КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (34), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.34.1305
UDC 004.056

Oleksandr Korchenko
Doctor of Technical Sciences, Professor
State University of Information and Communication Technologies, Kyiv
ORCID:0000-0003-3376-0631
agkorchenko@gmail.com

Yuliia Khokhlachova
Candidate of Technical Sciences, Professor
State University of Trade and Economics, Kyiv; State University of Information and Communication Technologies, Kyiv
ORCID:0000-0002-0787-5112
yuliiahohlachova@gmail.com

SET-THEORETICAL METRIC MODEL FOR ASSESSING CYBER RESILIENCE OF CRITICAL INFRASTRUCTURE FACILITIES

Abstract. The problem of formalized assessment of cyber resilience of critical infrastructure under increasing cyber threat complexity is addressed. Existing approaches are fragmented and lack a strict connection between basic cyber resilience measures and their evaluation metrics. This study aims to develop a set-theoretic metric model that formalizes the set of possible metrics for each base measure. A formal representation of metrics as a function of base measures is proposed, introducing the concept of set cardinality and its dependence on application context. Structural (ex-ante) and operational (ex-post) metrics are integrated within a unified mathematical framework, and a functional mapping "base measure → set of possible metrics" is defined. The results enable a transition to formalized quantitative evaluation and support the development of integral indicators and automated analysis, improving reproducibility, comparability, and validity of cyber resilience assessment.

Keywords: cyber resilience, cyber resilience assessment, critical infrastructure facilities, cyber resilience metrics, set-theoretic model, set-theoretic approach, MITRE CREF, information security, cybersecurity, information protection.

INTRODUCTION AND RELATED WORKS

Motivation. Modern critical infrastructure facilities (CIF) operate in an environment of constant cyber threats, which requires a transition from classical models of information security to the concept of cyber resilience as the ability of a system to maintain functionality under destructive influences. At the same time, existing approaches to assessing cyber resilience are fragmentary and do not provide a formalized connection between basic measures (BMs), approaches to their implementation, and corresponding metrics. The problem of a consistent representation of a set of possible metrics (SPMs) of different nature (external, universal, local) within a single mathematical model is of particular relevance.

This study develops a set-theoretic metric model (STMM) was developed, which formalizes the SPM for each BM and provides a mathematical basis for further calculation of integral indicators of cyber resilience.

Unlike existing approaches that use individual indicators metrics [1] without a single formal mapping on the BM, the proposed model forms a functional mapping of the form "BM → SPM". This allows us to move from a descriptive assessment to a mathematically defined process of measuring cyber resilience.

In this regard, a model is needed to assess cyber resilience that formalizes the SPM for each BM and provides a generalized description of the measurement processes regardless of the method of implementing the corresponding approaches.

The significance of this research stems from several critical factors: C1 – the lack of a formalized connection between the BM of cyber resilience and the corresponding metrics; C2 – methodological uncertainty in the formation of formalized assessment systems; C3 – the need to automate the processes of assessing cyber resilience in the conditions of digital transformation of the CIF and the growth of the cardinality of the set of threats; C4 – the need to integrate structural (ex-ante) and operational (ex-post) characteristics of the

implementation of measures; C5 – the requirements of modern regulatory approaches to the demonstrability and reproducibility of evaluation results.

In this regard, the transition from conceptual framework models to formal mathematical constructs capable of ensuring reproducibility, scalability and adaptability is important.

Related works. To visually represent the results of this systematic literature review and precisely delineate the identified research gaps, all reviewed sources (including classic systems engineering frameworks and recent process-oriented organizational models) were mapped against five core analysis criteria (C1-C5). These criteria directly reflect the pivotal requirements for modern cyber resilience assessment frameworks for critical infrastructure facilities operating under digital transformation. The comprehensive mapping of this comparative analysis is structured in Table 1.

Table 1

Mapping of the reviewed state-of-the-art sources against target methodological criteria

Source	C1	C2	C3	C4	C5
[1]	+	+	+-	+-	+
[2], [18]	+-	+	-	+-	+-
[3]	+-	+-	+	-	+
[4]	+-	+	+-	+	++
[5]	+	+-	-	+-	-
[6]	-	+-	-	-	-
[7]	+	+	+-	+-	+
[8]	+-	+-	+	-	+-
[9]	-	+	+-	-	+-
[10], [30]	+-	+	-	-	+
[11], [12]	-	+-	+	+-	-
[13]	+-	+	++	+	+
[14], [27], [40]	-	+	+	-	+
[15]	+	+	+	+	+-
[16]	+	+-	+	+-	+
[17], [23]	+-	+	+	+	+-
[19]	+-	+-	++	+	-
[20]	-	-	-	-	-
[21]	-	+-	+	+	+-
[22]	-	-	++	-	-
[24]	+	+	+-	++	+
[25]	+-	+-	-	+-	-
[26]	+-	+	+	++	+
[28]	+-	+	+	+-	+
[29]	-	+	+-	-	+-
[31], [33]	+-	++	+	+	++
[32]	+-	+	+	-	+
[34]	+	++	+-	+-	+
[35]	+	+	++	+	+
[36]	+-	+-	++	+-	+-
[37]	+	+	+	+-	+
[38], [39]	+-	++	+	-	+
Proposed STMM	++	++	++	++	++

Notation criteria checklist summary: ++ (fully resolved, mathematically formalized within the framework); + (partially resolved or explicitly addressed through specific parameters); +- (conceptually identified or declared as a gap without exact solutions); - (not considered / outside the scope of the cited research).

Objectives, structure, and scenario-based approach. There is a pressing scientific problem of developing a STMM that provides formalization of a set of metrics as a function of the BM and methods of their implementation. Therefore, the following problems remain unsolved: lack of a formalized SPM for each BM; uncertainty of the cardinality of the set of metrics depending on the implementation arguments; methodological

incompleteness of the assessment when using only structural or only operational indicators; complexity of constructing generalized cyber resilience indicators based on heterogeneous metrics.

The purpose of the study is to develop a STMM for assessing the cyber resilience of CIF, which formalizes the SPM for each BM and provides a mathematical basis for constructing integral resilience indicators. To achieve the goal, it is necessary to perform the following research tasks: 1) formalize the SPM for each BM; 2) determine the cardinality of the set of metrics and its dependence on the implementation arguments; 3) introduce the distinction between structural and operational metrics; 4) construct a functional mapping "BM→SPM"; 5) propose a generalized hierarchical metric construct; 6) verify the model's consistency with the MITRE Cyber Resiliency Engineering Framework (CREF).

RESEARCH RESULTS

To build the necessary data model, a set-theoretic approach will be used. For this, we introduce a set of goal identifiers $\boldsymbol{GS}$ that will enable ensuring the cyber resilience of CIF: $\boldsymbol{GS} = \left\{ \bigcup_{i=1}^{n} \boldsymbol{GS}_i \right\} = \{\boldsymbol{GS}_1, \boldsymbol{GS}_2, ..., \boldsymbol{GS}_n\}$, where $i = \overline{1,n}$, and n – number of goals. Next, we introduce the set:

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

which consists of the set of identifiers of the *i*-th tasks $\boldsymbol{OS}_i$ ($i = \overline{1,o}$), identifiers of *j*-th subtasks $\boldsymbol{OS}_{ij}$ ($j = \overline{1,s_i}$), functions OS_{ijk}, that implement basic activities ($k = \overline{1,r_{ij}}$), where o – number of task IDs, r_{ij} – number of basic measures to solve the s_i-th subproblem, 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 subtask, a_{ijk} – number of possible arguments for implementing the basic k-th measure. Thus, the hierarchical structure of parameters defined in (1) represents a set-theoretic data model (STDM) [41].

To implement the necessary evaluation (measurement) processes for each BM defined by the corresponding function OS_{ijk} ($i = \overline{1,o}$; $j = \overline{1,s_i}$; $k = \overline{1,r_{ij}}$) we introduce a set $OS_{ijkq}\left(\bigcup_{l=1}^{a_{ijkq}} A_{ijkql} \right)$ of possible metrics, then the generalized STMM for assessing cyber resilience takes the form:

$$\boldsymbol{OS}_{ijk} = \left\{ \bigcup_{q=1}^{m_{ijk}} \boldsymbol{OS}_{ijkq} \left(\bigcup_{l=1}^{a_{ijkq}} A_{ijkql} \right) \right\} = \left\{ OS_{ijk1} \left(\bigcup_{l=1}^{a_{ijk1}} A_{ijk1l} \right), OS_{ijk2} \left(\bigcup_{l=1}^{a_{ijk2}} A_{ij2l} \right), ..., OS_{ijkm_{ijk}} \left(\bigcup_{l=1}^{a_{ijkm_{ijk}}} A_{ijkm_{ijk}l} \right) \right\} \quad (2)$$

where OS_{ijkq} – SPM ($q = \overline{1,m_{ijk}}$), m_{ijk} – the number (cardinality) of possible metrics (sets of metrics) for evaluating the r_{ij}-th BM, $a_{ijkq} = a_{ijk}$.

