UDC 681.32:007.5
DOI: 10.15587/1729-4061.2022.263416

DEVELOPMENT OF A CONCEPT FOR CYBERSECURITY METRICS CLASSIFICATION

Serhii Yevseiev
Corresponding author
Doctor of Technical Sciences, Professor, Head of Department
Department of Cyber Security*
E-mail: Serhii.Yevseiev@gmail.com

Oleksandr Milov
Doctor of Technical Sciences, Professor
Department of Cyber Security*

Ivan Opirskyy
Doctor of Technical Sciences, Professor
Department of Information Security
Lviv Polytechnic National University
S. Bandery str., 12, Lviv, Ukraine, 79013

Olha Dunaievska
PhD, Associate Professor
Department of Computer Mathematics and Data Analysis*

Oleksandr Huk
Adjunct
Department of Communications and Automated Control Systems
National Defence University of Ukraine named after Ivan Cherniakhovskyi
Povitroflotskyi ave., 28, Kyiv, Ukraine, 03049

Volodymyr Pogorelov
PhD, Associate Professor
Department of Information Technology Security
National Aviation University
Liubomyra Huzara str., 1, Kyiv, Ukraine, 03058

Kyrylo Bondarenko
Postgraduate Student
Department of Cyber Security and Information Technologies
Simon Kuznets Kharkiv National University of Economics
Nauky ave., 9-A, Kharkiv, Ukraine, 61166

Nataliia Zviertseva
Postgraduate Student
Department of Software Engineering and Management Intelligent Technologies*

Yevgen Melenti
PhD, Associate Professor
Special Department No. 3 «Tactical-Special Training,
Marksmanship Training and Special Physical Training»
Juridical Personnel Training Institute for the Security Service
of Ukraine Yaroslav Mudryi National Law University
Myronosytska str., 71, Kharkiv, Ukraine, 61002

Bogdan Tomashevsky
PhD, Senior Researcher
Department of Cyber Security
Ternopil Ivan Puluj National Technical University
Ruska str., 56, Ternopil, Ukraine, 46001

*National Technical University «Kharkiv Polytechnic Institute»
Kyrpychva str., 2, Kharkiv, Ukraine, 61002

The development of the IT industry and computing resources allows the formation of cyberphysical social systems (CPSS), which are the integration of wireless mobile and Internet technologies and the combination of the Internet of things with the technologies of cyberphysical systems. To build protection systems, while minimizing both computing and economic costs, various sets of security profiles are used, ensuring the continuity of critical business processes. To assess/compare the level of CPSS security, various assessment methods based on a set of metrics are generally used. Security metrics are tools for providing up-to-date information about the state of the security level, cost characteristics/parameters from both the defense and attack sides. However, the choice of such sets is not always the same/understandable to the average person. This, firstly, leads to the absence of a generally accepted and unambiguous definition, which means that one system is more secure than another. Secondly, it does not take into account the signs of synergy and hybridity of modern targeted attacks. Without this knowledge, it is impossible to show that the metric measures the security level objectively. Thirdly, there is no universal formal model for all metrics that could be used for rigorous analysis. The paper explores the possibility of defining a basic formal model (classifier) for analyzing security metrics. The proposed security assessment model takes into account not only the level of secrecy of information resources, the level of provision of security services, but also allows, based on the requirements put forward, forming the necessary set of security assessment metrics, taking into account the requirements for the continuity of business processes. The average value of the provision of security services to CPSS information resources is 0.99, with an average value of the security level of information resources of 0.8

Keywords: security metrics, security assessment model, security metrics classifier, threat synergy

Received date 21.06.2022
Accepted date 04.08.2022
Published date 31.08.2022

How to Cite: *Yevseiev, S., Milov, O., Opirskyy, I., Dunaievska, O., Huk, O., Pogorelov, V., Bondarenko, K., Zviertseva, N., Melenti, Y., Tomashevsky, B. (2022). Development of a concept for cybersecurity metrics classification. Eastern-European Journal of Enterprise Technologies, 4 (4 (118)), 6–18. doi: https://doi.org/10.15587/1729-4061.2022.263416*

1. Introduction

The automation of information systems to ensure the efficient provision of services has led to a number of information security problems, manifested primarily in a multiple increase in the number of attacks on cyberphysical social systems. To prevent such cyber incidents, system owners are investing more and more in various protection mechanisms, as well as improving systems and workflows to make them more secure. However, the return on investment and/or subsequent security enhancement is largely unknown.

