УДК 004.652:004.056.5:332.1 DOI: 10.31673/2412-9070.2026.049815

O. KORCHENKO[1], Doctor of Technical Sciences, Professor;
ORCID ID: 0000-0003-3376-0631
V. KHARCHENKO[2], Doctor of Technical Sciences, Professor;
ORCID ID: 0000-0001-5352-077X
Yu. KHOKHLACHOVA[1,3], Candidate of Technical Sciences, Professor;
ORCID ID: 0000-0002-0787-5112
Yu. ZHUROV[4], Master's degree in cybersecurity,
ORCID ID: 0000-0002-8276-2230

[1]State University of Information and Communication Technologies, Kyiv
[2]M.E. Zhukovsky National Aerospace University "Kharkiv Aviation Institute", Kharkiv
[3]State University of Trade and Economics, Kyiv
[4]SMB Cybersecurity Advisors, Florida, US

SUSTAINABLE DEVELOPMENT OF SMART REGIONS: A SET-THEORETIC DATA MODEL FOR ASSESSING THE CYBER RESILIENCE OF CRITICAL INFRASTRUCTURE ENTITIES

The increasing complexity and intensity of cyber threats to critical infrastructure entities (CIE) necessitate a transition from classical protection methods to comprehensive cyber resilience strategies. The aim of this research is to create a formal mathematical toolkit for assessing the ability of infrastructure entities to anticipate attacks, withstand them, recover, and adapt to changes. This work proposes a set-theoretic data model (STDM) that, for example, generalizes and formalizes the hierarchical structure of the MITRE Cyber Resiliency Engineering Framework (CREF). The research methodology is based on the introduction of sets of identifiers for goals, objectives, sub-objectives, and basic resilience measures, as well as on the development of a unique indexing system for their unambiguous mapping. The modeling results create a rigorous mathematical foundation for systematic cyber resilience analysis, enabling the identifycation of protection gaps and informed resource prioritization. For instance, the generalization of CREF through a set-theoretic approach ensures high model flexibility to dynamic changes in the threat landscape and specific requirements of different types of CIE. It is concluded that the implementation of the model directly contributes to the long-term reliability and ensures the effectiveness of sustainable development of critical infrastructure in smart regions, aligning with the UN Sustainable Development Goals (SDGs 9 and 11) in the context of building resilient and secure socio-technical systems.

Keywords: sustainable development, smart regions, cyber resilience, critical infrastructure entities, set-theoretic data model, MITRE CREF, resilience assessment, decision support.

Introduction

The resilience of CIE is inextricably linked to the concept of sustainable development of smart regions. Ensuring the continuous operation of vital services such as energy, water supply, transport, etc., is a necessary condition for economic stability and social well-being. From the perspective of sustainable development of smart regions, cyber resilience is not merely a technical requirement but a strategic capability that supports the United Nations (UN) Sustainable Development Goals, particularly SDG 9 (Industry, Innovation and Infrastructure) and SDG 11 (Sustainable Cities and Communities).

The current stage of digitalization of critical infrastructure is characterized by exponential growth in the complexity and interconnectedness of control systems, accompanied by a corresponding

increase in the set of attacks and vulnerabilities. CIE refers to energy systems, transportation networks, water supply, telecommunications, financial institutions, healthcare systems, etc., which are be-coming increasingly dependent on digital technologies, making them attractive targets for adversaries – cybercriminals, hacktivists, state actors, etc.

Statistics on cyber incidents demonstrate a negative trend related to attacks on critical infrastructure, which are becoming not only more frequent but also more sophisticated and destructive. For example, DDoS attacks can paralyze entire industries, phishing campaigns compromise privileged user accounts, and Advanced Persistent Threats (APT) provide attackers with long-term unauthorized access to critical systems. Particularly dangerous are attacks on supply chains and "zero-day" attacks that exploit previously unknown vulnerabilities.

The traditional cybersecurity paradigm, based on the principle of "prevention and detection," shows its insufficiency in conditions where the assumption of inevitable successful compromise becomes realistic. This has led to the emergence of the concept of cyber resilience as one of the fundamental bases for sustainable development of smart regions, characterized by the system's ability not only to resist attacks but also to maintain critical functions during an incident, quickly recover, and adapt to new threats.

For example, CREF, developed by the MITRE Corporation [1] with support from the U.S. National Security Agency, offers a comprehensive approach to ensuring cyber resilience through structuring goals, objectives, sub-objectives, and specific technical and organizational actions. However, the practical application of CREF is complicated by the absence of formalized mathematical models that would allow effective assessment of cyber resilience levels, comparison of different protection strategies, and justification of management decisions regarding the allocation of limited resources to ensure the effectiveness of sustainable development of smart regions.

The use of a set-theoretic approach provides the opportunity to create powerful tools for formalizing complex hierarchical structures, establishing relationships between elements of different levels, and creating a mathematical foundation for developing assessment algorithms. Its application, for example, to model CREF allows the transition from qualitative descriptions to quantitative metrics of cyber resilience (cyber-resilience).

The creation of a formal set-theoretic model for assessing and enhancing cyber resilience will enable the maintenance of infrastructure durability and reliability, ensuring the sustainable development of smart regions in an increasingly volatile digital environment.

The growing number and complexity of cyberattacks on CIE creates serious challenges for national security and the stability of vital systems. Modern threats have high potential not only to disrupt the normal functioning of critical systems but also to cause cascading failures with long-term negative consequences for the sustainable development of smart regions. Traditional approaches to cybersecurity, which focus primarily on point protection and incident prevention, prove insufficient in conditions where complete avoidance of threats becomes practically impossible. Therefore, the concept of cyber resilience, as a fundamental component of ensuring the effectiveness of sustainable development of smart regions, provides systems with the ability to anticipate threats, withstand attacks, quickly recover, and adapt to new operating conditions, enabling the creation of cyber-resilient systems for CIE. One of the first steps in creating such systems is the development of a set-theoretic data model for assessing the cyber resilience of CIE. Such a model will allow formalization, for example, of the CREF structure, establish quantitative relationships between goals, objectives, and actions, and create a mathematical foundation for calculating integral indicators of CIE resilience under various cyber threat conditions. Therefore, the development of STDM for assessing the cyber resilience of CIE, as an element of ensuring sustainable development of smart regions, is a relevant scientific task.

Statement of the problem

Ensuring the cyber resilience of CIE, as a condition for ensuring the effectiveness of sustainable development of smart regions, is a complex multi-level task requiring coordination of efforts at strategic, tactical, and operational levels. For example, CREF defines four strategic goals (anticipate, with-

stand, recover, adapt), eight tactical objectives, and dozens of sub-objectives and specific actions to achieve them. However, the absence of a unified formalized model integrating all these elements creates a number of critical problems:

- the unstructured representation of knowledge about cyber resilience complicates the planning process for protective measures. Decision-makers face the need to analyze large amounts of documentation without a clear understanding of the relationships between goals at different levels and their relative importance for a specific infrastructure object;
- the absence of quantitative metrics makes it impossible to objectively assess the current level of cyber resilience and compare alternative strategies for its improvement. Management decisions are often made based on expert assessments without sufficient mathematical justification, which reduces the efficiency of using limited financial and human resources;
- the absence of a formalized connection between types of cyber threats and necessary basic cyber resilience measures complicates the risk-oriented planning process. Different threats (DDoS, phishing, APT, supply chain attacks, etc.) require different combinations of protective measures, but determining the optimal set of basic countermeasures for a specific threat profile remains a non-trivial task;
- the dynamic nature of the cyber threat landscape requires constant adaptation of cyber resilience strategies. Without a formalized model that allows quick reassessment of priorities and reallocation of resources in response to new threats, organizations remain vulnerable to dynamically evolving attacks;
- the complexity of integrating the concept of cyber resilience into the design and modernization process of CIE systems. System engineers and architects need clear, mathematically formalized recommendations for the informed selection and implementation of specific cyber resilience mechanisms at different stages of the system lifecycle.

Thus, to address these issues, at the first stage there is a need to develop a formalized STDM that will allow:

- structuring the hierarchy of all related elements ensuring the implementation of the cyber resilience concept through mathematical relationships;
- implementing unambiguous identification and indexing of all repeated cyber resilience measures;
- introducing quantitative indicators of goal importance and effectiveness of implementing basic cyber resilience measures;
- establishing a formal connection between sets of threats and basic cyber resilience measures;
- creating a mathematical foundation for calculating integral indicators of cyber-resilience;
- ensuring the possibility of adapting the model to the specifics of particular CIE.

This will allow the transition from qualitative descriptions of cyber resilience to quantitative assessment methods, which is a necessary condition for making informed management decisions in the field of CIE protection to ensure the effectiveness of sustainable development of smart regions.

Research objectives and tasks

The purpose of the article is to formalize the process of forming generalized data sets necessary for implementing the process of assessing the cyber resilience of CIE as an element of ensuring the effectiveness of sustainable development of smart regions.

To achieve the stated goal, it is necessary to solve the following **tasks**:

1. Formalize the hierarchical structure for implementing the assessment process by introducing sets of identifiers for goals, objectives, sub-objectives, and basic cyber resilience measures.
2. Based on the set-theoretic approach, establish mathematical relationships between elements of different hierarchy levels in assessment processes.

3. Develop an indexing system for unambiguous identification of each basic cyber resilience measure with binding to the corresponding sub-objective, objective, and goal.

4. Formalize the set of cyber threats and establish the relationship between types of threats and necessary basic measures for ensuring cyber resilience.

5. Create a generalized STDM and its structure that integrates all elements involved in the process of assessing the cyber resilience of CIE.

Analysis of recent studies and publications

The problem of ensuring cyber resilience of CIE is actively studied by the international and domestic scientific community. Based on the research tasks, let us define four key criteria (*formalization of hierarchical structure of cyber resilience elements* (C1); *establishment of mathematical relationships between elements of different hierarchy levels* (C2); *creation of indexing system for basic cyber resilience measures* (C3); *formalization of relationships between cyber threats and basic cyber resilience measures* (C4)) for analyzing existing approaches to implementing the process of assessing the cyber resilience of CIE described in known publications.

In the mentioned publications, there are separate studies linking threat types with countermeasures in specific contexts, but there is no generalized formalized model for mapping the set of cyber threats to the set of basic cyber resilience measures for CIE. A consolidated analysis of studies by criteria is presented in Table 1, where «0», «– –», «–», «– +», «+» respectively reflect development levels in the specified source as "Absent", "Very Low", "Low", "Below Average", "Average".