Taking into account (2), expression (1) can be written in the following form:

$$\boldsymbol{OS} = \left\{ \bigcup_{i=1}^{o} \boldsymbol{OS}_i \left\{ \bigcup_{j=1}^{s_i} \boldsymbol{OS}_{ij} \left\{ \bigcup_{k=1}^{r_{ij}} \boldsymbol{OS}_{ijk} \left\{ \bigcup_{q=1}^{m_{ijk}} \boldsymbol{OS}_{ijkq} \left(\bigcup_{l=1}^{a_{ijkq}} A_{ijkql} \right) \right\} \right\} \right\} \right\} = \quad (3)$$

$$\{\{\{\{OS_{1111}(\bigcup_{l=1}^{a_{1111}} A_{1111l}), OS_{1112}(\bigcup_{l=1}^{a_{1112}} A_{1112l}), ..., OS_{111m_{111}}(\bigcup_{l=1}^{a_{111m_{111}}} A_{111m_{111}l})\},$$

$$\{OS_{1121}(\bigcup_{l=1}^{a_{1121}} A_{1121l}), OS_{1122}(\bigcup_{l=1}^{a_{1122}} A_{1122l}), ..., OS_{112m_{112}}(\bigcup_{l=1}^{a_{112m_{112}}} A_{112m_{112}l})\}, ...,$$

$$\{OS_{11r_{11}1}(\bigcup_{l=1}^{a_{11r_{11}1}} A_{11r_{11}1l}), OS_{11r_{11}2}(\bigcup_{l=1}^{a_{11r_{11}2}} A_{11r_{11}2l}), ..., OS_{11r_{11}r_{11}r_{11}}(\bigcup_{l=1}^{a_{11r_{11}r_{11}r_{11}}} A_{11r_{11}r_{11}r_{11}l})\}\},$$

$$\{\{OS_{1211}(\bigcup_{l=1}^{a_{1211}} A_{1211l}), OS_{1212}(\bigcup_{l=1}^{a_{1212}} A_{1212l}), ..., OS_{121m_{121}}(\bigcup_{l=1}^{a_{121m_{121}}} A_{121m_{121}l})\},$$

$$\{OS_{1221}(\bigcup_{l=1}^{a_{1221}} A_{1221l}), OS_{1222}(\bigcup_{l=1}^{a_{1222}} A_{1222l}), ..., OS_{122m_{122}}(\bigcup_{l=1}^{a_{122m_{122}}} A_{122m_{122}l})\}, ...,$$

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

$$\{\{OS_{1s_11}(\bigcup_{l=1}^{a_{1s_111}} A_{1s_111l}), OS_{1s_112}(\bigcup_{l=1}^{a_{1s_112}} A_{1s_112l}), ..., OS_{1s_11m_{1s_11}}(\bigcup_{l=1}^{a_{1s_11m_{1s_11}}} A_{1s_11m_{1s_11}l})\},$$

$$\{OS_{1s_121}(\bigcup_{l=1}^{a_{1s_121}} A_{1s_121l}), OS_{1s_122}(\bigcup_{l=1}^{a_{1s_122}} A_{1s_122l}), ..., OS_{1s_12m_{1s_11}}(\bigcup_{l=1}^{a_{1s_12m_{1s_11}}} A_{1s_12m_{1s_11}l})\}, ...,$$

$$\{OS_{1s_1r_{1s_1}1}(\bigcup_{l=1}^{a_{1s_1r_{1s_1}1}} A_{1s_1r_{1s_1}1l}), OS_{1s_1r_{1s_1}2}(\bigcup_{l=1}^{a_{1s_1r_{1s_1}2}} A_{1s_1r_{1s_1}2l}), ..., OS_{1s_1r_{1s_1}m_{1s_1r_{1s_1}}}(\bigcup_{l=1}^{a_{1s_1r_{1s_1}m_{1s_1r_{1s_1}}}} A_{1s_1r_{1s_1}m_{1s_1r_{1s_1}}l})\}\}, ..., \}, ...,$$

$$\{\{\{OS_{os_o11}(\bigcup_{l=1}^{a_{os_o11}} A_{os_o11l}), OS_{os_o12}(\bigcup_{l=1}^{a_{os_o12}} A_{os_o12l}), ..., OS_{os_o1m_{os_o1}}(\bigcup_{l=1}^{a_{os_o1m_{os_o1}}} A_{os_o1m_{os_o1}l})\},$$

$$\{OS_{os_o21}(\bigcup_{l=1}^{a_{os_o21}} A_{os_o21l}), OS_{os_o22}(\bigcup_{l=1}^{a_{os_o22}} A_{os_o22l}), ..., OS_{os_o2m_{os_o2}}(\bigcup_{l=1}^{a_{os_o2m_{os_o2}}} A_{os_o2m_{os_o2}l})\}, ...,$$

$$\{OS_{os_or_{os_o}1}(\bigcup_{l=1}^{a_{os_or_{os_o}1}} A_{os_or_{os_o}1l}), OS_{os_or_{os_o}2}(\bigcup_{l=1}^{a_{os_or_{os_o}2}} A_{os_or_{os_o}2l}), ..., OS_{os_or_{os_o}m_{os_or_{os_o}}}(\bigcup_{l=1}^{a_{os_or_{os_o}m_{os_or_{os_o}}}} A_{os_or_{os_o}m_{os_or_{os_o}}l})\}\}\}\}.$$

For example, taking into account CREF MITRE [1] formula (3) at $m_{114}=m_{318}=m_{329}=m_{3210}=m_{543}=m_{544}=m_{612}=m_{635}=m_{639}=m_{811}=m_{812}=m_{813}=m_{829}=1$; $m_{112}=m_{127}=m_{128}=m_{226}=m_{228}=m_{231}=m_{313}=m_{315}=m_{316}=m_{221}=m_{322}=m_{324}=m_{326}=m_{327}=m_{328}=m_{446}=m_{511}=m_{531}=m_{532}=m_{542}=m_{614}=m_{632}=m_{634}=m_{636}=m_{638}=m_{6311}=m_{6312}=m_{6315}=m_{711}=m_{712}=m_{721}=m_{722}=m_{723}=m_{724}=m_{725}=m_{821}=m_{822}=m_{823}=m_{825}=m_{826}=2$; $m_{117}=m_{129}=m_{141}=m_{211}=m_{229}=m_{2210}=m_{314}=m_{323}=m_{421}=m_{422}=m_{432}=m_{433}=m_{441}=m_{442}=m_{513}=m_{621}=m_{624}=m_{625}=m_{637}=m_{6310}=m_{6313}=m_{713}=m_{824}=m_{828}=3$; $m_{111}=m_{121}=m_{123}=m_{223}=m_{225}=m_{2212}=m_{2213}=m_{411}=m_{431}=m_{445}=m_{514}=m_{522}=m_{523}=m_{633}=m_{6314}=m_{641}=m_{827}=4$; $m_{115}=m_{124}=m_{131}=m_{213}=m_{227}=m_{325}=m_{332}=m_{412}=m_{413}=m_{443}=m_{444}=m_{643}=5$; $m_{1210}=m_{312}=m_{317}=m_{331}=m_{333}=m_{334}=m_{447}=m_{512}=m_{611}=m_{642}=6$; $m_{113}=m_{122}=m_{132}=m_{232}=m_{521}=7$; $m_{142}=m_{212}=m_{221}=m_{814}=8$; $m_{126}=m_{631}=9$; $m_{125}=m_{311}=m_{321}=m_{524}=10$; $m_{116}=m_{613}=11$, takes the following form:

$$\boldsymbol{os}=\left\{\bigcup_{i=1}^{8}\boldsymbol{os}_i\left\{\bigcup_{j=1}^{s_i}\boldsymbol{os}_{ij}\left\{\bigcup_{k=1}^{r_{ij}}\boldsymbol{os}_{ijk}\left\{\bigcup_{q=1}^{m_{ijk}}\boldsymbol{os}_{ijkq}(\bigcup_{l=1}^{a_{ijkq}}A_{ijkql})\right\}\right\}\right\}\right\}=$$