It is a generally accepted fact that achieving «100 % system security» is an ideal condition [1]. However, one of the priorities in security research is the ability to measure how close an information system is to its ideal state (in terms of security) [2]. The paper [3] of the Infosec Research Council (IRC) published in November 2005 and the paper [4] of the US Department of Homeland Security published in 2009 mention «enterprise-level security metrics» as a challenging area of research. This confirms the fact that little progress has been made in this important field.

There are several well-known security standards such as ISO/IEC 27001:2005 [5], ISO/IEC 27002:2005 [6], COBIT 5 [7] and NISTSP 800-53 [8] that provide recommendations and best practices for managing information security in enterprises. However, these standards do not explicitly define security indicators that enterprises can implement. In turn, the ISO/IEC 27004:2009 [9] and NISTSP 800-55 [10] standards define ways to develop a program of enterprise security indicators. However, they do not provide specific enterprise-level metrics that could be used to measure and improve enterprise security. The main complaint about security standards is that they are poorly coordinated with each other, focusing on security auditing, but paying little attention to measuring security indicators [11].

This state of affairs raises the following questions:

– what is the amount of financial investment needed to «secure» oneself from attacks;

– how effective are security improvement changes made to software;

– are the company's workflows or processes safe enough;

– how the addition of a third-party software component will affect the system security;

– how can legislation requiring certain levels of security be enforced if the level of security is unknown.

With regard to cybersecurity, it should be possible to perform a cybersystem security analysis in order to obtain security indicators showing whether the system is protected from various forms of attacks and what are the vulnerabilities [12]. These questions can be answered if there is a way to measure the level of cybersystem security. The solution can be a well-defined, effective security metric. So, the issues of classification of existing security metrics, as well as the development of methodological foundations for the implementation of such methods, are relevant for the correct assessment and improvement of the security level of cyberphysical social systems.

2. Literature review and problem statement

For more than a decade, the security community has been looking for metrics that can measure security correctly and unambiguously. A number of different metrics have been proposed, from specific ones measuring a particular part of the system (such as the time between antivirus updates) to general metrics assessing overall security (such as attack surface). However, neither a single metric nor a closed set of metrics is generally accepted to measure security correctly, and many of these metrics are used concurrently.

Such a number and variety of metrics are caused by the inability to prove that the metric actually measures security. One reason for this uncertainty is that there is no clear, unambiguous, and generally accepted definition of «more secure» relationships. Every inventor of security metrics defines what is «more secure» with the help of metrics, but does not prove that the metric actually indicates security changes [12].

To assess the current state of the security level and individual security indicators, many different security indicators are used [13, 14]. However, most of them are far from the results described above. They may be ineffective and meaningless. For example, a traditional indicator is the number of viruses detected and removed, say, using a firewall. This metric doesn't make sense because it doesn't say anything about the number of viruses that weren't detected and entered the system, or why so many viruses even try to get in. In general, the safety indicator should [15]:

– measure indicators significant for the organization;

– be reproducible;

– be objective and impartial;

– evaluate progress towards the goal over time.

The noted properties of a good security metric also describe certain metrics having a scientific basis, such as throughput metrics in performance design. Throughput measures the number of tasks a computing system executes per second. It is a quantitative measure of a computing system based on the laws of physics. It is also meaningful, reproducible, objective, and unbiased, and can measure the improvement in system performance over time towards a throughput goal. This leads to the question of what scientific framework can lead to the emergence of such science-based indicators.

The published literature mainly focuses on finding ways to measure specific characteristics of security devices. However, in terms of enterprise information security, it is necessary to develop a comprehensive model that can measure the state of information security of the entire enterprise. It is crucial that this model includes formal syntax and semantics. The following categories of publications on security indicators and metrics can be distinguished: describing the nature of security indicators, measuring cybersystem security, managing IT security risks, and measuring the effectiveness of the security provision process.

The first group of publications is related to the description of the nature of cybersecurity indicators.