Table 1

Consolidated Analysis of Studies by Criteria

Source	C1: Hierarchy Formalization	C2: Mathematical Relationships	C3: Indexing Formalization	C4: Threats-Measures
[1]	+	– –	0	–
[2]	+	– –	– –	–
[3]	+	–	–	–
[4]	– +	–	– –	0
[5], [9], [18]	–	0	0	0
[6], [12]	0	+	0	0
[7], [16]	–	–	0	–
[8]	0	–	0	–
[10]	0	–	0	– –
[11]	–	– –	0	0
[13]	–	0	0	–
[14]	– +	+	–	0
[15], [29]	–	– +	0	–
[17]	– –	0	0	0
[19], [27]	0	0	0	0
[20], [23], [25]	–	+	0	0
[21]	0	– +	0	0
[22]	0	– +	0	– –
[24]	0	–	0	0
[26]	–	– +	0	– –
[28]	– +	– +	0	0
[30]	–	– +	0	0

Summarizing the results of the analysis of recent research, we can note:

1. *Critical gaps in formalization* regarding C1-C3: Despite the availability of structured frameworks (CREF, NIST), there is no generalized set-theoretic formalization of hierarchical cyber resilience structures with an unambiguous indexing system;
2. *Absence of formal mappings* regarding C4: There are no general models that formally define correspondence between types of cyber threats and necessary basic cyber resilience measures;
3. *Complexity of transition from theoretical provisions to practical solutions*: Conceptual frameworks (CREF, NIST) are widely used, but their practical application is complicated by the absence of formalized models for implementing automated assessment processes;
4. *Limited adaptability*: Most studies focus either on general principles (without specifics) or on narrow domains (SCADA, ICS); generalized mathematical data models that enable adaptation to different types of CIE are absent.

Taking into account the conducted analysis and research relevance, there arises a need to develop an appropriate STDM. It will enable generalization and formalization of the hierarchical structure of cyber resilience parameters, ensure unambiguous identification of all elements, establish relationships between components of different levels, and create a mathematical foundation for automating the process of assessing CIE resilience under dynamic cyber threat landscape conditions.

Research results

To build the necessary data model, we will use a set-theoretic approach. For this, we introduce a set of goal identifiers that will enable ensuring the cyber resilience of CIE:

$$\boldsymbol{GS} = \left\{ \bigcup_{i=1}^{n} \boldsymbol{GS}_i \right\} = \left\{ \boldsymbol{GS}_1, \boldsymbol{GS}_2, ..., \boldsymbol{GS}_n \right\}, \tag{1}$$

where $i = \overline{1,n}$, and n – number of goals.

For example, when n=4 taking into account CREF goals [1], expression (1) can be written as:

$$\boldsymbol{GS} = \left\{ \bigcup_{i=1}^{4} \boldsymbol{GS}_i \right\} = \left\{ \boldsymbol{GS}_1, \boldsymbol{GS}_2, \boldsymbol{GS}_3, \boldsymbol{GS}_4 \right\} = \left\{ \boldsymbol{ANT}, \boldsymbol{WITH}, \boldsymbol{REC}, \boldsymbol{AD} \right\}, \tag{2}$$

where $\boldsymbol{GS}_1$=**ANT** identifier of the first goal – «**ANTICIPATE**», $\boldsymbol{GS}_2$ =**WITH** identifier of the second – «**WITHSTAND**», $\boldsymbol{GS}_3$ =**REC** identifier of the third – «**RECOVER**», and $\boldsymbol{GS}_4$ =**AD** identifier of the fourth goal «**ADAPT**».

Next, we introduce a set of objective identifiers ***OS*** that need to be solved to achieve the goals whose identifiers are defined in the set ***GS***:

$$\boldsymbol{OS} = \left\{ \bigcup_{i=1}^{o} \boldsymbol{OS}_i \right\} = \left\{ \boldsymbol{OS}_1, \boldsymbol{OS}_2, ..., \boldsymbol{OS}_o \right\}, \tag{3}$$

where $\boldsymbol{OS}_i$ – identifier of the i-th objective ($i = \overline{1,o}$), and o – number of objective identifiers.

For example, when o=8 taking into account [1], formula (3) can be represented as:

$$\boldsymbol{OS} = \left\{ \bigcup_{i=1}^{o} \boldsymbol{OS}_i \right\} = \left\{ \boldsymbol{OS}_1, \boldsymbol{OS}_2, ..., \boldsymbol{OS}_8 \right\} = \left\{ \boldsymbol{PA}, \boldsymbol{PR}, \boldsymbol{CN}, \boldsymbol{CS}, \boldsymbol{RE}, \boldsymbol{UN}, \boldsymbol{TR}, \boldsymbol{RA} \right\}, \tag{4}$$

where $\boldsymbol{OS}_1$=***PA***, $\boldsymbol{OS}_2$ =***PR***, $\boldsymbol{OS}_3$ =***CN***, $\boldsymbol{OS}_4$ =***CS***, $\boldsymbol{OS}_5$ =***RE***, $\boldsymbol{OS}_6$ =***UN***, $\boldsymbol{OS}_7$ =***TR***, $\boldsymbol{OS}_8$ =***RA*** are also identifiers from the first to eighth objective «**PREVENT/AVOID**», «**PREPARE**», «**CONTINUE**», «**CONSTRAIN**», «**RECONSTITUTE**», «**UNDERSTAND**», «**TRANSFORM**», «**RE-ARCHITECT**» respectively.

To solve the objectives defined by their identifiers in the set $\boldsymbol{OS}_i$ ($i=\overline{1,o}$) (see (2)), we introduce a set of sub-objective identifiers $\boldsymbol{OS}_{ij}$ associated with solving each *i*-th objective:

$$\boldsymbol{OS}_i=\left\{\bigcup_{j=1}^{s_i}\boldsymbol{OS}_{ij}\right\}=\left\{\boldsymbol{OS}_{i1},\boldsymbol{OS}_{i2},\boldsymbol{OS}_{i3},...,\boldsymbol{OS}_{is_i}\right\}, \quad (5)$$

where $\boldsymbol{OS}_{ij}$ – identifier of each *j*-th sub-objective ($j=\overline{1,s_i}$) of the *i*-th objective, and s_i ($i=\overline{1,o}$) – number of sub-objectives necessary to solve the *i*-th objective.

Taking into account (5), expression (3) can be written as follows:

$$\boldsymbol{OS}=\left\{\bigcup_{i=1}^{o}\left\{\bigcup_{j=1}^{s_i}\boldsymbol{OS}_{ij}\right\}\right\}=\left\{\begin{array}{l}\left\{\boldsymbol{OS}_{11},\boldsymbol{OS}_{12},...,\boldsymbol{OS}_{1s_1}\right\},\\ \left\{\boldsymbol{OS}_{21},\boldsymbol{OS}_{22},...,\boldsymbol{OS}_{2s_2}\right\},...,\\ \left\{\boldsymbol{OS}_{o1},\boldsymbol{OS}_{o2},...,\boldsymbol{OS}_{os_o}\right\}\end{array}\right\}. \quad (6)$$

For example, based on [1], formula (5) when $s_1=s_4=s_5=s_6=4$, $s_2=s_3=3$, $s_7=s_8=2$ has the form:

$$\boldsymbol{OS}_1=\left\{\bigcup_{j=1}^{4}\boldsymbol{OS}_{ij}\right\}=\left\{\boldsymbol{OS}_{11},\boldsymbol{OS}_{12},\boldsymbol{OS}_{13},\boldsymbol{OS}_{14}\right\}=\left\{\boldsymbol{PA.S1},\boldsymbol{PA.S2},\boldsymbol{PA.S3},\boldsymbol{PA.S4}\right\},$$

where for the first objective $\boldsymbol{OS}_{11}=\boldsymbol{PA.S1}$ =«**APPLY BASIC HYGIENE AND RISK-ORIENTED CONTROLS**», $\boldsymbol{OS}_{12}=\boldsymbol{PA.S2}$ =«**LIMIT IMPACT OF THREATENING EVENTS**», $\boldsymbol{OS}_{13}=\boldsymbol{PA.S3}$ =«**REDUCE ADVERSARY'S PERCEIVED ADVANTAGES**», $\boldsymbol{OS}_{14}=\boldsymbol{PA.S4}$ =«**CHANGE CONFIGURATIONS BASED ON THREAT DATA**»;

$$\boldsymbol{OS}_2=\left\{\bigcup_{j=1}^{3}\boldsymbol{OS}_{ij}\right\}=\left\{\boldsymbol{OS}_{21},\boldsymbol{OS}_{22},\boldsymbol{OS}_{23}\right\}=\left\{\boldsymbol{PR.S1},\boldsymbol{PR.S2},\boldsymbol{PR.S3}\right\},$$

where for the second objective $\boldsymbol{OS}_{21}=\boldsymbol{PR.S1}$ =«**CREATE AND MAINTAIN CYBER STRATEGIES**», $\boldsymbol{OS}_{22}=\boldsymbol{PR.S2}$ =«**PROVIDE RESOURCES NECESSARY FOR CYBER MEASURES**», $\boldsymbol{OS}_{23}=\boldsymbol{PR.S3}$ =«**VERIFY REALISM OF CYBER PLANS FOR IMPLEMENTING MEASURES**»;

$$\boldsymbol{OS}_3=\left\{\bigcup_{j=1}^{3}\boldsymbol{OS}_{ij}\right\}=\left\{\boldsymbol{OS}_{31},\boldsymbol{OS}_{32},\boldsymbol{OS}_{33}\right\}=\left\{\boldsymbol{CN.S1},\boldsymbol{CN.S2},\boldsymbol{CN.S3}\right\},$$

where for the third objective $\boldsymbol{OS}_{31}=\boldsymbol{CN.S1}$ =«**MINIMIZE SERVICE QUALITY DEGRADATION**», $\boldsymbol{OS}_{32}=\boldsymbol{CN.S2}$ =«**MINIMIZE SERVICE INTERRUPTIONS**», $\boldsymbol{OS}_{33}=\boldsymbol{CN.S3}$ =«**ENSURE CURRENT FUNCTIONING IS CORRECT**»;

$$\boldsymbol{OS}_4=\left\{\bigcup_{j=1}^{4}\boldsymbol{OS}_{ij}\right\}=\left\{\boldsymbol{OS}_{41},\boldsymbol{OS}_{42},\boldsymbol{OS}_{43},\boldsymbol{OS}_{44}\right\}=\left\{\boldsymbol{CS.S1},\boldsymbol{CS.S2},\boldsymbol{CS.S3},\boldsymbol{CS.S4}\right\},$$

where for the fourth objective $\boldsymbol{OS}_{41}=\boldsymbol{CS.S1}$ =«**IDENTIFY POTENTIAL DAMAGE**», $\boldsymbol{OS}_{42}=\boldsymbol{CS.S2}$ =«**ISOLATE RESOURCES TO LIMIT FUTURE OR FURTHER DAMAGE**», $\boldsymbol{OS}_{43}=\boldsymbol{CS.S3}$ =«**MOVE RESOURCES TO LIMIT FUTURE OR FURTHER DAMAGE**», $\boldsymbol{OS}_{44}=\boldsymbol{CS.S4}$ =«**CHANGE OR REMOVE RESOURCES AND HOW THEY ARE USED TO LIMIT FUTURE OR FURTHER DAMAGE**»;

$$\boldsymbol{OS}_5 = \left\{ \bigcup_{j=1}^{4} \boldsymbol{OS}_{ij} \right\} = \left\{ \boldsymbol{OS}_{51}, \boldsymbol{OS}_{52}, \boldsymbol{OS}_{53}, \boldsymbol{OS}_{54} \right\} = \left\{ \boldsymbol{RE.S1}, \boldsymbol{RE.S2}, \boldsymbol{RE.S3}, \boldsymbol{RE.S4} \right\},$$