$$\{\{\{\{OS_{1111}(A_{11111},A_{11112}),...,OS_{1114}(A_{11141},A_{11142})\},\{OS_{1121}(A_{11211}),OS_{1122}(A_{11221})\},...,$$
$$\{OS_{1171}(),OS_{1172}(),OS_{1173}()\}\},$$
$$\{\{OS_{1211}(A_{12111}),...,OS_{1214}(A_{12141})\},$$
$$\{OS_{1221}(A_{12211},A_{12212},A_{12213}),...,OS_{1227}(A_{12271},A_{12272},A_{12273})\},...,$$
$$\{OS_{12101}(A_{12101},A_{12102}),...,OS_{12106}(A_{12101},A_{12102})\}\}\},$$
$$\{\{\{OS_{2111}(A_{21111},A_{21112}),...,OS_{2113}(A_{21131},A_{21132})\},\{OS_{2121}(A_{21211}),...,OS_{2128}(A_{21281})\},$$
$$\{OS_{2131}(A_{21311},A_{21312}),...,OS_{2135}(A_{21351},A_{21352})\}\},$$
$$\{\{OS_{2211}(A_{22111}),...,OS_{2218}(A_{22181})\},\{OS_{2221}(A_{22211},A_{22212}),...,OS_{2225}(A_{22241},A_{22242})\},...,$$
$$\{OS_{22131}(A_{221311},A_{221312}),...,OS_{22134}(A_{221341},A_{221342})\}\},$$
$$\{\{OS_{2311}(A_{23111},A_{23112}),OS_{2312}(A_{23121},A_{23122})\},\{OS_{2321}(A_{23211}),...,OS_{2327}(A_{23271})\}\}\},...,$$
$$\{\{\{OS_{8111}(A_{81111})\},\{OS_{8121}(A_{81211})\},...,\{OS_{8141}(A_{81411},A_{81412}),...,OS_{8148}(A_{81481},A_{81482})\}\},$$
$$\{\{OS_{8211}(A_{82111}),OS_{8212}(A_{82121})\},\{OS_{8221}(A_{82211},A_{82212}),OS_{8222}(A_{82221},A_{82222})\},...,\{OS_{8291}()\}\}\}\} =$$
$$\{\{\{\{PA.S1.A1.M1(PR,S),...,PA.S1.A1.M4(PR,S)\},\{PA.S1.A2.M1(PR),PA.S1.A2.M2(PR)\},$$
$$\{PA.S1.A7.MT-63(),...,PA.S1.A7.MT-121()\}\},\{\{PA.S2.A1.M1(CP),...,PA.S2.A1.M4(CP)\},$$
$$\{PA.S2.A2.RD-RE-1(AR,R,U),...,PA.S2.A2.M4(AR,R,U)\},...,$$
$$\{PA.S2.A10.PV-DP-1(PR,U),...,PA.S2.A10.M3(PR,U)\}\},...,$$
$$\{\{PA.S4.A1.M1(AR,PR),...PA.S4.A1.M3(AR,PR)\},\{PA.S4.A2.M1(CP,PR),...,$$
$$PA.S4.A2.MT-123(CP,PR)\},\{PA.S4.A3.MT-40(),...,PA.S4.A3.MT-135()\}\},...,$$
$$\{\{\{PR.S1.A1.M1(AR,CP),...,PR.S1.A1.MT-85(AR,CP)\},\{PR.S1.A2.M1\ (CP),...,$$
$$PR.S1.A2.MT-95\ (CP)\},...,\{PR.S1.A3.M2\ (AR,CP),...,$$
$$PR.S1.A3.MT-10\ (AR,CP)\}\},\{\{PR.S2.A1.M1\ (R),...PR.S2.A1.MT-183\ (R)\},$$
$$\{PR.S2.A2.M1\ (CP,R),...,PR.S2.A2.M4\ (CP,R)\},...,\{PR.S2.A13.M1(D,R),...,$$
$$PR.S2.A13.MT-202(D,R)\}\},\{\{PR.S3.A1.M1(CP,CA),PR.S3.A1.M2(CP,CA)\},$$
$$\{PR.S3.A2.M1(CP),PR.S3.A2.M7(CP)\}\},...,\{\{\{RA.S1.A1.M1(R)\},\{RA.S1.A2.M1(NP)\},...,$$
$$\{RA.S1.A4.M1(R,S),...,RA.S1.A4.M8(R,S)\}\},\{\{RA.S2.A1.M1(R),RA.S2.A1.M2(R)\},$$
$$\{RA.S2.A2.M1(R,CP),RA.S2.A2.M2(R,CP)\},\{RA.S2.A9.MT-86()\}\}\}.$$

Table 2 provides an example (taking into account CREF MITRE [1]) of a structured representation of SPM for individual BMs defined within the framework of STMM for cyber resilience assessment. In fact, the table demonstrates the hierarchical indexing of metrics by the considered parameters, and also reflects the correspondence of each metric to a specific BM, the presence of an appropriate approach and a corresponding content context. It is shown that for one BM there can be a set of metrics of different nature: external indicators (e.g., SI-IC-9); universal metrics (e.g., MT-115); local activity-specific metrics (e.g., CS-S1-A3-1, CS-S1-A3-2 etc.). A graphical representation of the proposed STMM, reflecting the relationship between the BM and the SPM of their evaluation, is shown in Figure 1. Let's consider the functioning of STMM (3) using the example of a phishing attack on a bank. For example, for the target $\boldsymbol{GS}_1$ =***ANT*** (Anticipate), BMs *UN.S1.A1* and *UN.S2.A1* were selected.

Table 2

Example of structured mapping of MMM in TMMM of cyber resilience assessment

i	*j*	*k*	*q*	$\boldsymbol{OS}_{ijkq}\left(\bigcup_{l=1}^{a_{ijkq}} A_{ijkql}\right)$	a_{ijkq}	Description (context) of the metric
1	1	1	1	*PA.S1.A1.M1 (PR,S)*	2	Percentage of cyber resources to which access is controlled based on criticality
1	1	1	2	*PA.S1.A1.M2 (PR,S)*	2	Percentage of cyber resources with access controlled based on sensitivity
…						
8	2	8	1	*RA.S2.A8.M1 (D,R)*	2	Number of different technical architecture standards for the same or similar capabilities in use
8	2	8	2	*RA.S2.A8.M2 (D,R)*	2	Percentage of critical data stores for which alternatives

						derived from different data sources are supported
8	2	8	3	*RA.S2.A8.M3 (D,R)*	2	Percentage of system resources for which alternatives from non-intersecting supply chains are stored
8	2	9	1	*RA.S2.A9.MT-86 ()*	0	Percentage of individually managed systems that have implemented one or more resilience techniques

Thus, for i=6, j=k=1, a_{611}=2, $l=\overline{1,a_{611}}$ BM $OS_{6111}(A_{6111},A_{61112})=$ *UN.S1.A1(AM,CA)* characterizes the work with Threat Intelligence (TI) through Analytical Monitoring (*AM*) and Contextual Awareness (*CA*), measuring the receipt and processing of threats based on logs, timestamps, and relevance to the system. The data are timestamps of indicator receipt, TI processing logs, protective Tactics, Techniques, and Procedures (TTP) publication events, etc.

Possible metrics :

1. When i=6, j=k=q=1, a_{6111}=2, $l=\overline{1,a_{6111}}$ metric $OS_{6111}(A_{6111},A_{61112})=$ *UN.S1.A1.M1(AM,CA)* taking into account [1] determines "Number of threat information streams used by the organization" and means how many independent TI channels the bank actually uses. Here, *AM* approaches are used to account for streams and *CA* to assess the usefulness of each stream. For example, these streams include national computer emergency response data (CERT-UA), sector-specific automated sharing platforms (such as the Financial Services Information Sharing and Analysis Center, FS-ISAC), commercial cyber TI feeds, and cross-banking trust-network clearing houses managed under Traffic Light Protocol (TLP) constraints; therefore, *UN.S1.A1.M1(AM,CA)*=4.

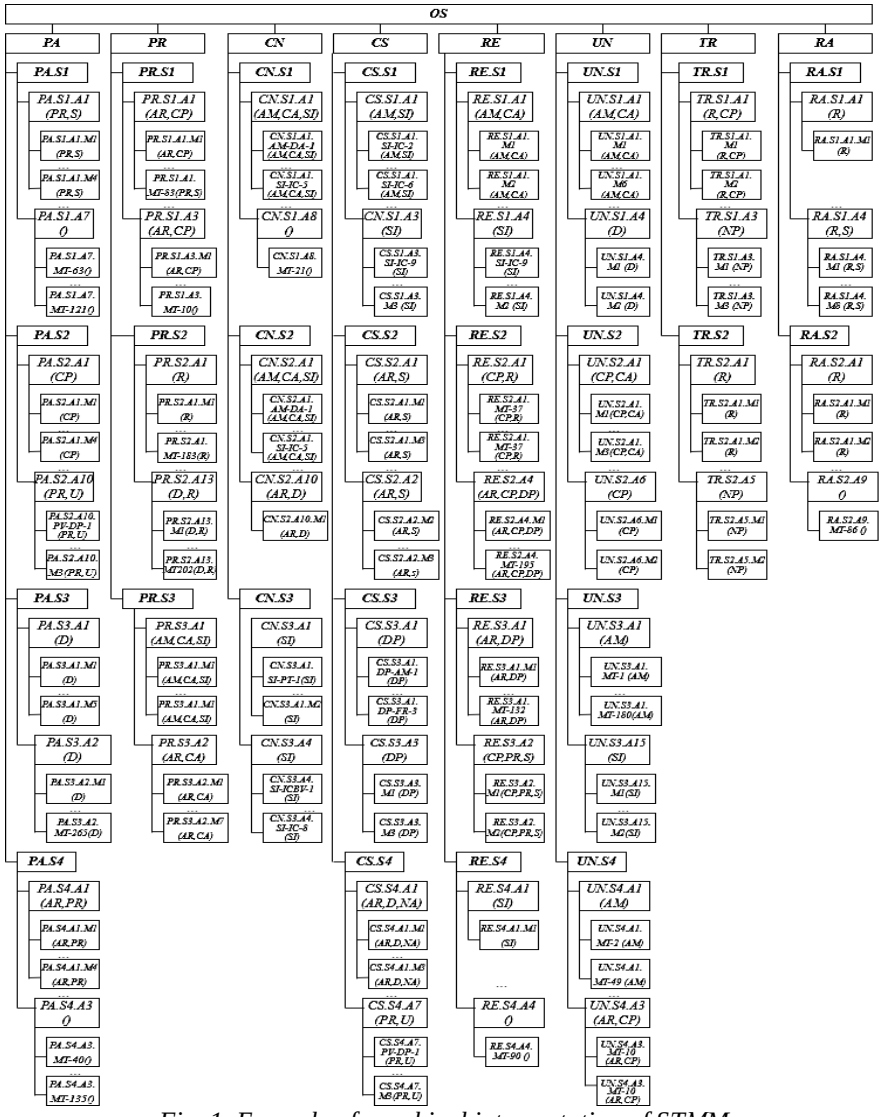

Fig. 1. Example of graphical interpretation of STMM

2. When *i*=6, *j*=*k*=1, *q*=a_{6112}=2, $l=\overline{1,a_{6112}}$ metric $OS_{6112}(A_{61121},A_{61122})=$*UN.S1.A1.M2(AM,CA)* taking into account [1] defines the "Frequency of threat information update received by the organization", which means how often the bank receives a new or updated TI. Here, *AM* approaches are used for timestamps of receipt and *CA* for selection of relevant updates. Data sources can be CERT-UA (1 time/day) and TI-provider (every 15 min), so, for example, *UN.S1.A1.M2(AM,CA)*=15 min.