The most fundamental publication on cybersecurity measurements and metrics and the existing problems is [16]. First of all, the publication defines a number of stakeholder expectations that contribute to the success of efforts being made in the field of measuring cybersecurity indicators used in certain metrics. It is noted that metrics, or underlying indicators, should underpin ongoing improvement efforts aimed at monitoring and improving security in the long term. To do this, the indicators included in the metric must exist in a form that facilitates measurement, requires minimal investment to organize data collection. It is noted that the gap between stakeholders' expectations and what can actually be achieved creates unfavorable conditions for the success of measuring the selected indicators.

With regards to automating measurements and using real-time cybersecurity metrics, it is emphasized that cybersecurity metrics must be properly designed with accurate data and carefully validated in order to automate the process of achieving the desired results.

As an important point in the development and use of cybersecurity metrics, it is noted that they must ensure the maximum and timely return on investment. This follows from the fact that senior managers generally want to use metrics to measure the cost-effectiveness of their security programs.

The factors for the successful creation and use of effective cybersecurity metrics are as follows. First of all, attention is drawn to the management's commitment to the chosen security program. Because cybersecurity programs never «end» and are a critical component of organizations' efforts to improve overall security, continued success requires regular confirmation of the leadership's commitment to the chosen direction. Having reliable data is the second main driver behind successful cybersecurity programs. Without reliable data, these programs are unreliable and fail to meet stakeholder expectations. Metrics that are easy to use and understand are the key to success. Easy-to-use and understandable metrics require the use of a common collection, analysis and reporting methodology, and stakeholders' involvement in the creation, use and refinement of these metrics. Proactive and preventative metrics that can be used to predict the future are challenging as most measurement data are based on the recent past. The ability to determine in advance the course of action to prevent adverse events based on the indicators included in the metric depends on the ability of the organization to process and analyze measurement data and extrapolate their value to future periods of work.

The publication also notes gaps in various aspects of the construction and use of cybersecurity metrics, the elimination of which will help improve the efficiency, effectiveness and impact of cybersecurity programs at all levels of cyberphysical social systems. These are measures aimed at real-time operation and/or self-healing of systems. «Self-healing» metrics is a new term for metrics that allow an improvement action to be taken automatically based on a current or predicted value recorded by an automated tool. Improving the unification of data formats used in metrics and using experience and lessons learned from other industries aim to expand the knowledge base of specialists in measuring security indicators and improving cybersecurity metrics.

The paper [17] discusses the scientific basis for security and security metrics with examples and research ideas from various industries. Particular attention is paid to the security of the computer system. At the same time, the work does not touch upon the issues of building a cybersecurity metric as an integral indicator of system security. The focus on the industry of computer equipment manufacturing is typical for [18]. The paper proposes not only a taxonomy of high-level security indicators for information and communication technology companies, but also considers a specific example of a taxonomy of security indicators, which makes the work interesting in terms of a practical approach to security.

The publications [19–22] are more theoretical. A discussion of the shortcomings of traditional security metrics is given in [19], the characteristics of «good» metrics are presented; security maturity models with examples are considered. The topics discussed provide answers to questions about the theoretical aspects of the practical application of metrics in terms of «more or less» secure systems, as an approach to comparing the security of different systems. An increase in the level of theorization is presented in [20], where not only formal models of security measurement are presented, but also artificial intelligence methods are proposed for a wide range of applications. A brief description of risk as a security metric, alternative security metrics, and what constitutes a «good» metric can be found in [21]. At the same time, it should be noted that the security metric is reduced to the selection of one or another set of system indicators.

The monograph [22] discusses security indicators for enterprise applications; moreover, security indicators are widely applied not only to computing systems, but to all types of corporate processes. And [11] focuses on the enterprise, covers security indicators in terms of efficiency, implementation, operations, compliance, costs, people, organizations.

A common remark for the cited sources is as follows: reducing the metric to the selection of a set of measured or estimated indicators, and not to the method of aggregating the selected indicators into one integral indicator.

The following group of publications deals with the measurement of system security.

The paper [23] suggests considering the «attack surface» as a security measure of one system in relation to another. The attack surface is described in three dimensions:

– goals and factors contributing to implementation;

– channels and protocols;

– access rights.

The development of [23], the work [24] contains practical advice to developers on how to reduce the «attack surface» of the program code focused on classic Microsoft operating systems, both for workstations and servers.

The works [25, 26] propose a structure for assessing network security based on attack schedules or access paths for carrying out an attack. Two networks are compared having different numbers of attack paths, and on this basis, a comparative security assessment of these networks is given. As an example, the initial filling («weighting») of the attack graph with known vulnerabilities and probabilities of their exploitation is considered, and then «checked» to obtain a metric of the overall security and risks of the network. Thus, the concept of a metric is reduced to a single indicator of the number of ways to implement attacks and their quantitative indicators.