where for the fifth objective $\boldsymbol{OS}_{51} = \boldsymbol{RE.S1}$ =«**IDENTIFY DAMAGE AND UNTRUSTWORTHY RESOURCES**», $\boldsymbol{OS}_{52} = \boldsymbol{RE.S2}$ =«**RESTORE FUNCTIONALITY**», $\boldsymbol{OS}_{53} = \boldsymbol{RE.S3}$ =«**HEIGHTEN PROTECTIONS DURING RECONSTITUTION**», $\boldsymbol{OS}_{54} = \boldsymbol{RE.S4}$ =«**DETERMINE THE TRUSTWORTHINESS OF RESTORED OR RECONSTRUCTED RESOURCES**»;

$$\boldsymbol{OS}_6 = \left\{ \bigcup_{j=1}^{4} \boldsymbol{OS}_{ij} \right\} = \left\{ \boldsymbol{OS}_{61}, \boldsymbol{OS}_{62}, \boldsymbol{OS}_{63}, \boldsymbol{OS}_{64} \right\} = \left\{ \boldsymbol{UN.S1}, \boldsymbol{UN.S2}, \boldsymbol{UN.S3}, \boldsymbol{UN.S4} \right\},$$

where for the sixth objective $\boldsymbol{OS}_{61} = \boldsymbol{UN.S1}$ =«**UNDERSTAND ADVERSARIES**», $\boldsymbol{OS}_{62} = \boldsymbol{UN.S2}$ =«**UNDERSTAND DEPENDENCIES ON AND AMONG CYBER RESOURCES**», $\boldsymbol{OS}_{63} = \boldsymbol{UN.S3}$ = **UNDERSTAND THE STATUS OF RESOURCES WITH RESPECT TO THREAT EVENTS**», $\boldsymbol{OS}_{64} = \boldsymbol{UN.S4}$ =«**UNDERSTAND THE EFFECTIVENESS OF CYBER SECURITY AND CYBER RESILIENCY CONTROLS**»;

$$\boldsymbol{OS}_7 = \left\{ \bigcup_{j=1}^{2} \boldsymbol{OS}_{ij} \right\} = \left\{ \boldsymbol{OS}_{71}, \boldsymbol{OS}_{72} \right\} = \left\{ \boldsymbol{TR.S1}, \boldsymbol{TR.S2} \right\},$$

where for the seventh objective $\boldsymbol{OS}_{71} = \boldsymbol{TR.S1}$ =«**REDEFINE MISSION THREADS FOR AGILITY**», $\boldsymbol{OS}_{72} = \boldsymbol{TR.S2}$ =«**REDEFINE MISSION/BUSINESS FUNCTIONS TO MITIGATE RISKS**»;

$$\boldsymbol{OS}_8 = \left\{ \bigcup_{j=1}^{2} \boldsymbol{OS}_{ij} \right\} = \left\{ \boldsymbol{OS}_{81}, \boldsymbol{OS}_{82} \right\} = \left\{ \boldsymbol{RA.S1}, \boldsymbol{RA.S2} \right\},$$

where for the eighth objective $\boldsymbol{OS}_{81} = \boldsymbol{RA.S1}$ =«**RESTRUCTURE SYSTEMS OR SUB-SYSTEMS TO REDUCE RISKS**», $\boldsymbol{OS}_{82} = \boldsymbol{RA.S2}$ =«**MODIFY SYSTEMS OR SUB-SYSTEMS TO REDUCE RISKS**».

To solve the sub-objectives defined in the set of their identifiers $\boldsymbol{OS}_{ij}$ ($i = \overline{1,o}$; $j = \overline{1,s_i}$) (see (3)), we introduce a set of functions $OS_{ijk}\left(\bigcup_{l=1}^{a_{ijk}} A_{ijkl}\right)$ for implementing basic measures of each s_i-th sub-objective based on a set of corresponding methods $\bigcup_{l=1}^{a_{ijk}} A_{ijkl}$, then:

$$\boldsymbol{OS}_{ij} = \left\{ \bigcup_{k=1}^{r_{ij}} \boldsymbol{OS}_{ijk}\left(\bigcup_{l=1}^{a_{ijk}} A_{ijkl}\right) \right\} = \left\{ OS_{ij1}\left(\bigcup_{l=1}^{a_{ij1}} A_{ij1l}\right), OS_{ij2}\left(\bigcup_{l=1}^{a_{ij2}} A_{ij2l}\right), \ldots, OS_{ijr_{ij}}\left(\bigcup_{l=1}^{a_{ijr_{ij}}} A_{ijr_{ij}l}\right) \right\}, \quad (7)$$

where OS_{ijk} – function implementing basic measures $(k = \overline{1,r_{ij}})$, r_{ij} – number of basic measures for solving the s_i-th sub-objective, $A_{ijkl}\,(l = \overline{1,a_{ijk}})$ – l-th argument defining the method (approach, technical solution, etc.) for implementing the basic k-th measure of the s_i-th sub-objective, a_{ijk} – number of possible arguments for implementing the basic k-th measure (note: in case of absence of method, approach, universal technical solution, etc., this particular condition means that $l = \overline{1,0}$ and, as a consequence, the function has no arguments).

Taking into account (7), expression (3) can be written as follows:

$$\boldsymbol{OS} = \left\{ \bigcup_{i=1}^{o} \boldsymbol{OS}_i \left\{ \bigcup_{j=1}^{s_i} \boldsymbol{OS}_{ij} \left\{ \bigcup_{k=1}^{r_{ij}} OS_{ijk} \left(\bigcup_{l=1}^{a_{ijk}} A_{ijkl} \right) \right\} \right\} \right\} =$$

$$\{\{\{OS_{111}(\bigcup_{l=1}^{a_{111}} A_{111l}), OS_{112}(\bigcup_{l=1}^{a_{112}} A_{112l}), ..., OS_{11r_{11}}(\bigcup_{l=1}^{a_{11r_{11}}} A_{11r_{11}l})\}, \{OS_{121}(\bigcup_{l=1}^{a_{121}} A_{121l}), OS_{122}(\bigcup_{l=1}^{a_{122}} A_{122l}), ...,$$

$$OS_{12r_{12}}(\bigcup_{l=1}^{a_{12r_{12}}} A_{12r_{12}l})\}, ..., \{OS_{1s_1 1}(\bigcup_{l=1}^{a_{1s_1 1}} A_{1s_1 1l}), OS_{1s_1 2}(\bigcup_{l=1}^{a_{1s_1 2}} A_{1s_1 2l}), ..., OS_{1s_1 r_{1s_1}}(\bigcup_{l=1}^{a_{1s_1 r_{1s_1}}} A_{1s_1 r_{1s_1} l})\}\},$$

$$\{\{OS_{211}(\bigcup_{l=1}^{a_{211}} A_{211l}), OS_{212}(\bigcup_{l=1}^{a_{212}} A_{212l}), ..., OS_{21r_{21}}(\bigcup_{l=1}^{a_{21r_{21}}} A_{21r_{21}l})\}, \{OS_{221}(\bigcup_{l=1}^{a_{111}} A_{111l}), OS_{222}(\bigcup_{l=1}^{a_{222}} A_{222l}), ...,$$

$$OS_{22r_{22}}(\bigcup_{l=1}^{a_{22r_{22}}} A_{22r_{22}l})\}, ..., \{OS_{2s_1 1}(\bigcup_{l=1}^{a_{2s_1 1}} A_{2s_1 1l}), OS_{2s_2 2}(\bigcup_{l=1}^{a_{2s_2 2}} A_{2s_2 2l}), ..., OS_{2s_2 r_{2s_2}}(\bigcup_{l=1}^{a_{2s_2 r_{2s_2}}} A_{2s_2 r_{2s_2} l})\}\}, ...,$$

$$\{\{OS_{o11}(\bigcup_{l=1}^{a_{o11}} A_{o11l}), OS_{o12}(\bigcup_{l=1}^{a_{o12}} A_{o12l}), ..., OS_{o1r_{o1}}(\bigcup_{l=1}^{a_{o1r_{o1}}} A_{o1r_{o1}l})\}, \{OS_{o21}(\bigcup_{l=1}^{a_{o21}} A_{o21l}), OS_{o22}(\bigcup_{l=1}^{a_{o22}} A_{o22l}), ...,$$

$$OS_{o2r_{o2}}(\bigcup_{l=1}^{a_{o2r_{o2}}} A_{o2r_{o2}l})\}, ..., \{OS_{os_o 1}(\bigcup_{l=1}^{a_{os_o 1}} A_{os_o 1l}), OS_{os_o 2}(\bigcup_{l=1}^{a_{os_o 2}} A_{os_o 2l}), ..., OS_{os_o r_{os_o}}(\bigcup_{l=1}^{a_{os_o r_{os_o}}} A_{os_o r_{os_o} l})\}\}\}. \quad (8)$$

For example, taking into account [1], formula (7) when $r_{31}=8$, $r_{11}=r_{44}=7$; $r_{12}=r_{32}=10$; $r_{13}=r_{23}=r_{42}=r_{53}=2$; $r_{14}=r_{21}=r_{41}=r_{43}=r_{64}=r_{71}=3$; $r_{22}=13$; $r_{33}=r_{51}=r_{52}=r_{54}=r_{61}=r_{81}=4$; $r_{62}=6$; $r_{63}=15$; $r_{72}=5$; $r_{82}=9$; $a_{523}=6$; $a_{122}=a_{123}=a_{125}=a_{311}=a_{321}=a_{326}=a_{411}=a_{524}=a_{532}=a_{613}=a_{633}=3$; $a_{111}=a_{113}=a_{124}=a_{127}=a_{1210}=a_{141}=a_{211}=a_{213}=a_{222}=a_{225}=a_{2212}=a_{2213}=a_{231}=a_{312}=a_{313}=a_{315}=a_{317}=a_{322}=a_{324}=a_{325}=a_{327}=a_{328}=a_{329}=a_{3210}=a_{412}=a_{413}=a_{421}=a_{422}=a_{442}=a_{444}=a_{446}=a_{447}=a_{511}=a_{512}=a_{513}=a_{521}=a_{522}=a_{531}=a_{611}=a_{621}=a_{632}=a_{637}=a_{638}=a_{643}=a_{711}=a_{722}=a_{813}=a_{814}=a_{822}=a_{827}=a_{828}=2$; $a_{116}=a_{117}=a_{143}=a_{318}=a_{544}=a_{829}=0$ (all other values of parameter a are equal to 1), takes the following form:

$$\boldsymbol{OS} = \left\{ \bigcup_{i=1}^{8} \boldsymbol{OS}_i \left\{ \bigcup_{j=1}^{s_i} \boldsymbol{OS}_{ij} \left\{ \bigcup_{k=1}^{r_{ij}} OS_{ijk} \left(\bigcup_{l=1}^{a_{ijk}} A_{ijkl} \right) \right\} \right\} \right\} =$$