3. When *i*=6, *j*=*k*=1, *q*=3, a_{6113}=2, $l=\overline{1,a_{6113}}$ metric $OS_{6113}(A_{61131},A_{61132})=$*UN.S1.A1.3(AM,CA)* taking into account [1] defines “Time between receiving threat intelligence and determining its relevance”, which means the delay between the arrival of TI and understanding its importance for the API. Here, *AM* approaches are used to capture the time of receipt and *CA* to analyze the relevance of the context, and for example, *UN.S1.A1.3(AM,CA)*=25 min.

4. When *i*=6, *j*=*k*=1, *q* 4, a_{6114}=2, $l=\overline{1,a_{6114}}$ metric $OS_{6114}(A_{61141},A_{61142})=$*UN.S1.A1.M4(AM,CA)* taking into account [1] defines the "Time between determining the relevance of TI and publishing defense plans (TTP)", which means how quickly TI is converted into defensive actions. Here, *AM* approaches are used to fix the moment of publication and *CA* to coordinate with current defense plans, and for example, *UN.S1.A1.M4(AM,CA)*=45 min.

5. When *i*=6, *j*=*k*=1, *q*=5, a_{6115}=2, $l=\overline{1,a_{6115}}$ metric $OS_{6115}(A_{61151},A_{61152})=$*UN.S1.A1.M5(AM,CA)* taking into account [1] determines the "Frequency of the organization's provision of information about threats to the wider community", which means how actively the bank shares its own observations. Here, the *AM* approaches are used to account for publications and *CA* to check correctness and relevance, and *UN.S1.A1.M5(AM,CA)*=1, if, for example, publication in FS-ISAC is carried out 1 time/week.

6. When *i*=*q*=6, *j*=*k*=1, a_{6116}=2, $l=\overline{1,a_{6116}}$ metric $OS_{6116}(A_{61161},A_{61162})=$*UN.S1.A1.M6(AM,CA)* taking into account [1] defines "Number of threat types (communities) that the organization controls", which means the breadth of coverage of the threat landscape. Here, *CA* approaches are used to classify threat types and *AM* to control their emergence. For example, botnet operators, criminal groups, hacktivists, state actors in total mean 4 types.

When *i*=6, *j*=a_{621}=2, *k*=1, $l=\overline{1,a_{621}}$ *UN.S2.A1(SR,SA)* BM $OS_{621}(A_{6211},A_{6212})=$*UN.S2.A1(CP,CA)* in the phishing example the targets people, roles, business processes, and the consequences depend on which function was compromised and which process this user supported. Therefore, this measure is critical, because without understanding the mission and business context, it is impossible to assess the real impact of phishing. *CA* approaches are used here (since Mission Impact Assessment (MIA), Business Impact Analysis (BIA), and Cyber Journey Analysis (CJA) describe the role of people, processes, and phishing does not affect the system, but the context of its use) and *CP* approaches (since the mission analysis is agreed between Information Security (IS), Human Resources (HR), business units, and the results are used jointly for protection).

Possible metrics :

1. When *i*=6, *j*=a_{6211}=2, *k*=*q*=*1*, $l=\overline{1,a_{6211}}$ the metric $OS_{6211}(A_{62111},A_{62112})=$*UN.S2.A1.M1(CP,CA)* taking into account [1] determines “Time since last MIA, BIA or CJA update” and measures the relevance of the mission’s contextual understanding as the time since the last MIA/BIA/CJA update (e.g., *UN.S2.A1.M1(SR,SA)*=490 days), which determines the accuracy of the impact assessment and the quality of the Cyber Course of Action (CCoA).

2. When *i*=6, *k*=1, *j*=*q*=a_{6212}=2, $l=\overline{1,a_{6212}}$ metric $OS_{6212}(A_{62121},A_{62122})=$*UN.S2.A1.M2(CP,CA)* taking into account [1] determines “MIA, BIA or CJA verification level”, which means the extent to which it is verified that user roles, business functions and critical processes are correctly described and updated. For example, the BIA for payment processes is up-to-date, roles and critical functions are verified and updated less than 12 months ago and the value *UN.S2.A1.M2(CP,CA)*=1 corresponds to the “fully verified” level.

3. When *i*=6, *j*=a_{6213}=2, *k*=1, *q*=3, $l=\overline{1,a_{6213}}$ metric $OS_{6213}(A_{62131},A_{62132})=$*UN.S2.A1.M3(CP,CA)* taking into account [1] determines "Percentage of cyber resources that are rated critical", which means how many accounts, email services, and business applications are rated critical. For example, if *UN.S2.A1.M3(SR,SA)*=80%, then out of 120 relevant resources, 96 are rated critical.

For example, for the target $\boldsymbol{GS}_2$ =*WITH* (Withstand) BMs *CN.S1.A1* and *CN.S1.A2* were selected.

So, for *i*=a_{311}=3, *j*=*k*=1, $l=\overline{1,a_{311}}$ BM *CN.S1.A1(AM,CA,SI)* $OS_{311}(A_{3111},A_{3112},A_{3113})=$ *CN.S1.A1(AM,CA,SI)* is directly aimed at confirming the integrity and behavior after the start of CCoA, and this

is what is critical in phishing. The *AM* (telemetry, logs, inspection results), *CA* (understanding what is critical and what to check first) and Substantiated Integrity (*SI*) (external signs of compromise, checklists, signatures) approaches are used here.

Possible metrics :

1. When $i=a_{3111}=3$, $j=k=q=1$, $l=\overline{1,a_{3111}}$ the metric $OS_{3111}(A_{31111},A_{31112},A_{31113})=$ *CN.S1.A1.AM-DA-1(AM,CA,SI)* taking into account [1] determines "Time spent on mission damage assessment".

2. When $i=a_{3112}=3$, $j=k=1$, $q=2$, $l=\overline{1,a_{3112}}$ the metric $OS_{3112}(A_{31121},A_{31122},A_{31123})=$ *CN.S1.A1.SI-IC-1(AM,CA,SI)* taking into account [1] determines "Average (minimum, maximum) time required to confirm the integrity and/or quality of critical data".

3. When $i=q=a_{3113}=3$, $j=k=1$, $l=\overline{1,a_{3113}}$ the metric $OS_{3113}(A_{31131},A_{31132},A_{31133})=$ *CN.S1.A1.SI-IC-2(AM,CA,SI)* taking into account [1] determines "Percentage of critical data for which integrity (quality) verification is possible".

4. When $i=a_{3114}=3$, $j=k=1$, $q=4$, $l=\overline{1,a_{3114}}$ the metric $OS_{3114}(A_{31141},A_{31142},A_{31143})=$ *CN.S1.A1.M1(AM,CA,SI)* taking into account [1] determines "Percentage of critical data for which integrity (quality) has been confirmed since CCoA initialization".

5. When $i=a_{3115}=3$, $j=k=1$, $q=5$, $l=\overline{1,a_{3115}}$ the metric $OS_{3115}(A_{31151},A_{31152},A_{31153})=$ *CN.S1.A1.SI-IC-3(AM,CA,SI)* taking into account [1] determines "Time required to verify the integrity (quality) of security-critical data".

6. When $i=a_{3116}=3$, $j=k=1$, $q=6$, $l=\overline{1,a_{3116}}$ the metric $OS_{3116}(A_{31161},A_{31162},A_{31163})=$ *CN.S1.A1.SI-BV-1(AM,CA,SI)* taking into account [1] determines "Time to verify the integrity and (or) behavior of critical services or processes". The data are BPM logs, Application monitoring, Transaction traces.

7. When $i=a_{3117}=3$, $j=k=1$, $q=7$, $l=\overline{1,a_{3117}}$ the metric $OS_{3117}(A_{31171},A_{31172},A_{31173})=$ *CN.S1.A1.M2(AM,CA,SI)* taking into account [1] determines "Percentage of critical applications for which integrity (behavior) has been verified since CCoA initiation".

8. When $i=a_{3118}=3$, $j=k=1$, $q=8$, $l=\overline{1,a_{3118}}$ the metric $OS_{3118}(A_{31181},A_{31182},A_{31183})=$ *CN.S1.A1.SI-BV-2(AM,CA,SI)* taking into account [1] determines "Time to check the integrity (behavior) of security-critical services or processes" is similar to *CN.S1.A1.SI-BV-1*, but for an extended set of security-relevant services.

9. When $i=a_{3119}=3$, $j=k=1$, $q=9$, $l=\overline{1,a_{3119}}$ the metric $OS_{3119}(A_{31191},A_{31192},A_{31193})=$ *CN.S1.A1.M3(AM,CA,SI)* taking into account [1] determines "Percentage of security-critical applications for which integrity (behavior) has been verified since CCoA initiation".

10. When $i=a_{31110}=3$, $j=k=1$, $q=10$, $l=\overline{1,a_{31110}}$ the metric $OS_{31110}(A_{311101},A_{311102},A_{311103})=$ *CN.S1.A1.SI-IC-5(AM,CA,SI)* taking into account [1] determines "Software (Service) Integrity Check Frequency".