A similar approach based on the attack graph is presented in [27]. An attack graph-based attack resilience metric is proposed to measure the relative security of network configurations. The metric includes two composition operators for calculating the total attack resistance based on given individual resistances, taking into account the relationship between them. Despite taking into account more complex dependencies, the metric is still reduced to attack graph indicators.

The use of attack graphs as the basis of a security metric is suggested in a number of papers cited below.

The work [28] proposes an attack graph-based metric for network security that includes the likelihood of potential multistage attacks combining multiple vulnerabilities to achieve an attack target. The definition of the metric is claimed to have an intuitive and meaningful interpretation that is useful in real-world decision-making. The paper [23] presents an attack graph-based method for evaluating network security based on the probability of an attack. The metric is designed based on a set of vulnerabilities of components whose security levels are already known. The disadvantage of the proposed solutions is the static nature of the constructed metric, which makes it difficult to use it in real time, as well as when vulnerability indicators change. To determine the dynamic nature of vulnerabilities that change over time, [29] proposes a dynamic Bayesian network (DBN) model. The attack graph is converted into a DBN by applying conditional probabilities to the nodes calculated based on the common vulnerability scoring system (CVSS). The network security is calculated based on the probability of successful attacks. The work [30] also proposes to measure network security using Bayesian network attack graphs so that relationships such as the exploitation of one vulnerability facilitating the exploitation of another vulnerability can be captured.

The initial proposal and analysis of mathematical definitions of security indicators, such as «number of attacks», «minimum cost of attack», «maximum probability of attack» and even «attack surface» are given in [31]. The paper [32] proposes an initial framework for assessing system security by decomposing the system into security-sensitive components and assigning security ratings to each component. Summation of the scores of the components allows an assessment of system reliability. As you can see, the metric as a way to form an integral security indicator is reduced to a simple summation. In other words, the metric is an additive convolution of individual security estimates, which, on the one hand, greatly simplifies the metric, and on the other hand, limits its use due to primitiveness.

The work [33] considers the taxonomy of security indicators in relation to telecommunication systems, which can be considered a certain progress in the design of metrics. This is because they allow ranking security indicators by importance and selecting those that are most significant in the formation of a cybersecurity indicator. The advantage of the paper is also the broad overview of security indicators.

A separate group of works is the publications devoted to a review of various security indicators and standards that may be applicable to software development. The paper [34] compares the relevance of different approaches to security properties such as authenticity and confidentiality. The work [35] presents the formulation of security indicators in terms of weaknesses and vulnerabilities. However, it does not show how the significance (weight) of vulnerabilities could be determined for completely new software. So, it is unclear how the final security metric can be used to improve security.

The paper [36] discusses the software security properties that can be measured and proposes a number of software security properties along with related metrics. In [20], an approach to assessing the security of a software system being developed is proposed, security requirements are derived and a method for assessing the probability of violation of requirements based on individual risks of system components is given.

A model of the effect of interaction with the user system for the systematic identification and analysis of security problems in service-oriented architectures is proposed in [37]. The model is claimed to provide a framework for the security metrics of software services, and one such metric is identified and illustrated. At the same time, the work does not contain data on the possibilities of using other metrics for these purposes.

The paper [38] describes a robust but incomplete framework that can be used to accurately identify and evaluate new security metrics defined by intrinsic software security attributes. The work argues that the properties are necessary but not sufficient conditions for good security indicators, and hence the question of good or bad metrics remains open.

The paper [39] proposes a security model derived from UML sequence diagrams. This model can be used as the basis for architecture-level security metrics and, for example, model-based privacy metrics. The advantage of the work is its sufficient formalization, which can be used to evaluate the effectiveness of certain security metrics.

The publication [40] proposes «*k*-zero-day safety» as a security metric. This metric counts the number of unknown zero-day vulnerabilities that would be required to compromise a network asset, regardless of what those vulnerabilities might be. The metric is defined in terms of an abstract model of networks and attacks. Algorithms for calculating the metric are included, making this publication practically useful.

The paper [41] proposes to quantify security using partial test results, the tool code is checked until a failure is detected. The totality of such failures determines the level of software insecurity.