$$\{\{\{OS_{111}(A_{1111}, A_{1112}), OS_{112}(A_{1121}), ..., OS_{117}()\}, \{OS_{121}(A_{1211}), OS_{122}(A_{1221}, A_{1222}, A_{1223}), ...,$$
$$OS_{1210}(A_{12101}, A_{12102})\}, \{OS_{121}(A_{1211}), OS_{122}(A_{1221}, A_{1222}, A_{1223}), ..., OS_{1210}(A_{12101}, A_{12102})\}$$
$$\{OS_{121}(A_{1211}), OS_{122}(A_{1221}, A_{1222}, A_{1223}), ..., OS_{1210}(A_{12101}, A_{12102})\}, ...,$$
$$\{OS_{141}(A_{1411}, A_{1412}), OS_{142}(A_{1421}, A_{1422}), OS_{143}()\}\}, \{\{OS_{211}(A_{2111}, A_{2112}), OS_{212}(A_{2121}), OS_{213}(A_{2131}, A_{2132})\},$$
$$\{OS_{221}(A_{2211}), OS_{222}(A_{2221}, A_{2222}), ..., OS_{2213}(A_{22131}, A_{22132})\}, \{OS_{231}(A_{2311}, A_{2312}), OS_{232}(A_{2321})\}\}, ...,$$
$$\{\{OS_{811}(A_{8111}), OS_{812}(A_{8121}), ..., OS_{814}(A_{8141}, A_{8142})\}, \{OS_{821}(A_{8211}), OS_{822}(A_{8221}, A_{8222}), ..., OS_{829}()\}\}\} =$$
$$\{\{\{PA.S1.A1(PR,S), PA.S1.A2(PR), ..., PA.S1.A7()\}, \{PA.S2.A1(CP), PA.S2.A2(AR,R,U), ...,$$
$$PA.S2.A10(PR,U)\}, ..., \{PA.S4.A1(AR,PR), PA.S4.A2(CP,PR), PA.S4.A3()\}\},$$
$$\{\{PR.S1.A1(AR,CP), PR.S1.A2(CP), PR.S1.A3(AR,CP)\}, \{PR.S2.A1(R), PR.S2.A2(CP,R), ...,$$
$$PR.S2.A13(D,R)\}, \{PR.S3.A1(CP,CA), PR.S3.A2(CP)\}\}, ..., \{\{RA.S1.A1(R), RA.S1.A2(NP), ...,$$
$$RA.S1.A4(R,S)\}, \{RA.S2.A1(R), RA.S2.A2(R,CP), ..., RA.S2.A9()\}\}\}, \quad (9)$$

where, for example, when $i = j = 1, k = \overline{1,7}$ $OS_{111}(A_{1111}, A_{1112})$=*PA.S1.A1*(*PR,S*)=RESTRICT ACCESS TO RESOURCES BASED ON CRITICALITY AND SENSITIVITY (*PRIVILEGE RESTRICTION; SEGMENTATION*), $OS_{112}(A_{1121})$=*PA.S1.A2*(*PR*)=RESTRICT BEHAVIORS OF USERS AND CYBER ENTITIES (*PRIVILEGE RESTRICTION*), $OS_{113}(A_{1131}, A_{1132})$ =*PA.S1.A3*(*S,R*)=ENFORCE CLEAR BOUNDARIES ON SETS OF CYBER RESOURCES (*SEGMENTATION; REALIGNMENT*), $OS_{114}(A_{1141})$=*PA.S1.A4*(*CP*)=APPLY MULTIPLE DEFENSES TO CRITICAL ASSETS (*COORDINATED PROTECTION*), $OS_{115}(A_{1151}$)=*PA.S1.A5*(*D*)=PROTECT DATA IN DIFFERENT STATES (*DECEPTION*), OS_{116} ()=*PA.S1.A6*()=GENERAL (), OS_{117} ()=*PA.S1.A7*()=GENERAL (), and the argument $A_{1111} = A_{1121}$ =*PR – PRIVILEGE RESTRICTION*, $A_{1112} = A_{1131}$ =*S – SEGMENTATION*; A_{1132} =*R – REALIGNMENT*, A_{1141} =*CP – COORDINATED PROTECTION*, A_{1151} =*D – DECEPTION*.

An example of all $OS_{ijk}(\bigcup_{l=1}^{a_{ijk}} A_{ijkl})$ ($i = \overline{1,8}$; $j = \overline{1,s_i}$; $k = \overline{1,r_{ij}}$; $l = \overline{1,a_{ijk}}$) taking into account [1] is presented in Table 2 (where Representative Activity are Basic Measures and Corresponding Approaches are Methods), and the corresponding graphical representation of STDM is shown in fig. 1.

Table 2

Basic Cyber Resilience Measures and their Formalization within CREF

i	***j***	***k***	$OS_{ijk}(\bigcup_{l=1}^{a_{ijk}} A_{ijkl})$	a_{ijk}	**REPRESENTATIVE ACTIVITY (*CORRESPONDING APPROACHES*)**
1	1	1	*PA.S1.A1*(*PR,S*)	2	RESTRICT ACCESS TO RESOURCES BASED ON CRITICALITY AND SENSITIVITY (*PRIVILEGE RESTRICTION, SEGMENTATION*)
1	1	2	*PA.S1.A2*(*PR*)	1	RESTRICT BEHAVIORS OF USERS AND CYBER ENTITIES (*PRIVILEGE RESTRICTION*)
1	1	3	*PA.S1.A3*(*S,R*)	2	ENFORCE CLEAR BOUNDARIES ON SETS OF CYBER RESOURCES (*SEGMENTATION, REALIGNMENT*)
1	1	4	*PA.S1.A4*(*CP*)	1	APPLY MULTIPLE DEFENSES TO CRITICAL ASSETS (*COORDINATED PROTECTION*)
…….					
8	2	8	*RA.S2.A8*(*D,R*)	2	CREATE AND MAINTAIN A DEMONSTRABLY DIFFERENT VERSION OF THE SYSTEM OR OF CRITICAL SUB-SYSTEMS (*DIVERSITY, REDUNDANCY*)
8	2	9	*RA.S2.A9*()	0	GENERAL

The graphical visualization of the complete STDM, reflecting hierarchical connections between goals, objectives, sub-objectives, basic measures, and cyber resilience methods according to CREF, is presented in fig. 1.

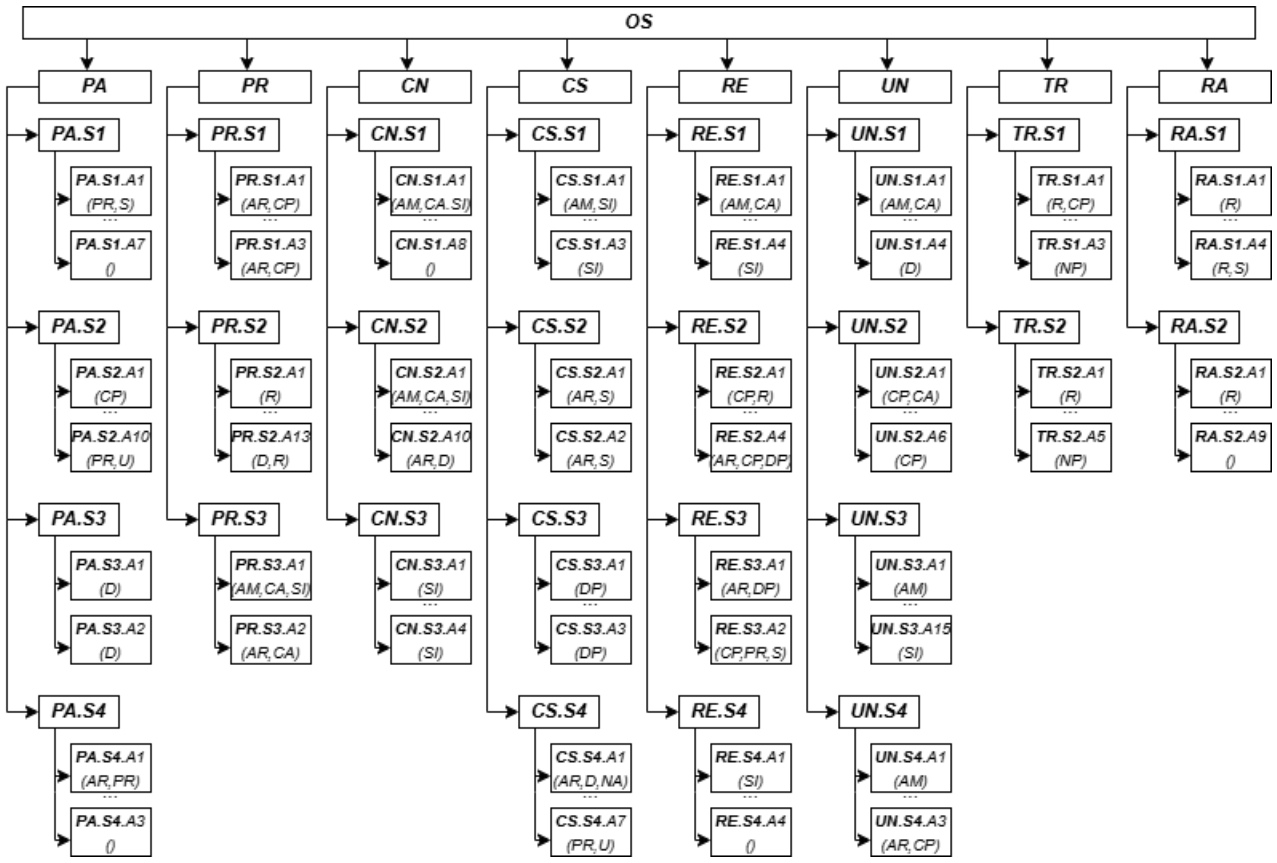

Fig. 1. Hierarchical structure of the STDM for CIE cyber resilience assessment

Let us consider the operation of the model using specific examples, taking into account that elements of the formed sets are selected only those that are directly relevant to a specific threat type and affect the cyber resilience of specific information resources.

Example 1. DDoS Attack Scenario on Banking API

The assessment of cyber resilience for the specified DDoS attack scenario is associated with data formation based on all the targets defined in the ***GS*** set. In this case, the following elements are initialized:

$GS_1=\{ANT\}$ – necessary to assess the bank's ability to identify threats related to DDoS campaigns in advance;

$GS_2=\{WITH\}$ – is a key target, as DDoS is aimed at disrupting the availability of services;

$GS_3=\{REC\}$ – reflects the ability to quickly restore APIs and related services after an attack;

$GS_4=\{AD\}$ – provides an assessment of the bank's ability to take into account lessons learned and increase resilience to future attacks.

Thus, formula (1) for this scenario will take the form:

$$GS=\{ANT, WITH, REC, AD\}. \quad (10)$$

For each element from the set, we determine the corresponding elements of the set ***OS***:

– for ***ANT***, we will form the element $OS_6=\{UN\}$, since effective counteraction to DDoS requires understanding the sources, tools, and attack patterns, and thus this task is basic;

– for ***WITH*** we will form the element $OS_3=\{CN\}$, since a DDoS attack is not aimed at compromising data, but at disrupting service provision, the main objective is to continue critical functions;

– for ***REC*** we will form the element $OS_5=\{RE\}$, because after the attack is over, it is necessary to restore full functionality of services and check their status;

– for ***AD*** we will form the element $\boldsymbol{OS}_7 = \{\boldsymbol{TR}\}$, because within, for example, CREF, this task is responsible for systemic changes based on the lessons learned.

