-1-84564-562-5/03.
5. Huang J., Cui Y., Zhang L., Tong W., Shi Y., Liu Z. An Overview of Agent-Based Models for Transport Simulation and Analysis. Journal of Advanced Transportation Vol. 2022. URL: https://doi.org/10.1155/2022/1252534.
6. Thompson J.R., Frezza D., Necioglu B., Cohen M., Hoffman K., Rosfjord K. Interdependent Critical Infrastructure Model (ICIM): An agent-based model of power and water infrastructure. International Journal of Critical Infrastructure Protection. 24 (2019). pp. 144—165.
7. Sako D.J.S, Igiri C.G., Bennet E.O., Deedam F.B. ESARS: A Situation-Aware Multi-Agent System for Real-Time Emergency Response Management. European Journal of Information Technologies and Computer Science Vol. 4, Issue 1. February 2024.
8. Mukhopadhyay A., Vazirizade S.M. Multi Agent Systems for Emergency Response. URL: https://ayanmukhopadhyay.github.io/files/talks/MultiAgentEmergency.pdf.
9. Ferrario E. System-of-systems modeling and simulation for the risk analysis of industrial installations and critical infrastructures. Engineering Sciences [physics]. Ecole Centrale Paris, 2014. English. NNT : 2014ECAP0046ff. URL: https://theses.hal.science/tel-01127194/
10. Fang Y., Zio E. Game-Theoretic Decision Making for the Resilience of Interdependent Infrastructures Exposed to Disruptions. Gritzalis Dimitris; Theocharidou Marianthi; Stergiopoulos George. Critical Infrastructure Security and Resilience – Theories, Methods, Tools and Technologies, 2019, pp. 97—114. DOI: https://doi.org/10.1007/978-3-030-00024-0_6.
11. Schotten R., Bachmann D. "Critical infrastructure network modelling for flood risk analyses: Approach and proof of concept in Accra, Ghana". Journal of Flood Risk Managemen, 2023. DOI: https://doi.org/10.1111/jfr3.12913.
12. Zio E., Sansavini G. Modeling Interdependent Network Systems for Identifying Cascade-Safe Operating Margins. IEEE Transactions on Reliability, 60 (1), 2011, pp. 94—101. DOI: https://doi.org/10.1109/TR.2010.2104211.
13. Newman D.E., Nkei B., Carreras B.A., Dobson I., Lynch V.E., Gradney P. Risk assessment in complex interacting infrastructure systems. In: Proceedings of the Thirty-eighth Hawaii international conference on system science. Big Island, HI, USA, 2005, 63 p. DOI: https://doi.org/10.1109/HICSS.2005.524.
14. Hellmann F., Schultz P.l, Grabow C., Heitzig J., Kurths J. Survivability: A Unifiying Concept for the Transient Resilience of Deterministic Dynamical Systems. DOI: http://arxiv.org/abs/1506.01257v1.
15. Armenia S., Cardazzone A., Carlini C , Assogna P., D'Alessandro C.N. , Limone E., Brein E. A System Dynamics approach to Critical Infrastructures Interdependency Analysis: the experience of the CRISADMIN Project. In Proceedings of the 32nd International Conference of the System Dynamics Society.
16. Rodrigue J-P., Ducruet C. "The Geography of Transportation Networks". The Geography of Transport System. Site. URL: https://www.fh777.org/index-31.html.
17. NATO's Chemical, Biological, Radiological and Nuclear (CBRN) Defence Policy. NATO, 05 Jul. 2022. URL: https://www.nato.int/cps/en/natohq/official_texts_197768.htm.