When $i=a_{321}=3$, $j=2$, $k=1$, $l=\overline{1,a_{321}}$ the BM $OS_{321}(A_{3211},A_{3212},A_{3213})=$ *CN.S2.A1(AM,CA,SI)* is essential because establishing operationalized trust in data and services following a phishing incident requires comprehensive damage assessment and programmatic verification of system integrity once a CCoA is initiated. Since a successful phishing vector leads to the compromise of an employee's account and subsequent risks, such as the distortion of payment details, unauthorized alteration of customer records, modification of system logs, and violation of business service logic – a multi-pronged evaluation approach is mandatory. This measurement process relies on three distinct engineering approaches: analytical monitoring (*AM*) to capture the exact time, frequency, and execution facts of security events; contextual awareness (*CA*) to determine asset criticality within the mission workflow; and substantiated integrity (*SI*) to provide evidentiary, rigorous verification of data and service behavior under stress.

Possible metrics :

The metrics OS_{3211} $(A_{32111},A_{32112},A_{32113})$ = *CN.S2.A1.AM-DA-1 (AM,CA,SI),* OS_{3212} $(A_{32121},A_{32122},A_{32123})$ = *CN.S2.A1.SI-IC-1 (AM,CA,SI),* OS_{3213} $(A_{32131},A_{32132},A_{32133})$ = *CN.S2.A1.SI-IC-2 (AM,CA,SI),* OS_{3214} $(A_{32141},A_{32142},A_{32143})$ = *CN.S2.A1.M1 (AM,CA,SI),* OS_{3215} $(A_{32151},A_{32152},A_{32153})$ = *CN.S2.A1.SI-IC-3 (AM,CA,SI),* OS_{3216} $(A_{32161},A_{32162},A_{32163})$ = *CN.S2.A1.SI-BV-1 (AM,CA,SI),* OS_{3217} $(A_{32171},A_{32172},A_{32173})$ = *CN.S2.A1.M2 (AM,CA,SI),* OS_{3218} $(A_{32181},A_{32182},A_{32183})$ = *CN.S2.A1.SI-BV-2*

(AM,CA,SI), $OS_{3219}\ (A_{32191}, A_{32192}, A_{32193})$ = *CN.S2.A1.M3 (AM,CA,SI),* $OS_{3219}\ (A_{32191}, A_{32192}, A_{32193})$ = *CN.S2.A1.SI-IC-5 (AM,CA,SI)* taking into account [1] determines “Time elapsed to assess mission damage”, "Critical Data Integrity Check Time", "Percentage of data assets for which integrity can be verified", "Percentage of assets for which verification was performed after CCoA", "Time to check security-critical data", "Critical Service Behavior Verification Time", "Percentage of applications for which behavior is verified after CCoA", "Security services verification time", "Percentage of security applications verified after CCoA" and "Frequency of software (service) integrity verification" accordingly.

For target $\boldsymbol{GS}_3$ = *REC* (Recover) for *i*=5, *j*=1, *k*=a_{512} =2, $l=\overline{1,a_{512}}$ the BM was chosen $OS_{512}(A_{5121}, A_{5122})$ =*RE.S1.A2(AM,SI),* which works with suspicious (corrupted) data, and not with the availability of services, and answers the question: “Can we trust the data used by the mission again, and how quickly is this established?”. Phishing compromises credentials and involves unauthorized changes to data, substitution of details, distortion of transactional or reference records. *AM* is used here , since it is necessary to detect suspicious information, record the time of detection, places of verification, notifications, analyze logs, events, alerts. The data are transaction logs, database change logs, DLP (SIEM) notifications, format (range) mismatch signals. The use of *SI* is due to the fact that the metrics directly speak about confirmation of integrity (quality) and checks of origin, format, permissible values are required, and the result is evidentiary trust, not assumptions.

Possible metrics: The metrics $OS_{5121}(A_{51211}, A_{51212})$ = *RE.S1.A2.SI-IC-2(AM,SI),* $OS_{5122}(A_{51221}, A_{51222})$ = *RE.S1.A2.SI-IC-5 (AM,SI),* $OS_{5123}(A_{51231}, A_{51232})$ = *RE.S1.A2.RE-S1-A1-1 (AM,SI),* $OS_{5124}(A_{51241}, A_{51242})$ = *RE.S1.A2.CS-S1-A1-2 (AM,SI),* $OS_{5125}(A_{51251}, A_{51252})$ = *RE.S1.A2.SI-IC-6 (AM,SI)* and $OS_{5126}(A_{51261}, A_{51262})$ = *RE.S1.A2.RE-S1-A1-2 (AM,SI)* taking into account [1] determines “Percentage of mission-critical data assets with integrity (quality) confirmed”, "Percentage of mission-supporting data assets for which integrity (quality) is confirmed", “Average (minimum, maximum) time to detect suspicious information”, "Number of places where checks for corrupted (falsified) information are performed" , "Data validation, including format, types and ranges (yes/no)" and “Time to notify services (business functions) about removing or ignoring suspicious data” accordingly.

For example, for target $\boldsymbol{GS}_4$ = *AD* (Adapt), BMs was selected *TR.S1.A1* and *TR.S2.A2.*

So, for *i*=7, *j*=*k*=1, a_{711}=2, the $l=\overline{1,a_{711}}$ BM $OS_{711}(A_{7111}, A_{7112})$=*TR.S1.A1(R,CP)* is selected because phishing reveals dependence on individual people and the focus shifts from training a person to independence from one person. The Redundancy (*R*) approaches are used because reducing the risk of phishing is eliminating dependence on one role and the Coordinated Protection (*CP*) approach because role changes require coordination with the business and HR.

Possible metrics: The metrics $OS_{7111}(A_{71111}, A_{71112})$ = *TR.S1.A1.M1(R,CP)* and $OS_{7112}(A_{71121}, A_{71122})$ = *TR.S1.A1.M2(R,CP)* taking into account [1] determines "Percentage of mission flows that have been analyzed for shared dependencies and potential single points of failure Single Point of Failure (SPOF)" and "Percentage of mission flows for which no single point of failure SPOF could be identified" accordingly.

When *i*=7, *j*=*k*=a_{722}=2, the $l=\overline{1,a_{722}}$ BM $OS_{722}(A_{7221}, A_{7222})$ =*TR.S2.A2(R,CP)* is used because phishing directly exploits excessive privileges and uses errors in access control. This BM is aimed at preventing privilege escalation after a successful attack, which reduces the risk of system compromise. The *R* approaches are used here because after phishing, there is a redistribution of privileges and the *CP* approaches because access rights are changed in a coordinated manner between IS, IT and the business.

Possible metrics :

1. The metrics $OS_{7221}(A_{72211}, A_{72212})$ = *TR.S2.A2.M1(R,CP)* and $OS_{7222}(A_{72221}, A_{72222})$ = *TR.S2.A2.M2(R,CP)* taking into account [1] determines “Percentage of resources for which privilege requirements have been analyzed in terms of risk-benefit trade-offs” and “Percentage of problematic privilege assignments that have been changed since the last analysis” accordingly.

Taking into account the defined elements of the corresponding sets, formula (3) will take the following form:

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

$$\{\{OS_{3111}(A_{31111}, A_{31112}, A_{31113}), OS_{3112}(A_{31121}, A_{31122}, A_{31123}),$$
$$OS_{3113}(A_{31131}, A_{31132}, A_{31133}), OS_{3114}(A_{31141}, A_{31142}, A_{31143}), OS_{3115}(A_{31151}, A_{31152}, A_{31153}),$$
$$OS_{3116}(A_{31161}, A_{31162}, A_{31163}), OS_{3117}(A_{31171}, A_{31172}, A_{31173}), OS_{3118}(A_{31181}, A_{31182}, A_{31183}),$$
$$OS_{3119}(A_{31191}, A_{31192}, A_{31193}), OS_{31110}(A_{311101}, A_{311102}, A_{311103})\},$$
$$\{OS_{3211}(A_{32111}, A_{32112}, A_{32113}), OS_{3212}(A_{32121}, A_{32122}, A_{32123}), OS_{3213}(A_{32131}, A_{32132}, A_{32133}),$$
$$OS_{3214}(A_{32141}, A_{32142}, A_{32143}), OS_{3215}(A_{32151}, A_{32152}, A_{32153}), OS_{3216}(A_{32161}, A_{32162}, A_{32163}),$$
$$OS_{3217}(A_{32171}, A_{32172}, A_{32173}), OS_{3218}(A_{32181}, A_{32182}, A_{32183}), OS_{3219}(A_{32191}, A_{32192}, A_{32193}),$$
$$OS_{3219}(A_{32191}, A_{32192}, A_{32193})\}\}, \{\{OS_{5121}(A_{51211}, A_{51212}), OS_{5122}(A_{51221}, A_{51222}),$$
$$OS_{5123}(A_{51231}, A_{51232}), OS_{5124}(A_{51241}, A_{51242}), OS_{5125}(A_{51251}, A_{51252}),$$
$$OS_{5126}(A_{51261}, A_{51262})\}\}, \{\{OS_{7111}(A_{71111}, A_{71112}), OS_{7112}(A_{71121}, A_{71122})\},$$
$$\{OS_{7221}(A_{72211}, A_{72212}), OS_{7222}(A_{72221}, A_{72222})\}\}\} = \{\{\{\{UN.S1.A1.M1(AM, CA),$$
$$UN.S1.A1.M2(AM, CA), UN.S1.A1.M3(AM, CA), UN.S1.A1.M4(AM, CA),$$
$$UN.S1.A1.M5(AM, CA), UN.S1.A1.M6(AM, CA)\},$$
$$\{UN.S2.A1.M1(CP, CA), UN.S2.A1.M2(CP, CA), UN.S2.A1.M3(CP, CA)\}\},$$
$$\{\{CN.S1.A1.AM - DA - 1(AM, CA, SI), CN.S1.A1.SI - IC - 1(AM, CA, SI),$$
$$CN.S1.A1.SI - IC - 2(AM, CA, SI), CN.S1.A1.M1(AM, CA, SI),$$
$$CN.S1.A1.SI - IC - 3(AM, CA, SI), CN.S1.A1.SI - BV - 1(AM, CA, SI),$$
$$CN.S1.A1.M2(AM, CA, SI), CN.S1.A1.SI - BV - 2(AM, CA, SI),$$
$$CN.S1.A1.M3(AM, CA, SI), CN.S1.A1.SI - IC - 5(AM, CA, SI)\},$$
$$\{CN.S2.A1.AM - DA - 1(AM, CA, SI), CN.S2.A1.SI - IC - 1\ (AM, CA, SI),$$
$$CN.S2.A1.SI - IC - 2\ (AM, CA, SI), CN.S2.A1.M1\ (AM, CA, SI),$$
$$CN.S2.A1.SI - IC - 3\ (AM, CA, SI), CN.S2.A1.SI - BV - 1(AM, CA, SI),$$
$$CN.S2.A1.M2\ (AM, CA, SI), CN.S2.A1.SI - BV - 2(AM, CA, SI),$$
$$CN.S2.A1.M3\ (AM, CA, SI), CN.S2.A1.SI - IC - 5\ (AM, CA, SI)\}\},$$
$$\{\{RE.S1.A2.SI - IC - 2(AM, SI), RE.S1.A2.SI - IC - 5(AM, SI),$$
$$RE.S1.A2.RE - S1 - A1 - 1(AM, SI), RE.S1.A2.CS - S1 - A1 - 2(AM,\ SI),$$
$$RE.S1.A2.SI - IC - 6(AM,\ SI), RE.S1.A2.RE - S1 - A1 - 2(AM, SI)\}\},$$
$$\{\{TR.S1.A1.M1(R, CP), TR.S1.A1.M2(R, CP)\}, \{TR.S2.A2.M1(R, CP),$$
$$TR.S2.A2.M2(R, CP)\}\}\}.$$