Thus, formula (4) for this scenario will take the form:

$$\boldsymbol{OS} = \{\boldsymbol{OS}_3, \boldsymbol{OS}_5, \boldsymbol{OS}_6, \boldsymbol{OS}_7\} = \{\boldsymbol{CN}, \boldsymbol{RE}, \boldsymbol{UN}, \boldsymbol{TR}\}, \quad (11)$$

where $\boldsymbol{OS}_1 = \boldsymbol{OS}_2 = \boldsymbol{OS}_4 = \boldsymbol{OS}_8 = \varnothing$.

Next, for the elements of the set ***OS*** (see (11)), we form the corresponding sets. Since the DDoS attack on the banking API is primarily aimed at disrupting the availability and stability of services, this determines the choice of subtasks related to load management, limiting the impact of attacks, and restoring functionality. Then, based on (4) and (5), we define the members of the corresponding sets.

For $\boldsymbol{OS}_3 = \{\boldsymbol{CN}\}$ we will form the following elements:

$\boldsymbol{OS}_{31} = \{\boldsymbol{CN.S1}\}$ – chosen because the main goal of a DDoS attack is to disrupt the availability of services, not to compromise data. For the banking system, it is critical to maintain the functioning of key APIs and business services during an attack, which directly corresponds to the goal *Withstand*;

$\boldsymbol{OS}_{32} = \{\boldsymbol{CN.S2}\}$ – chosen because during a DDoS attack it is necessary to limit the scale and effect of the attacker's actions, reducing their impact on system performance. This sub-goal reflects the system's ability to localize the negative impact of the attack without completely stopping services.

So $\boldsymbol{OS}_3 = \{\boldsymbol{OS}_{31}, \boldsymbol{OS}_{32}\} = \{\boldsymbol{CN.S1}, \boldsymbol{CN.S2}\}$, where $\boldsymbol{OS}_{33} = \varnothing$.

For $\boldsymbol{OS}_5 = \{\boldsymbol{RE}\}$ we will form the element $\boldsymbol{OS}_{51} = \{\boldsymbol{RE.S1}\}$, which was chosen because after the DDoS attack is over or mitigated, the banking system must be able to quickly restore full functionality of the API and related services. This sub-goal directly reflects the recovery phase in the cyber resilience cycle and then $\boldsymbol{OS}_5 = \{\boldsymbol{OS}_{51}\} = \{\boldsymbol{RE.S1}\}$, де $\boldsymbol{OS}_{52} = \boldsymbol{OS}_{53} = \boldsymbol{OS}_{54} = \varnothing$.

For $\boldsymbol{OS}_6 = \{\boldsymbol{UN}\}$ we will form the following elements:

$\boldsymbol{OS}_{61} = \{\boldsymbol{UN.S1}\}$ – chosen because DDoS attacks are characterized by the use of typical patterns, botnet infrastructures and repetitive vectors of influence. Understanding the actions of the adversary is a necessary prerequisite for early preparation and reduction of the effectiveness of the attack, which, for example, fully corresponds to the *Anticipate* goal in CREF;

$\boldsymbol{OS}_{63} = \{\boldsymbol{UN.S3}\}$ – chosen because the success of a DDoS attack depends largely on the presence of open or critical access points, in particular API endpoints. Identifying such exposures allows for an assessment of the attack surface and is a logical element of preventive threat analysis.

So $\boldsymbol{OS}_6 = \{\boldsymbol{OS}_{61}, \boldsymbol{OS}_{63}\} = \{\boldsymbol{UN.S1}, \boldsymbol{UN.S3}\}$, where $\boldsymbol{OS}_{62} = \boldsymbol{OS}_{64} = \varnothing$.

For $\boldsymbol{OS}_7 = \{\boldsymbol{TR}\}$ we will form the element $\boldsymbol{OS}_{71} = \{\boldsymbol{TR.S1}\}$, which was chosen because DDoS attacks often reveal architectural limitations or shortcomings in the organization of protection. Formalizing the experience gained is necessary to increase the system's resilience to future similar threats and then $\boldsymbol{OS}_7 = \{\boldsymbol{OS}_{71}\} = \{\boldsymbol{TR.S1}\}$, where $\boldsymbol{OS}_{72} = \varnothing$.

Next, we select basic measures. For $\boldsymbol{OS}_{32} = \{\boldsymbol{CN.S2}\}$ we will form the following elements:

$OS_{321} = CN.S2.A1$ – chosen because during a DDoS attack, the key task is to reduce the impact of malicious traffic on system performance. This activity is directly aimed at localizing the effects of the attack and preventing a complete shutdown of services;

$OS_{322} = CN.S2.A2$ – chosen because isolating overloaded or attacked components allows the functionality of other parts of the system to be preserved. For a banking API, this is critically important given the need to maintain at least a minimum level of service during an attack.

So $\boldsymbol{OS}_{32} = \{OS_{321}, OS_{322}\} = \{CN.S2.A1, CN.S2.A2\}$, where $OS_{323} = OS_{324} = OS_{325} = OS_{326} = OS_{327} = OS_{328} = OS_{329} = OS_{3210} = \varnothing$.

For $\boldsymbol{OS}_{51}$={ ***RE.S1*** } we will form the element $OS_{511} = RE.S1.A1$, which was chosen because after the DDoS attack is over, it is necessary to quickly restore the normal operation of the API and related services. This activity directly reflects the ability of the system to return to performing its mission functions and then $\boldsymbol{OS}_{51} = OS_{511} = RE.S1.A1$, where $OS_{512} = OS_{513} = OS_{514} = \varnothing$.

For $\boldsymbol{OS}_{61}$={ ***UN.S1*** } we will form the element $OS_{611} = UN.S1.A1$, which was chosen because DDoS attacks are usually massive, repetitive in nature and spread quickly across different organizations and sectors. The use of shared threat intelligence allows for early detection of characteristic signs of the preparation or active phase of an attack, which directly supports the sub-goal of understanding the enemy's actions and then $\boldsymbol{OS}_{61} = OS_{611} = UN.S1.A1$, where $OS_{612} = OS_{613} = OS_{614} = \varnothing$.

For $\boldsymbol{OS}_{63}$={ ***UN.S3*** } we will form the element $OS_{631} = UN.S3.A1$, which was chosen because banking APIs are critical access points on which the functioning of numerous services depends. Identification of dependencies and exposures allows us to determine the most vulnerable infrastructure elements that can be used to implement a DDoS attack and then $\boldsymbol{OS}_{63} = OS_{631} = UN.S3.A1$, where $OS_{632} = OS_{633} = OS_{634} = OS_{635} = OS_{636} = OS_{637} = OS_{638} = OS_{639} = OS_{6310} = OS_{6312} = OS_{6313} = OS_{6314} = OS_{6315} = \varnothing$.

For $\boldsymbol{OS}_{71}$={ ***TR.S1*** } we will form the element $OS_{711} = TR.S1.A1$, which was chosen because DDoS attacks allow us to identify limitations in architecture, response processes, and defense organization. Recording and analyzing the lessons learned is a necessary condition for increasing the cyber resilience of the system in the long term, and then $\boldsymbol{OS}_{71} = OS_{711} = TR.S1.A1$, where $OS_{712} = OS_{713} = \varnothing$.

For each basic measure, we select the appropriate methods. For OS_{321}=*CN.S2.A1*, we form the following elements: *AM* – analytical monitoring was chosen because assessing the impact of a DDoS attack on API performance and availability requires constant analysis of system health indicators; *CA* – contextual awareness is chosen because decisions to limit the impact of an attack should be made taking into account the priorities of business functions and the contemporary landscape of the system; *SI* – substantiated integrity is chosen because it is necessary to confirm the correct operation of the service stations and the absence of hidden damage disguised as overload. So $OS_{321}(A_{3211}, A_{3212}, A_{3213}) = CN.S2.A1(AM,CA,SI)$.

For OS_{322}=*CN.S2.A2* we will form the following elements: *AR* – analytical monitoring was chosen because isolating attacked API components requires dynamic, adaptive actions in response to changing DDoS attack intensity; *CA* – contextual awareness is chosen because isolation must take into account interdependencies between components so as not to cause additional disruptions to business processes. So $OS_{322}(A_{3221}, A_{3222}) = CN.S2.A2(AR,CA)$.

For $OS_{511} = RE.S1.A1$ we will form the following elements: *AM* – analytical monitoring was chosen because restoring functionality requires monitoring the status of resources and identifying damaged or inaccessible components after an attack; *CA* – contextual awareness was chosen because prioritization of service restoration should be carried out taking into account their significance for banking operations. So $OS_{511}(A_{5111}, A_{5112}) = RE.S1.A1(AM,CA)$.

For $OS_{611} = UN.S1.A1$ we will form the following elements: *AM* – analytical monitoring was chosen because the use of shared information about DDoS threats requires analytical processing of large volumes of telemetry (network flows, API logs, external threat feeds, etc.) to identify characteristic signs of massive attacks; *CA* – contextual awareness was chosen because effective interpretation of shared threat information is possible only taking into account the current operational context of the banking API, its load, and the criticality of services. So $OS_{611}(A_{6111}, A_{6112}) = UN.S1.A1(AM,CA)$.

For $OS_{631} = UN.S3.A1$ we will form the element CA – contextual awareness, which was chosen because identifying critical dependencies and exposures requires understanding the role of each resource in supporting the bank's business functions and their relationships in a holistic architecture, and then $OS_{631}(A_{6311}) = UN.S3.A1(CA)$.

For $OS_{711} = TR.S1.A1$ we will form the following elements: R – redundancy was chosen because analysis of DDoS incidents allows identifying individual points of failure and justifying the need for resource redundancy; CP – coordinated protection was chosen because integrating lessons learned into the protection system requires coordinated changes in policies, architecture, and processes. So $OS_{711}(A_{7111}, A_{7112}) = TR.S1.A1(R,CP)$.