Надійшла 01.05.2024

І.М. Оксанич, к.т.н, с.н.с., відділ Інтелектуальних інформаційно-аналітичних систем,
Інститут проблем математичних машин і систем (ІПММС НАН України),
03187, м. Київ, просп. Академіка Глушкова, 42, Україна,
ORCID: https://orcid.org/0000-0002-1208-3427,
inokc2018@gmail.com
В.Ф. Гречанінов, к.т.н., зав. відділом Інтелектуальних інформаційно-аналітичних систем,
Інститут проблем математичних машин і систем (ІПММС НАН України),
03187, м. Київ, просп. Академіка Глушкова, 42, Україна,
ORCID: https://orcid.org/0000-0001-6268-3204,
vgrechaninov@gmail.com
А.В. Лопушанський, наук. співробітник, відділ Інтелектуальних інформаційно-аналітичних систем,
Інститут проблем математичних машин і систем (ІПММС НАН України),
03187, м. Київ, просп. Академіка Глушкова, 42, Україна,
ORCID: https://orcid.org/0000-0002-4840-0236,
anatoliy.lopushanskyi@gmail.com
І.Є. Новгородський, старший науковий співробітник,
Інститут проблем математичних машин і систем (ІПММС НАН України),
ORCID: https://orcid.org/0000-0002-6498-1819,
03187, м. Київ, просп. Академіка Глушкова, 42, Україна,
stanislavnovgorodskij@gmail.com
В.Ф. Головський, старший науковий співробітник,
Інститут проблем математичних машин і систем (ІПММС НАН України),
03187, м. Київ, просп. Академіка Глушкова, 42, Україна,
ORCID: https://orcid.org/0009-0001-4959-0940,
rusgol05@gmail.com

ІНТЕГРАЦІЯ РІЗНИХ ПІДХОДІВ ДО МОДЕЛЮВАННЯ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Вступ. Широкомасштабна війна Російської Федерації проти України, підвищення рівня терористичних загроз, а також світові тенденції до тяжких наслідків надзвичайних ситуацій (НС) природного та техногенного характеру зумовили актуалізацію питання захисту систем, об'єктів та ресурсів, які критично важливі для життєдіяльності суспільства та забезпечення національної безпеки, тобто захисту об'єктів критичної інфраструктури (КІ). Аналіз викликів та загроз, що впливають на стійкість об'єктів КІ, оцінка стану їхньої захищеності з метою виявлення та запобігання інцидентам, а також розробка комплексу заходів щодо контролю за ризиками безпеки на об'єктах КІ є першорядним завданням та проблемою в державі.

Мета статті. Метою статті є аналіз різних підходів до моделювання стійкості КІ та побудова моделі їх інтеграції для всебічного аналізу, захисту та відновлення. Предметом досліджень є система систем КІ, у склад якої входять системи енергетики, транспорту та ліквідації наслідків НС.

Результати. Проведено аналіз чотирьох підходів до моделювання стійкості КІ: агентного; мережевого; підходу, що базується на системній динаміці; економічного підходу. Розроблено структуру мультиагентної моделі систем КІ енергетики, транспорту та ліквідації наслідків НС. Описано вхідні та вихідні дані моделі, ролі та функції агентів. На основі розробленої мультиагентної моделі показано застосування методів системної динаміки, мережевого моделювання (заснованого на топології мережі та на потоках) та економічного моделювання. Наведено алгоритм оцінки стійкості мережі КІ при моделюванні, заснованому на потоках з урахуванням взаємозалежностей. Показано використання методу економічного моделювання "витрати — випуск".

Висновки. У результаті проведених досліджень можна дійти висновку, що системи КІ та їх мережі є складними динамічними системами з безліччю зв'язків і взаємозалежностей. Кожен із розглянутих методів моделювання має свої переваги та недоліки і не може повністю описати стійкість та ризики КІ. Однак інтеграція цих методів моделювання в одну систему дає змогу провести всебічний аналіз стійкості КІ та виявити слабкі вузли з метою вкладення інвестицій для підвищення їхньої стійкості.

Результати роботи можуть бути корисними при побудові прототипу моделюючого комплексу для оцінки стійкості мереж та систем КІ до загроз з використанням різних методів моделювання.

Ключові слова: *моделювання стійкості критичної інфраструктури, агентне моделювання, мережеве моделювання, методи системної динаміки.*