A graphical representation of the STMM for a specific example of a phishing attack on a bank with the selection of relevant elements of the sets ***GS*** and ***OS***, the corresponding BMs, and possible metrics is shown in Fig. 2.

So, STMM was first developed to assess the cyber resilience of CIF, which, by introducing SPM for each BM, formalizing the functional mapping "BM → SPM" and distinguishing structural and operational metrics, provides an opportunity to create a basis for forming an integral cyber resilience index. Therefore, the work translates the concept of cyber resilience from the level of structural formalization (data modeling) to the level of quantitative measurement (metric formalization). From a practical point of view, the model further enables: automation of cyber resilience assessment processes; formation of sound management decisions regarding prioritization of activities; model integration into risk management systems and SIEM/SOC platforms; development of software tools for monitoring the state of resilience; adaptation of the model to the requirements of national critical infrastructure protection standards; use for educational and scientific purposes for formalized training in the concept of cyber resilience. The model can be directly applied to: building digital twin models of cyber resilience of CIF; assessing the effectiveness of implemented CCoA; conducting audits and benchmarking of protection strategies.

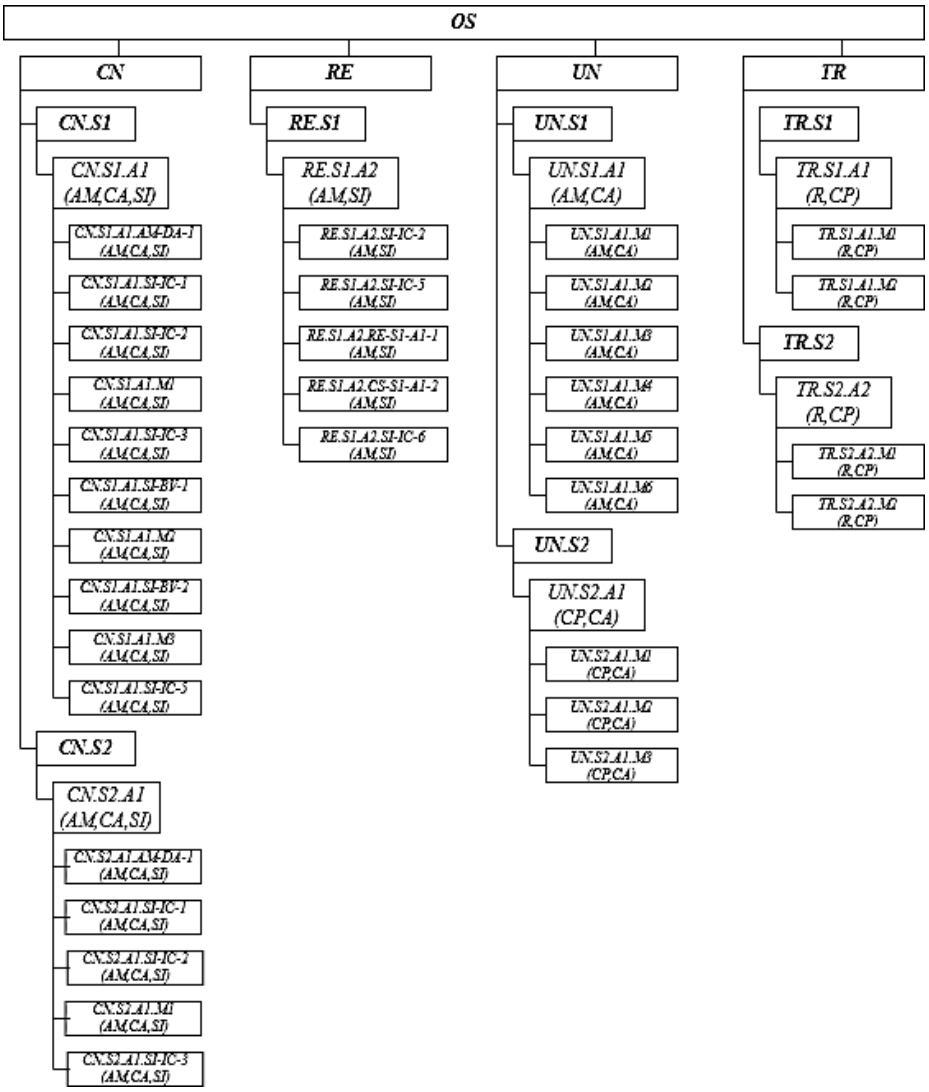

Fig. 2. Graphical representation of STMM using the example of a phishing attack on a bank

Discussion. The results confirm that the proposed STMM eliminates key limitations of existing cyber resilience assessment approaches, particularly the lack of a formalized link between base measures and metrics. Unlike prior work relying on isolated or heuristic metrics, the model introduces a strict functional mapping "BM → SPM", ensuring consistency and reproducibility. A significant contribution is the introduction of metric set cardinality, reflecting the complexity and multidimensionality of assessment. Its variability depends on the implementation context, providing a formal representation of cyber resilience adaptability. In this framework, "cyber resilience adaptability" is formally defined as the operational capability of the metric model to dynamically alter its assessment structure and the cardinality of its evaluation sets in response to shifts in the system implementation context, architectural configurations, or evolving threat landscapes. Rather than relying on a static compliance baseline, adaptability ensures that the measurement framework scales its precision, expanding or condensing the active set of metrics, based on the specific arguments implemented at a given critical infrastructure facility.

The distinction between structural (ex-ante) and operational (ex-post) metrics enables integrated evaluation of system readiness and behavior during incidents, overcoming limitations of models focused solely on compliance or incidents. The model complements existing frameworks (MITRE CREF, NIST CSF, DORA) by adding a formal metric layer, supporting quantitative assessment and automation. It also enables the construction of integral indicators and the use of heterogeneous data sources, enhancing practical applicability. Limitations include the lack of universal normalization and aggregation rules and dependence on high-quality data and monitoring infrastructure. Overall, the results provide a foundation for further development of quantitative cyber resilience assessment methods.

It is worth noting that while the mathematical core of the proposed STMM is strictly generalized and applicable to any structured taxonomy, its practical verification in this study is purposely aligned with the MITRE CREF taxonomy due to its status as an industry standard. Given the standard page constraints of a journal manuscript, an exhaustive breakdown of the underlying MITRE matrix is omitted; readers seeking a deeper dive into specific technique definitions are encouraged to utilize the framework's baseline documentation alongside the integrated variable maps provided in Table 2.