Taking into account the defined elements of the corresponding sets, formula (9) will take the following form:

$$\boldsymbol{OS} = \left\{ \bigcup_{i=1}^{8} \boldsymbol{OS}_i \left\{ \bigcup_{j=1}^{s_i} \boldsymbol{OS}_{ij} \left\{ \bigcup_{k=1}^{r_{ij}} OS_{ijk} \left(\bigcup_{l=1}^{a_{ijk}} A_{ijkl} \right) \right\} \right\} \right\} =$$

$$\{\{\{OS_{311}(A_{3111}, A_{3112}, A_{3113})\}, \{OS_{322}(A_{3221}, A_{3222})\}, \{OS_{331}(A_{3311})\}\}, \{\{OS_{511}(A_{5111}, A_{5112})\},$$
$$\{OS_{521}(A_{5211}, A_{5212})\}\}, \{\{OS_{611}(A_{6111}, A_{6112})\}, \{OS_{631}(A_{6311})\}\}, \{\{OS_{711}(A_{7111}, A_{7112})\}, \{OS_{722}(A_{7221})\}\}\} =$$
$$\{\{\{CN.S1.A1(AM,CA,SI)\}, \{CN.S2.A2(AR,CA)\}, \{CN.S3.A1(SI)\}\}, \{\{RE.S1.A1(AM,CA)\},$$
$$\{RE.S2.A1(CP,R)\}\}, \{\{UN.S1.A1(AM,CA)\}, \{UN.S3.A1(AM)\}\}, \quad (12)$$
$$\{\{TR.S1.A1(R,CP)\}, \{TR.S2.A2(R,CP)\}\}\}.$$

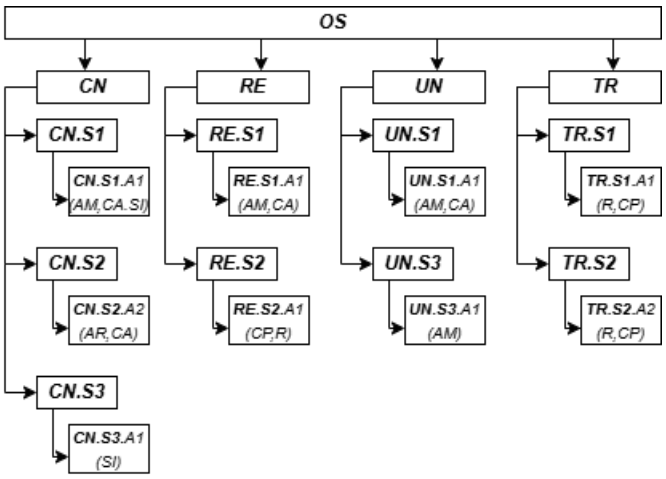

Fig. 2. Graphical representation of STDM on the example of a DDoS attack scenario on a banking API

A graphical representation of the STDM for a specific scenario of a DDoS attack on a banking API with the selection of relevant elements of the sets ***GS***, ***OS*** and the corresponding basic measures is shown in fig. 2.

Example 2. Phishing attack on a bank

The cyber resilience assessment for the scenario of a phishing attack on a banking institution involves generating data based on all the targets defined in the ***GS*** set. In this case, the following elements are initialized:

$\boldsymbol{GS}_1 = \{\boldsymbol{ANT}\}$ – chosen because a phishing attack is based on prior preparation of the attacker and the use of repetitive social engineering patterns. The ability to identify the signs of phishing campai-gns and potential vectors of influence in advance can significantly reduce the likelihood of a success-sful attack;

$\boldsymbol{GS}_2 = \{\boldsymbol{WITH}\}$ – chosen because even if there is partial compromise of users, the bank must be able to limit the consequences of the incident and maintain the operability of key business processes. This goal reflects the need to contain the impact of the attack without complete degradation of the system;

$\boldsymbol{GS}_3 = \{\boldsymbol{REC}\}$ – chosen because phishing often leads to loss of control over accounts or breach of trust in the system. Restoring normal status, access and functionality is a mandatory step in ensuring cyber resilience;

$\boldsymbol{GS}_4 = \{\boldsymbol{AD}\}$ – chosen because phishing techniques are constantly changing and evolving. Without the ability to adapt organizational and technical protection measures, a bank will remain vulnerable to future attacks even after successfully responding to the current incident.

Thus, formula (1) for this scenario will take the form:

$$\boldsymbol{GS} = \{\boldsymbol{ANT}, \boldsymbol{WITH}, \boldsymbol{REC}, \boldsymbol{AD}\}. \quad (13)$$

For each element of the set, we formulate the corresponding elements of the set ***OS***:

– for ***ANT*** let's form an element $\boldsymbol{OS}_6 = \{\boldsymbol{UN}\}$, which was chosen because effective countermeasures against phishing require a deep understanding of the attacker's tactics, techniques, and procedures, as well as the context in which they are used. Analyzing the enemy's actions is the basis for developing adequate prevention and response measures;

– for ***WITH*** let's form an element $\boldsymbol{OS}_3 = \{\boldsymbol{CN}\}$, which was chosen because phishing, as a rule, is not aimed at completely disabling the information system, but can disrupt individual processes. The bank must ensure the continuity of critical operations even in the event of an incident, which is key to financial stability;

– for ***REC*** let's form an element $\boldsymbol{OS}_5 = \{\boldsymbol{RE}\}$, which was chosen because after a phishing attack, it is necessary to restore trust in users, accounts, and system components. This task reflects the need to return the system to a correct and secure state;

– for ***AD*** let's form an element $\boldsymbol{OS}_7 = \{\boldsymbol{TR}\}$, which was chosen because the results of the analysis of phishing incidents should be used to improve approaches to personnel training, response procedures and architectural solutions. System transformation based on the experience gained is a necessary condition for long-term cyber resilience.

Thus, formula (4) for this scenario will take the form:

$$\boldsymbol{OS} = \{\boldsymbol{OS}_3, \boldsymbol{OS}_5, \boldsymbol{OS}_6, \boldsymbol{OS}_7\} = \{\boldsymbol{CN}, \boldsymbol{RE}, \boldsymbol{UN}, \boldsymbol{TR}\}. \quad (14)$$

Assessing cyber resilience for a phishing attack scenario differs from a DDoS attack in that the primary target is the user, not the infrastructure, and that staff awareness and information context play a critical role. This results in a slightly different emphasis in the selection of subtasks and methods while maintaining the overall structure of the goals.

For $\boldsymbol{OS}_3 = \{\boldsymbol{CN}\}$ we will form the following elements:

$\boldsymbol{OS}_{31} = \{\boldsymbol{CN.S1}\}$ – chosen because even in the event of successful phishing of individual users, banking business processes must remain operational. Ensuring continuity of core functions is critically important for a financial institution;

$\boldsymbol{OS}_{32} = \{\boldsymbol{CN.S2}\}$ – chosen because phishing often results in partial compromise of accounts, but not the entire system. Limiting the attacker's capabilities reduces the scale of the incident and prevents further spread of the attack.

So $\boldsymbol{OS}_3 = \{\boldsymbol{OS}_{31}, \boldsymbol{OS}_{32}\} = \{\boldsymbol{CN.S1}, \boldsymbol{CN.S2}\}$, where $\boldsymbol{OS}_{33} = \varnothing$.

For $\boldsymbol{OS}_5 = \{\boldsymbol{RE}\}$ let's form an element $\boldsymbol{OS}_{51} = \{\boldsymbol{RE.S1}\}$, which was chosen because after a phishing incident it is necessary to regain control over compromised accounts and related services. This sub-goal reflects the bank's ability to return the system to a normal state and then $\boldsymbol{OS}_5 = \{\boldsymbol{OS}_{51}\} = \{\boldsymbol{RE.S1}\}$, where $\boldsymbol{OS}_{52} = \boldsymbol{OS}_{53} = \boldsymbol{OS}_{54} = \varnothing$.

For $\boldsymbol{OS}_6 = \{\boldsymbol{UN}\}$ we will form the following elements:

$\boldsymbol{OS}_{61} = \{\boldsymbol{UN.S1}\}$ – chosen because phishing campaigns have characteristic signs, scenarios and indicators that are repeated in different attacks. Analysis of enemy actions allows for timely identifycation of phishing threats and reduction of their effectiveness;

$\boldsymbol{OS}_{62} = \{\boldsymbol{UN.S2}\}$ – chosen because phishing is primarily aimed at exploiting the human factor. The level of preparedness of users and staff directly determines the likelihood of a successful attack, making this sub-goal a key one within the *Anticipate* goal.

So $\boldsymbol{OS}_6 = \{\boldsymbol{OS}_{61}, \boldsymbol{OS}_{62}\} = \{\boldsymbol{UN.S1}, \boldsymbol{UN.S2}\}$, where $\boldsymbol{OS}_{63} = \boldsymbol{OS}_{64} = \varnothing$.

For $\boldsymbol{OS}_7 = \{\boldsymbol{TR}\}$ we will form the following elements:

$\boldsymbol{OS}_{71} = \{\boldsymbol{TR.S1}\}$ – chosen because the analysis of phishing incidents allows you to identify weaknesses in procedures, staff training and organizational measures, which is the basis for increasing overall cyber resilience;

$\boldsymbol{OS}_{72} = \{\boldsymbol{TR.S2}\}$ – chosen because phishing methods are constantly evolving and the bank must systematically increase the level of staff readiness and response processes, updating approaches to protection.

So $\boldsymbol{OS}_7 = \{\boldsymbol{OS}_{71}, \boldsymbol{OS}_{72}\} = \{\boldsymbol{TR.S1, TR.S2}\}$.

Next, we select basic measures.

For $\boldsymbol{OS}_{31} = \{\boldsymbol{CN.S1}\}$ let's form an element $OS_{311} = CN.S1.A1$, which was chosen because even in the presence of compromised accounts, the bank must ensure the continuity of key business processes and services for customers and then $\boldsymbol{OS}_{31} = OS_{311} = CN.S1.A1$, where $OS_{312} = OS_{313} = OS_{314} = OS_{315} = OS_{316} = OS_{317} = OS_{318} = \varnothing$.

For $\boldsymbol{OS}_{32} = \{\boldsymbol{CN.S2}\}$ let's form an element $OS_{321} = CN.S2.A1$, which was chosen because in the event of successful phishing it is important to limit the attacker's further actions, in particular to prevent the compromise from expanding within the system and then $\boldsymbol{OS}_{32} = OS_{321} = CN.S2.A1$, where $OS_{322} = OS_{323} = OS_{324} = OS_{325} = OS_{326} = OS_{327} = OS_{328} = OS_{329} = OS_{3210} = \varnothing$.

For $\boldsymbol{OS}_{51} = \{\boldsymbol{RE.S1}\}$ let's form an element $OS_{512} = RE.S1.A2$, which was chosen because after a phishing incident it is necessary to restore trust in accounts, systems and processes by resetting acesses and checking the state of the system and then $\boldsymbol{OS}_{51} = OS_{512} = RE.S1.A2$, where $OS_{511} = OS_{513} = OS_{514} = \varnothing$.

For $\boldsymbol{OS}_{61} = \{\boldsymbol{UN.S1}\}$ let's form an element $OS_{611} = UN.S1.A1$, which was chosen because phishing campaigns are widespread and have common indicators (message templates, domains, social engineering tactics, etc.). Sharing information about threats allows for rapid identification of new waves of phishing and then $\boldsymbol{OS}_{61} = OS_{611} = UN.S1.A1$, where $OS_{612} = OS_{613} = OS_{614} = \varnothing$;

For $\boldsymbol{OS}_{62} = \{\boldsymbol{UN.S2}\}$ let's form an element $OS_{621} = UN.S2.A1$, which was chosen because phishing directly exploits the human factor. Training staff to recognize phishing messages is a key activity to reduce the likelihood of a successful attack and then $\boldsymbol{OS}_{62} = OS_{621} = UN.S2.A1$, where $OS_{622} = OS_{623} = OS_{624} = OS_{625} = OS_{626} = \varnothing$.

For $\boldsymbol{OS}_{71} = \{\boldsymbol{TR.S1}\}$ let's form an element $OS_{711} = TR.S1.A1$, which was chosen because the analysis of phishing incidents allows for the improvement of both technical and organizational protection measures, increasing the overall level of cyber resilience of the bank and then $\boldsymbol{OS}_{71} = OS_{711} = TR.S1.A1$, where $OS_{712} = OS_{713} = \varnothing$.

For $\boldsymbol{OS}_{72} = \{\boldsymbol{TR.S2}\}$ let's form an element $OS_{722} = TR.S2.A2$, which was chosen because phishing methods are constantly evolving, and staff training programs must adapt to new attack scenarios and then $\boldsymbol{OS}_{72} = OS_{722} = TR.S2.A2$, where $OS_{721} = OS_{723} = OS_{724} = OS_{725} = \varnothing$.

For each basic measure, we select appropriate methods.

For $OS_{311} = CN.S1.A1$ we will form the following elements: *AM* – analytical monitoring was chosen because maintaining continuity requires constant monitoring of the state of processes; *CA* – contextual awareness is chosen because decisions about supporting operations must take into account business priorities.; *SI* – reasonable integrity is chosen because it is necessary to confirm the reliability of processes that continue to run during an incident. So $OS_{311}(A_{3111}, A_{3112}, A_{3113}) = CN.S1.A1(AM,CA,SI)$.

For OS_{321}=*CN.S2.A1* we will form the following elements: *AM* – analytical monitoring was chosen because in the phishing attack scenario, the implementation is aimed at limiting the impact of the attacker's actions after the initial compromise, and in such a case, it is critically important to detect anomalous behavior of already legitimate but compromised accounts. Thus, it allows for timely identification of the attacker's actions and reducing the scale of their impact; *CA* – contextual awareness was chosen because effective mitigation of a phishing attack is impossible without taking into account the user context, role, business process, and current system state. It allows distinguishing between real business operations and malicious ones; making decisions on access restrictions based on the criticality of processes; minimizing the side effects of protective measures on legitimate activities, and thus *CA* is a necessary complement to analytical monitoring in a phishing scenario; *SI* – reasoned integrity is chosen because a phishing attack often does not lead to an obvious disruption of the system, but creates a hidden threat to the trust in accounts, transactions and data. It provides: verification of the correctness of changes made under compromised accounts; confirmation that transactions have not been changed or forged; restoration of trust in the state of the system without completely stopping it. This is critically important for the banking sector, where limiting the impact of an attack means not only stopping malicious actions, but also guaranteeing the integrity of financial transactions. So $OS_{321}(A_{3211}, A_{3212}, A_{3213}) = CN.S2.A1(AM,CA,SI)$.

For $OS_{512} = RE.S1.A2$ we will form the following elements: *AM* – analytical monitoring was chosen because identifying suspicious or compromised entities requires analytical control. *SI* – reasoned integrity is chosen because trust can only be restored after the integrity of accounts and data is confirmed. So $OS_{512}(A_{5121}, A_{5122}) = RE.S1.A2(AM,SI)$.

For $OS_{611} = UN.S1.A1$ we will form the following elements: AM – analytical monitoring was chosen because correlation of data on phishing campaigns requires analytical processing of indicators of compromise and behavioral signs.; *CA* – contextual awareness is chosen because the effectiveness of shared information depends on the context of users, roles, and business processes. So $OS_{611}(A_{6111}, A_{6112}) = UN.S1.A1(AM,CA)$.

For $OS_{711} = TR.S1.A1$ we will form the following elements: *R* – redundancy was chosen because incident analysis allows identifying organizational and technical weaknesses; *CP* – coordinated protection was chosen because integrating the results of the analysis requires coordinated changes in policies and processes. So $OS_{711}(A_{7111}, A_{7112}) = TR.S1.A1(R,CP)$.

For $OS_{722} = TR.S2.A2$ we will form the following elements: *R* – reorientation is chosen because curriculum renewal is a form of reorientation of resources based on a new risk; *CP* – coordinated protection was chosen because changes in training must be coordinated with other elements of the cyber defense system. So $OS_{722}(A_{7221}, A_{7222}) = TR.S2.A2(R,CP)$.

The methods for these baseline measures are given only where they are present in the CREF tables, which is consistent with the framework methodology, and formula (9) will take the following form:

$$\boldsymbol{OS} = \left\{ \bigcup_{i=1}^{8} \boldsymbol{OS}_i \left\{ \bigcup_{j=1}^{s_i} \boldsymbol{OS}_{ij} \left\{ \bigcup_{k=1}^{r_{ij}} OS_{ijk} \left(\bigcup_{l=1}^{a_{ijk}} A_{ijkl} \right) \right\} \right\} \right\} =$$

$$\{\{\{OS_{311}(A_{3111}, A_{3112}, A_{3113})\}, \{OS_{321}(A_{3211}, A_{3212}, A_{3213})\}\}, \{\{OS_{512}(A_{5121}, A_{5122})\}\},$$
$$\{\{OS_{611}(A_{6111}, A_{6112})\}, \{OS_{621}(A_{6211}, A_{6212})\}\}, \{\{OS_{711}(A_{7111}, A_{7112})\}, \{OS_{722}(A_{7221}, A_{7222})\}\}\} =$$
$$\{\{\{CN.S1.A1(AM,CA,SI)\}, \{CN.S2.A1(AM,CA,SI)\}\}, \{\{RE.S1.A2(AM,SI)\},$$
$$\{\{UN.S1.A1(AM,CA)\}, \{UN.S2.A1(CP,CA)\}\}, \{\{TR.S1.A1(R,CP)\}, \{TR.S2.A2(R,CP)\}\}\}. \quad (15)$$

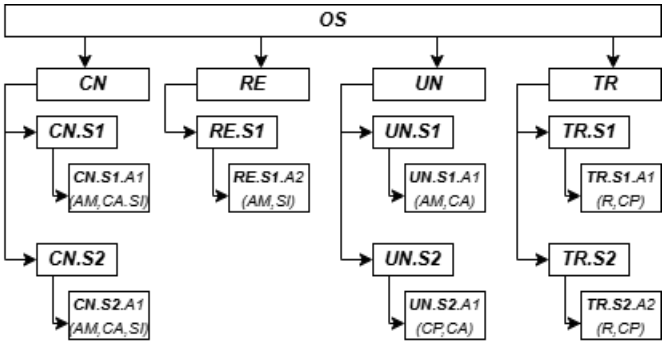

Fig. 3. Graphical representation of STDM on the example of a phishing attack scenario on a bank

A graphical representation of the STDM for the scenario of a phishing attack on a bank, demon-strating the differences in the choice of targets and measures compared to a DDoS attack, is shown in fig. 3.

Thus, in the considered examples, the selection of chain elements based on [1] for the scenarios of a DDoS attack on a banking API and a phishing attack on a bank:

– is carried out strictly within the framework of the MITRE CREF;

– is based on the semantic correspondence of the threat and the goal of cyber resilience;

– ensures the completeness of the cyber resilience cycle without redundant or irrelevant elements;

– allows for a unified assessment of different types of threats within a single formal model.

Discussion

The STDM proposed in the article fills the following critical gaps according to the criteria presented in Table 1:

For C1 – introduction of identifier sets for the set ***GS*** and for all ***OS*** levels (***OS***$_i$, ***OS***$_{ij}$, ***OS***$_{ijk}$ та A_{ijkl});

For C2 – establishment of formal connections through set-theoretic operations;

For C3 – unambiguous identification (for example, relative to the MITRE CREF) of 114 basic measures through hierarchical structur (*i.j.k*);

For C4 – creation of mathematical foundation for mapping the set of threats to the set of measures.

If we compare this development with the results of known studies mentioned in Table 1, it becomes obvious that the proposed model regarding the development level for C1, C2, C3, and C4 has a value of "++" ("High").

In the context of sustainability management, the proposed STDM provides advantages for further optimization of the allocation of limited resources to protective measures. Unlike traditional security models focused solely on preventing attacks, the proposed approach, based on set-theoretic interpretation, which allows, for example, to generalize MITRE CREF, emphasizes the system's capacity for self-recovery. This minimizes cascading effects from cyber incidents that could lead to significant environmental or social damage, thereby ensuring the environmental and economic sustainability of infrastructure ecosystems in the paradigm of ensuring the effectiveness of sustainable development of smart regions.

If we consider STDM in terms of such aspects as formalization, indexation, threat linkage, quantification, adaptability, and scalability, Table 3 also presents its advantages over existing approaches.

Table 3

Comparative Analysis of the Proposed Model with Existing Approaches to Cyber Resilience Assessment

Aspect	Existing Approaches	Proposed Model
Formalization	Descriptive (CREF) or partial	Complete set-theoretic
Indexing	Absent or informal	Unambiguous hierarchical system
Connection with threats	Qualitative, examples	Formalized set model
Quantitative assessment	Fragmented metrics	Unified mathematical foundation
Adaptability	Static or domain-specific	Parameterized for different CIEs
Scalability	Limited	Expandable structure

Conclusions and prospects for further research

Based on the analysis of known sources, the following conclusions can also be made:

1. Critical state of formalization: analysis shows that less than a third of studies touch on issues of formalizing cyber resilience structures, with none proposing a complete STDM;
2. Research relevance: the proposed STDM is the first to comprehensively solve all four criterial tasks within a unified formalized approach;
3. Scientific contribution: the model has a generalizing character and creates a bridge between conceptual frameworks (for example, for CREF) and practical quantitative assessment tools, which was lacking in previous studies;
4. Practical significance: formalization allows transition from expert assessments to an algorithmized, reproducible, and scalable process of assessing CIE cyber resilience;
5. Development directions: based on the proposed model, algorithms for calculating integral cyber-resilience indicators, decision support systems for prioritizing measures, automated assessment tools for different types of CIE, adaptive response strategies to dynamic changes in the threat landscape can be developed.

As a generalizing conclusion, it can be said that the work has developed for the first time an STDM for assessing the cyber resilience of CIE, which through formalization of the hierarchical structure of goals, objectives, sub-objectives, basic cyber resilience measures through introduction of identifier sets and implementation functions, establishment of mathematical relationships between elements of different hierarchy levels, creation of a system of unambiguous indexing of necessary actions, and formalization of the relationship between the set of cyber threats and basic cyber resilience measures, allows creating a mathematical foundation for transition from qualitative expert assessments to quantitative methods of systematic assessment of cyber-resilience, informed decision-making regarding prioritization of protective measures, and adaptation to specific requirements of different types of CIE under conditions of dynamic changes in the cyber threat landscape that negatively affect the effectiveness of sustainable development.

Next, based on the developed STDM, it is necessary to develop a method for assessing the cyber resilience of CIE, which will allow calculating integral cyber-resilience indicators, determining optimal combinations of basic measures for countering specific threat types, and ensuring automation of the assessment process under conditions of limited resources. In particular, the development of methods for assessing the impact of cyber incidents on the social and environmental components of CIE functioning is planned. This will enable the creation of a comprehensive decision support system that will consider not only technical cybersecurity parameters but also the overall contribution of infrastructure entities to ensuring the stability and effectiveness of sustainable development of smart regions.