Conclusions. As a result of the study, the scientific task of developing a set-theoretic metric model for assessing the cyber resilience of CIF was solved, which is confirmed by the following: 1) the SPM for each BM is formalized as an element of a set-theoretic construction, which allowed moving from the fragmentary use of individual indicators to a systematic representation of metrics in the form of sets. It is shown that for one BM there can be several metrics of different nature (external, universal, local); 2) the cardinality of the set of metrics was determined and its dependence on the methods of implementing the database and the context of application was demonstrated. In particular, for different databases, the cardinality varies from 1 to 11 metrics, which quantitatively confirms the variability and complexity of assessing cyber resilience; 3) a distinction has been introduced between structural (ex-ante) and operational (ex-post) metrics, which eliminates the methodological incompleteness of the assessment and ensures simultaneous consideration of both the system's preparedness and its actual behavior during incidents; 4) a functional mapping "BM → SPM" was constructed, which formalizes the relationship between cyber resilience measures and their quantitative measurement, which allowed us to move to algorithmization of the assessment process and creates the basis for automated analysis systems; 5) a generalized metric model has been developed that provides a single mathematical basis for combining disparate metrics within a single evaluation system, which increases the reproducibility and comparability of results; 6) specific examples confirm the consistency of the model with MITRE CREF, in particular through the mapping of real databases onto sets of metrics with a specific cardinality, which demonstrates the practical applicability of the model and its scalability for different types of CIF.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Bodeau, D., Graubart, R., McQuaid, R., & Woodill, J. (2018). *Cyber resiliency metrics, measures of effectiveness, and scoring: Enabling systems engineers and program managers to select the most useful assessment methods*. MITRE Technical Report.
2. Bodeau, D., Brtis, J., Graubart, R., & Salwen, J. (2015). *Cyber resiliency engineering aid-The updated cyber resiliency engineering framework and guidance on applying cyber resiliency techniques* (MITRE Technical Report MTR150264). MITRE.
3. Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., & McQuaid, R. (2021). *Developing cyber-resilient systems: A systems security engineering approach* (NIST Special Publication 800-160, Vol. 2, Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-160v2r1
4. Linkov, I., Eisenberg, D., Plourde, K., et al. (2013). Resilience metrics for cyber systems. *Environment Systems and Decisions, 33*(4), 471-476. https://doi.org/10.1007/s10669-013-9485-y
5. Björck, F., Henkel, M., Stirna, J., & Zdravkovic, J. (2015). Cyber resilience-Fundamentals for a definition. In *New contributions in information systems and technologies* (pp. 311–316). Springer. https://doi.org/10.1007/978-3-319-16486-1_31
6. Cam, H., Mouallem, P., Mo, J., & Farris, J. (2016). Resilience metrics for cyber systems. *INCOSE International Symposium, 26*(1), 1476-1489.
7. Linkov, I., & Kott, A. (2019). *Cyber resilience of systems and networks*. Springer.
8. Zio, E. (2016). Challenges in the vulnerability and risk analysis of critical infrastructures. *Reliability Engineering & System Safety, 152*, 137-150. https://doi.org/10.1016/j.ress.2016.02.009
9. Petersen, L., Fallou, L., Reilly, P., & Serafinelli, E. (2019). A resilience assessment framework for critical infrastructure. *International Journal of Critical Infrastructure Protection, 25*, 1-14. https://doi.org/10.1016/j.ijcip.2019.01.002
10. Yusta, J., Correa, G., & Lacal-Arántegui, R. (2011). Methodologies and applications for critical infrastructure protection: State-of-the-art. *Energy Policy, 39*(10), 6100-6119. https://doi.org/10.1016/j.enpol.2011.07.010
11. Rinaldi, S., Peerenboom, J., & Kelly, T. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine, 21*(6), 11-25. https://doi.org/10.1109/37.969131
12. Ouyang, M. (2014). Review on modeling and simulation of interdependent critical infrastructure systems. *Reliability Engineering & System Safety, 121*, 43-60. https://doi.org/10.1016/j.ress.2013.06.040

13. Alcaraz, C., & Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. *International Journal of Critical Infrastructure Protection, 8*, 53-66. https://doi.org/10.1016/j.ijcip.2014.12.002
14. Musman, S., & Temin, A. (2015). A cyber mission impact assessment tool. In *IEEE International Symposium on Technologies for Homeland Security (HST)* (pp. 1-7).
15. Falco, G., Caldera, C., & Shrobe, H. (2018). IIoT cybersecurity risk modeling for SCADA systems. *IEEE Internet of Things Journal, 5*(6), 4486-4495. https://doi.org/10.1109/JIOT.2018.2822842
16. Haque, M., Shetty, S., & Krishnappa, B. (2020). Cybersecurity resilience model for industrial control systems. *IET Cyber-Physical Systems: Theory & Applications, 5*(3), 271-282.
17. Jackson, S., & Ferris, T. (2013). Resilience principles for engineered systems. *Systems Engineering, 16*(2), 152-164. https://doi.org/10.1002/sys.21228
18. Rieger, C., Gertman, D., & McQueen, M. (2009). Resilient control systems: Next generation design research. In *IEEE Conference on Human System Interactions* (pp. 632-636).
19. Woods, D. (2015). Four concepts for resilience and the implications for the future of resilience engineering. *Reliability Engineering & System Safety, 141*, 5-9. https://doi.org/10.1016/j.ress.2015.03.018
20. Stergiopoulos, G., Kotzanikolaou, P., Theocharidou, M., et al. (2016). Time-based critical infrastructure dependency analysis for large-scale and cross-sectoral failures. *International Journal of Critical Infrastructure Protection, 12*, 46-60. https://doi.org/10.1016/j.ijcip.2015.12.002
21. Hossain, M., Moniruzzaman, M., Muhammad, G., et al. (2014). Big data-driven service composition using parallel clustered particle swarm optimization in mobile environment. *IEEE Transactions on Services Computing, 9*(5), 806-817.
22. Teixeira, A., Shames, I., Sandberg, H., & Johansson, K. H. (2015). A secure control framework for resource-limited adversaries. *Automatica, 51*, 135-148. https://doi.org/10.1016/j.automatica.2014.10.067
23. Vugrin, E., Warren, D., Ehlen, M., & Camphouse, R. (2010). A framework for assessing the resilience of infrastructure and economic systems. In *Sustainable and resilient critical infrastructure systems* (pp. 77-116). Springer. https://doi.org/10.1007/978-3-642-11405-2_3
24. Hosseini, S., Barker, K., & Ramirez-Marquez, J. (2016). A review of definitions and measures of system resilience. *Reliability Engineering & System Safety, 145*, 47-61. https://doi.org/10.1016/j.ress.2015.08.006
25. Ganin, A., Massaro, E., Gutfraind, A., et al. (2016). Operational resilience: Concepts, design and analysis. *Scientific Reports, 6*(1), 19540. https://doi.org/10.1038/srep19540
26. Amin, M. (2005). Energy infrastructure defense systems. *Proceedings of the IEEE, 93*(5), 861-875. https://doi.org/10.1109/JPROC.2005.847254
27. Pursiainen, C. (2018). Critical infrastructure resilience: A Nordic model in the making? *International Journal of Disaster Risk Reduction, 27*, 632-641. https://doi.org/10.1016/j.ijdrr.2017.10.007
28. Theocharidou, M., Kotzanikolaou, P., & Gritzalis, D. (2016). A multi-layer criticality assessment methodology based on interdependencies. *Computers & Security, 62*, 251-272. https://doi.org/10.1016/j.cose.2016.08.004
29. Giannopoulos, G., Filippini, R., & Schimmer, M. (2012). *Risk assessment methodologies for critical infrastructure protection. Part I: A state of the art* (European Commission Joint Research Centre Technical Report 25286).
30. Setola, R., Rosato, V., Kyriakides, E., & Rome, E. (Eds.). (2016). *Managing the complexity of critical infrastructures: A modeling and simulation approach*. Springer International Publishing. https://doi.org/10.1007/978-3-319-31074-9
31. National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSWP 29). https://doi.org/10.6028/NIST.CSWP.29
32. National Institute of Standards and Technology. (2025). *Integrating cybersecurity and enterprise risk management (ERM)* (NIST IR 8286 Rev. 1). https://doi.org/10.6028/NIST.IR.8286r1
33. European Parliament & Council of the European Union. (2022). Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA). *Official Journal of the European Union, L 333*.
34. MITRE Corporation. (2024). *Cyber Resiliency Engineering Framework (CREF) Navigator*. The MITRE Corporation.
35. AlHidaifi, A., et al. (2024). Simulation-based quantification of cyber resilience for critical systems. *Decision Support Systems, 178*.
36. Lezzi, M., et al. (2025). Measuring cyber resilience in Industrial IoT: A systematic review. *Service Oriented Computing and Applications*.
37. Cho, H., et al. (2025). A quantitative framework for cyber resilience assessment with normalization techniques. *Electronics, 14*, 2465.

38. Cybersecurity and Infrastructure Security Agency. (2020). *Cyber Resilience Review (CRR): Method description and self-assessment user guide*. CISA.
39. Caralli, R. A., Allen, J. H., & White, D. W. (2011). *CERT resilience management model (CERT-RMM): A maturity model for managing operational resilience*. Addison-Wesley Professional.
40. *Cyber Resilience Capability Maturity Model (CR-CMM): Standard and tools for organizational resilience assessment*. (n.d.). https://cr-cmm.org/
41. Korchenko, O., Kharchenko, V., Khokhlachova, Yu., & Zhurov, Yu. (2026). Sustainable development of smart regions: A set-theoretic data model for assessing the cyber resilience of critical infrastructure entities. *Zviazok, 4*, 22-44.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (34), 2026
ISSN 2663 – 4023

Корченко Олександр Григорович
Доктор технічних наук, професор
Державний університет інформаційно-комунікаційних технологій, Київ
ORCID:0000-0003-3376-0631
agkorchenko@gmail.com

Хохлачова Юлія Євгеніївна
Кандидат технічних наук, професор
Державний торговельно-економічний університет, м. Київ;
Державний університет інформаційно-комунікаційних технологій, Київ
ORCID:0000-0002-0787-5112
yuliiahohlachova@gmail.com

ТЕОРЕТИКО-МНОЖИННА МЕТРИЧНА МОДЕЛЬ ДЛЯ ОЦІНКИ КІБЕРСТІЙКОСТІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Анотація. Розглядається проблема формалізованої оцінки кіберстійкості критичної інфраструктури в умовах зростаючої складності кіберзагроз. Існуючі підходи є фрагментованими та не мають чіткого зв'язку між базовими показниками кіберстійкості та їх оціночними метриками. Метою цього дослідження є розробка теоретико-множинної метричної моделі, яка формалізує набір можливих показників для кожного базового показника. Запропоновано формальне представлення показників як функції базових показників, що вводить концепцію кардинальності множин та її залежність від контексту застосування. Структурні (ex-ante) та операційні (ex-post) показники інтегровані в єдину математичну структуру, а також визначено функціональне відображення «базовий показник → набір можливих показників». Результати дозволяють перейти до формалізованої кількісної оцінки та підтримують розробку інтегральних показників та автоматизованого аналізу, покращуючи відтворюваність, порівнянність та валідність оцінки кіберстійкості.