Authors' contributions

O. KORCHENKO – conceptualization; methodology; V. KHARCHENKO – analysis of sources, preparation of a literature review or theoretical basis of the research; Yu. KHOKHLACHOVA – empirical research, collection and verification of empirical data; Yu. ZHUROV – software.

Declaration on artificial intelligence

During the preparation of this work, the authors used [Google Gemini / ChatGPT] in order to improve the English language phrasing, grammar, and overall readability of the text. After using this tool, the authors rigorously reviewed and edited the content as needed and take full responsibility for the final content of the publication.

Conflict of interest

The author declares that there is no conflict of interest and confirms that during the preparation of this work there were no commercial, financial, or other relationships that could be construed as

influencing the results of the study or their interpretation. The work was performed in accordance with the principles of academic integrity, ethical standards for conducting scientific research, and editorial policy requirements for preventing conflicts of interest.

References

1. Bodeau DJ, Graubart RD, McQuaid RM, Woodill J. Cyber Resiliency Metrics, Measures of Effectiveness, and Scoring: Enabling Systems Engineers and Program Managers to Select the Most Useful Assessment Methods. MITRE Technical Report MTR180314; The MITRE Corporation: Bedford, MA, USA, 2018. Available online: https://www.mitre.org/sites /default/files/publications/pr-18-2579-cyber-resiliency-metrics-measures-of-effectiveness-and-scoring.pdf (accessed on 15 January 2026).

2. Bodeau DJ, Graubart RD. Cyber Resiliency Engineering Framework. MITRE Technical Report MTR110237; The MITRE Corporation: Bedford, MA, USA, 2011. Available online: https://www.mitre.org/sites/default/files/pdf/11_4436.pdf (accessed on 15 January 2026).

3. Bodeau DJ, Brtis J, Graubart RD, Salwen J. Cyber Resiliency Engineering Aid—The Updated Cyber Resiliency Engineering Framework and Guidance on Applying Cyber Resiliency Techniques. MITRE Technical Report MTR150264; The MITRE Corporation: Bedford, MA, USA, 2015. Available online:https://www.mitre.org/sites/default/files/publications/pr-15-1334-cyber-resiliency-engineering-aid-framework-update.pdf (accessed on 15 January 2026).

4. Ross RS, Pillitteri VY, Graubart R, Bodeau D, McQuaid R. Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. NIST Special Publication 800-160, Volume 2, Revision 1; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2021. https://doi.org/10.6028/NIST.SP.800-160v2r1

5. Björck F, Henkel M, Stirna J, Zdravkovic J. Cyber Resilience—Fundamentals for a Definition. In: Á. Rocha, A.M. Correia, H. Adeli, L.P. Reis, M.M. Teixeira (Eds.) New Contributions in Information Systems and Technologies; Advances in Intelligent Systems and Computing, Vol. 353; Springer: Cham, Switzerland, 2015; pp. 311–316. https://doi.org/10. 1007/978-3-319-16486-1_31

6. Cam H, Mouallem P, Mo J, Farris J. Resilience metrics for cyber systems. INCOSE Int. Symp. 2016, 26, 1476–1489. https://doi.org/10.1002/j.2334-5837.2016.00233.x

7. Giannopoulos G, Filippini R, Schimmer M. Risk Assessment Methodologies for Critical Infrastructure Protection. Part I: A State of the Art. European Commission Joint Research Centre Technical Report EUR 25286 EN; Publications Office of the European Union: Luxembourg, 2012. https://doi.org/10.2788/22260

8. Zio E. Challenges in the vulnerability and risk analysis of critical infrastructures. Reliab. Eng. Syst. Saf. 2016, 152, 137–150. https://doi.org/10.1016/j.ress.2016.02.009

9. Musman S, Temin A. A cyber mission impact assessment tool. In Proceedings of the 2015 IEEE International Symposium on Technologies for Homeland Security (HST); Waltham, MA, USA, 14–16 April 2015; pp. 1–7. https://doi.org/10.1109/THS.2015.7225283

10. Falco G, Caldera C, Shrobe H. IIoT cybersecurity risk modeling for SCADA systems. IEEE Internet Things J. 2018, 5, 4486–4495. https://doi.org/10.1109/JIOT.2018.2822842

11. Woods DD. Four concepts for resilience and the implications for the future of resilience engineering. Reliab. Eng. Syst. Saf. 2015, 141, 5–9. https://doi.org/10.1016/j.ress.2015.03.018

12. Ganin AA, Massaro E, Gutfraind A, Steen N, Keisler JM, Kott A, Mangoubi R, Linkov I. Operational resilience: Concepts, design and analysis. Sci. Rep. 2016, 6, 19540. https://doi.org/10.1038/srep19540

13. Pursiainen C. Critical infrastructure resilience: A Nordic model in the making? Int. J. Disaster Risk Reduct. 2018, 27, 632–641. https://doi.org/10.1016/j.ijdrr.2017.08.006

14. Kott A, Linkov I (Eds.). Cyber Resilience of Systems and Networks; Springer International Publishing: Cham, Switzerland, 2019. https://doi.org/10.1007/978-3-319-77492-3

15. Hosseini S, Barker K, Ramirez-Marquez JE. A review of definitions and measures of system resilience. Reliab. Eng. Syst. Saf. 2016, 145, 47–61. https://doi.org/10.1016/ j.ress.2015.08.006

16. Amin M. Energy infrastructure defense systems. Proc. IEEE 2005, 93, 861–875. https://doi.org/10.1109/JPROC.2005.847257

17. Ouyang M. Review on modeling and simulation of interdependent critical infrastructure systems. Reliab. Eng. Syst. Saf. 2014, 121, 43–60. https://doi.org/10.1016/j.ress.2013.06.040

18. Alcaraz C, Zeadally S. Critical infrastructure protection: Requirements and challenges for the 21st century. Int. J. Crit. Infrastruct. Prot. 2015, 8, 53–66. https://doi.org/10.1016/j.ijcip.2014.12.002

19. Hossain, M. S., Moniruzzaman, M., Muhammad, G., et al. Big data-driven service composition using parallel clustered particle swarm optimization in mobile environment. IEEE Transactions on Services Computing 2014, 9(5), 806-817.

20. Rieger C, Gertman D, McQueen M. Resilient control systems: Next generation design research. In Proceedings of the 2009 2nd Conference on Human System Interactions; Catania, Italy, 21–23 May 2009; pp. 632–636. https://doi.org/10.1109/HSI.2009.5091051

21. Stergiopoulos G, Kotzanikolaou P, Theocharidou M, Lykou G, Gritzalis D. Time-based critical infrastructure dependency analysis for large-scale and cross-sectoral failures. Int. J. Crit. Infrastruct. Prot. 2016, 12, 46–60. https://doi.org/10.1016/j.ijcip.2015.12.002

22. Haque MA, Shetty S, Krishnappa B. Cybersecurity resilience model for industrial control systems. IET Cyber-Phys. Syst. Theory Appl. 2020, 5, 271–282. https://doi.org/10.1049/iet-cps.2020.0059

23. Theocharidou M, Kotzanikolaou P, Gritzalis D. A multi-layer criticality assessment methodology based on interdependencies. Comput. Secur. 2016, 62, 251–272. https://doi.org/10.1016/j.cose.2016.07.010

24. Yusta JM, Correa GJ, Lacal-Arántegui R. Methodologies and applications for critical infrastructure protection: State-of-the-art. Energy Policy 2011, 39, 6100–6119. https://doi.org/10.1016/j.enpol.2011.07.010

25. Jackson S, Ferris TL. Resilience principles for engineered systems. Syst. Eng. 2013, 16, 152–164. https://doi.org/10.1002/sys.21228

26. Rinaldi SM, Peerenboom JP, Kelly TK. Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Syst. Mag. 2001, 21, 11–25. https://doi.org/10.1109/37.969131

27. Petersen L, Fallou L, Reilly P, Serafinelli E. A resilience assessment framework for critical infrastructure. Int. J. Crit. Infrastruct. Prot. 2019, 25, 1–14. https://doi.org/10.1016/j.ijcip.2019.01.003

28. Setola R, Rosato V, Kyriakides E, Rome E (Eds.). Managing the Complexity of Critical Infrastructures: A Modelling and Simulation Approach; Studies in Systems, Decision and Control, Vol. 90; Springer International Publishing: Cham, Switzerland, 2016. https://doi.org/10.1007/978-3-319-51043-9

29. Teixeira A, Shames I, Sandberg H, Johansson KH. A secure control framework for resource-limited adversaries. Automatica 2015, 51, 135–148. https://doi.org/10.1016/j.automatica.2014.10.067

30. Vugrin ED, Warren DE, Ehlen MA, Camphouse RC. A framework for assessing the resilience of infrastructure and economic systems. In: Gopalakrishnan K, Peeta S (Eds.) Sustainable and Resilient Critical Infrastructure Systems; Springer: Berlin/Heidelberg, Germany, 2010; pp. 77–116. https://doi.org/10.1007/978-3-642-11405-2_3

О. Г. Корченко, В. С. Харченко, Ю. Є. Хохлачова, Ю. С. Журов

СТАЛИЙ РОЗВИТОК РОЗУМНИХ РЕГІОНІВ: ТЕОРЕТИКО-МНОЖИННА МОДЕЛЬ ДАНИХ ДЛЯ ОЦІНКИ КІБЕРСТІЙКОСТІЙКОСТІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Зростаюча складність та інтенсивність кіберзагроз об'єктам критичної інфраструктури (КІ) вимагає переходу від класичних методів захисту до комплексних стратегій кіберстійкості. Метою цього дослідження є створення формального математичного інструмен-

тарію для оцінки здатності об'єктів інфраструктури передбачати атаки, протистояти їм, відновлюватися та адаптуватися до змін. У цій роботі пропонується теоретико-множинна модель даних (STDM), яка, наприклад, узагальнює та формалізує ієрархічну структуру MITRE Cyber Resiliency Engineering Framework (CREF). Методологія дослідження базується на введенні наборів ідентифікаторів для цілей, завдань, підцілей та основних показників стійкості, а також на розробці унікальної системи індексації для їх однозначного відображення. Результати моделювання створюють сувору математичну основу для систематичного аналізу кіберстійкості, що дозволяє виявляти прогалини в захисті та обґрунтовано визначати пріоритети ресурсів. Наприклад, узагальнення CREF за допомогою теоретико-множинного підходу забезпечує високу гнучкість моделі до динамічних змін у ландшафті загроз та специфічних вимог різних типів КІ. Зроблено висновок, що впровадження моделі безпосередньо сприяє довгостроковій надійності та забезпечує ефективність сталого розвитку критичної інфраструктури в розумних регіонах, що відповідає Цілям сталого розвитку ООН (ЦСР 9 та 11) у контексті побудови стійких та безпечних соціально-технічних систем.

Ключові слова: сталий розвиток, розумні регіони, кіберстійкість, об'єкти критичної інфраструктури, теоретико-множинна модель даних, MITRE CREF, оцінка стійкості, підтримка прийняття рішень.

Надійшла до редакції: 09.06.2026
Прийнята до друку: 23.06.2026
Опубліковано: 17.08.2026