Ключові слова: кіберстійкість, оцінка кіберстійкості, об'єкти критичної інфраструктури, показники кіберстійкості, теоретико-множинна модель, теоретико-множинний підхід, MITER CREF, інформаційна безпека, кібербезпека, захист інформації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Bodeau, D., Graubart, R., McQuaid, R., & Woodill, J. (2018). *Cyber resiliency metrics, measures of effectiveness, and scoring: Enabling systems engineers and program managers to select the most useful assessment methods*. MITRE Technical Report.
2. Bodeau, D., Brtis, J., Graubart, R., & Salwen, J. (2015). *Cyber resiliency engineering aid-The updated cyber resiliency engineering framework and guidance on applying cyber resiliency techniques* (MITRE Technical Report MTR150264). MITRE.
3. Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., & McQuaid, R. (2021). *Developing cyber-resilient systems: A systems security engineering approach* (NIST Special Publication 800-160, Vol. 2, Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-160v2r1
4. Linkov, I., Eisenberg, D., Plourde, K., et al. (2013). Resilience metrics for cyber systems. *Environment Systems and Decisions, 33*(4), 471-476. https://doi.org/10.1007/s10669-013-9485-y
5. Björck, F., Henkel, M., Stirna, J., & Zdravkovic, J. (2015). Cyber resilience-Fundamentals for a definition. In *New contributions in information systems and technologies* (pp. 311–316). Springer. https://doi.org/10.1007/978-3-319-16486-1_31
6. Cam, H., Mouallem, P., Mo, J., & Farris, J. (2016). Resilience metrics for cyber systems. *INCOSE International Symposium, 26*(1), 1476-1489.
7. Linkov, I., & Kott, A. (2019). *Cyber resilience of systems and networks*. Springer.
8. Zio, E. (2016). Challenges in the vulnerability and risk analysis of critical infrastructures. *Reliability Engineering & System Safety, 152*, 137-150. https://doi.org/10.1016/j.ress.2016.02.009
9. Petersen, L., Fallou, L., Reilly, P., & Serafinelli, E. (2019). A resilience assessment framework for critical infrastructure. *International Journal of Critical Infrastructure Protection, 25*, 1-14. https://doi.org/10.1016/j.ijcip.2019.01.002

10. Yusta, J., Correa, G., & Lacal-Arántegui, R. (2011). Methodologies and applications for critical infrastructure protection: State-of-the-art. *Energy Policy, 39*(10), 6100-6119. https://doi.org/10.1016/j.enpol.2011.07.010
11. Rinaldi, S., Peerenboom, J., & Kelly, T. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine, 21*(6), 11-25. https://doi.org/10.1109/37.969131
12. Ouyang, M. (2014). Review on modeling and simulation of interdependent critical infrastructure systems. *Reliability Engineering & System Safety, 121*, 43-60. https://doi.org/10.1016/j.ress.2013.06.040
13. Alcaraz, C., & Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. *International Journal of Critical Infrastructure Protection, 8*, 53-66. https://doi.org/10.1016/j.ijcip.2014.12.002
14. Musman, S., & Temin, A. (2015). A cyber mission impact assessment tool. In *IEEE International Symposium on Technologies for Homeland Security (HST)* (pp. 1-7).
15. Falco, G., Caldera, C., & Shrobe, H. (2018). IIoT cybersecurity risk modeling for SCADA systems. *IEEE Internet of Things Journal, 5*(6), 4486-4495. https://doi.org/10.1109/JIOT.2018.2822842
16. Haque, M., Shetty, S., & Krishnappa, B. (2020). Cybersecurity resilience model for industrial control systems. *IET Cyber-Physical Systems: Theory & Applications, 5*(3), 271-282.
17. Jackson, S., & Ferris, T. (2013). Resilience principles for engineered systems. *Systems Engineering, 16*(2), 152-164. https://doi.org/10.1002/sys.21228
18. Rieger, C., Gertman, D., & McQueen, M. (2009). Resilient control systems: Next generation design research. In *IEEE Conference on Human System Interactions* (pp. 632-636).
19. Woods, D. (2015). Four concepts for resilience and the implications for the future of resilience engineering. *Reliability Engineering & System Safety, 141*, 5-9. https://doi.org/10.1016/j.ress.2015.03.018
20. Stergiopoulos, G., Kotzanikolaou, P., Theocharidou, M., et al. (2016). Time-based critical infrastructure dependency analysis for large-scale and cross-sectoral failures. *International Journal of Critical Infrastructure Protection, 12*, 46-60. https://doi.org/10.1016/j.ijcip.2015.12.002
21. Hossain, M., Moniruzzaman, M., Muhammad, G., et al. (2014). Big data-driven service composition using parallel clustered particle swarm optimization in mobile environment. *IEEE Transactions on Services Computing, 9*(5), 806-817.
22. Teixeira, A., Shames, I., Sandberg, H., & Johansson, K. H. (2015). A secure control framework for resource-limited adversaries. *Automatica, 51*, 135-148. https://doi.org/10.1016/j.automatica.2014.10.067
23. Vugrin, E., Warren, D., Ehlen, M., & Camphouse, R. (2010). A framework for assessing the resilience of infrastructure and economic systems. In *Sustainable and resilient critical infrastructure systems* (pp. 77-116). Springer. https://doi.org/10.1007/978-3-642-11405-2_3
24. Hosseini, S., Barker, K., & Ramirez-Marquez, J. (2016). A review of definitions and measures of system resilience. *Reliability Engineering & System Safety, 145*, 47-61. https://doi.org/10.1016/j.ress.2015.08.006
25. Ganin, A., Massaro, E., Gutfraind, A., et al. (2016). Operational resilience: Concepts, design and analysis. *Scientific Reports, 6*(1), 19540. https://doi.org/10.1038/srep19540
26. Amin, M. (2005). Energy infrastructure defense systems. *Proceedings of the IEEE, 93*(5), 861-875. https://doi.org/10.1109/JPROC.2005.847254
27. Pursiainen, C. (2018). Critical infrastructure resilience: A Nordic model in the making? *International Journal of Disaster Risk Reduction, 27*, 632-641. https://doi.org/10.1016/j.ijdrr.2017.10.007
28. Theocharidou, M., Kotzanikolaou, P., & Gritzalis, D. (2016). A multi-layer criticality assessment methodology based on interdependencies. *Computers & Security, 62*, 251-272. https://doi.org/10.1016/j.cose.2016.08.004
29. Giannopoulos, G., Filippini, R., & Schimmer, M. (2012). *Risk assessment methodologies for critical infrastructure protection. Part I: A state of the art* (European Commission Joint Research Centre Technical Report 25286).
30. Setola, R., Rosato, V., Kyriakides, E., & Rome, E. (Eds.). (2016). *Managing the complexity of critical infrastructures: A modeling and simulation approach*. Springer International Publishing. https://doi.org/10.1007/978-3-319-31074-9
31. National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSWP 29). https://doi.org/10.6028/NIST.CSWP.29
32. National Institute of Standards and Technology. (2025). *Integrating cybersecurity and enterprise risk management (ERM)* (NIST IR 8286 Rev. 1). https://doi.org/10.6028/NIST.IR.8286r1
33. European Parliament & Council of the European Union. (2022). Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA). *Official Journal of the European Union, L 333*.

34. MITRE Corporation. (2024). *Cyber Resiliency Engineering Framework (CREF) Navigator*. The MITRE Corporation.
35. AlHidaifi, A., et al. (2024). Simulation-based quantification of cyber resilience for critical systems. *Decision Support Systems, 178*.
36. Lezzi, M., et al. (2025). Measuring cyber resilience in Industrial IoT: A systematic review. *Service Oriented Computing and Applications*.
37. Cho, H., et al. (2025). A quantitative framework for cyber resilience assessment with normalization techniques. *Electronics, 14*, 2465.
38. Cybersecurity and Infrastructure Security Agency. (2020). *Cyber Resilience Review (CRR): Method description and self-assessment user guide*. CISA.
39. Caralli, R. A., Allen, J. H., & White, D. W. (2011). *CERT resilience management model (CERT-RMM): A maturity model for managing operational resilience*. Addison-Wesley Professional.
40. *Cyber Resilience Capability Maturity Model (CR-CMM): Standard and tools for organizational resilience assessment*. (n.d.). https://cr-cmm.org/
41. Korchenko, O., Kharchenko, V., Khokhlachova, Yu., & Zhurov, Yu. (2026). Sustainable development of smart regions: A set-theoretic data model for assessing the cyber resilience of critical infrastructure entities. *Zviazok, 4*, 22-44.

Отримано редакцією журналу / Received: 06.02.26
Прорецензовано / Revised: 16.02.26
Схвалено до друку / Accepted: 24.09.26