The transition from the analysis of a software product to the information system as a whole was made in [8]. The work provides guidance on the design, selection, and implementation of measures at the level of the information system and security program to evaluate the implementation, performance, and impact of security controls and other security-related activities.

The publication [42] can be considered as a guide to evaluating the effectiveness of information security and a basis for developing security measures. The work describes recommended security measures, including risk assessment as a control.

The reference [43] discusses the requirements for software certification. It is proposed that certification be based on the product and not on the development process, considers the Common Criteria (CC) as a possible product-based certification model. Although this document focuses on software certification, it is relevant to security metrics as it describes the CC elements that are relevant to software product security assessment. Special mention should be made of fundamental monographs.

The reference [44] describes the process of security risk management, discusses the pros and cons of various risk measures, including threat and attack risks. The work [45] provides a framework for developing a risk management program, contains definitions and recommendations for assessing and mitigating risks in IT systems as a basis for designing security metrics. The paper [46] describes the stages of the cybersecurity resilience model, which can be a measure of the security status of an organization as a whole. The work [47] describes complex persistent threats and stages of the cybersecurity resilience model.

The presented review of publications on cybersecurity metrics showed that the presence of such a number of metrics does not provide an objective assessment of the security level of the network infrastructure. In addition, many approaches do not take into account the computing resources (the emergence of a full-scale quantum computer) of the attacking side. The level of secrecy of information resources is also not taken into account, which sometimes leads to a significant excess of resources spent and the «excess» of protection mechanisms, financing and energy costs. The proposed approach makes it possible to systematize the aggregation of metrics by priorities, taking into account the hybridity and synergy of targeted attacks. In addition, the level of secrecy (required security time) of information resources (cyberphysical social system, CPSS), as well as the computational and economic costs of ensuring the required level of security, are taken into account.

3. The aim and objectives of the study

The aim of the work is to develop a concept for building a security metrics classifier, as well as a stochastic model for assessing the current state of security of CPSS infrastructure elements. This approach minimizes the cost of preventive protection measures, selects optimal security strategies, and also takes into account the level of secrecy of CPSS information assets (resources).

To achieve the aim, the following objectives were set:

– to develop a classifier of security metrics, a model for selecting metrics based on CPSS continuous business processes;

– to develop a stochastic model of the current security level of CPSS information assets (resources).

4. Materials and methods

In the formation of a high-tech society, social networks based on Internet services have become one of the most effective and popular means of mass communication. Such a synthesis of social Internet services (SIS) with cyberphysical systems makes it possible to form a cyberphysical social system (CPSS).

CPSS is a set of subjects and objects of the cybernetic, physical and social worlds that allow the formation of «smart» communities, on the one hand, and intellectual space, on the other. In CPSS, users are service consumers, and physical objects in the form of various devices are service providers. To provide security services, cryptographic protection mechanisms are commonly used in such systems, which allows, depending on the level of secrecy of information assets, forming various security profiles. The object of research is security metrics and the possibility of their classification to assess the current state of the CPSS security level. To assess the level of security, various methods of analysis based on security metrics are used. In addition, security metrics allow not only evaluating quantitative or qualitative security indicators, but also comparing systems with each other in terms of security. For simplicity of presentation, it is proposed to consider the main aspects of security metrics that significantly affect the assessment of the current security status of critical infrastructure objects. The main aspects of security metrics are proposed to include:

– the degree of provision of security services (confidentiality, integrity, authenticity, availability and involvement);

– evaluation of computational and financial costs on each side (attack and defense);

– the likelihood of meeting the requirements of regulators of international and legislative acts of the state;

– taking into account the secrecy level of information resources.

When considering the Concept, specific targeted cyberattacks on critical infrastructure elements are neglected, but their hybridity and synergy are taken into account.

In [48], a formal representation of the metric is given: the metric is a function M on a set Q that determines the distance between two members of the set $\left(M:Q\times Q\mapsto\mathbb{R}\right)$ and satisfies the following properties:

$$M\left(q_1,q_2\right)\rangle 0,\ \forall q_1,q_2\in Q\ \text{(positivity)};$$

$$M\left(q_1,q_2\right)\rangle 0,\text{if } fq_1=q_2,\ \forall q_1,q_2\in Q\ \text{(identity)};$$

$$M\left(q_1,q_2\right)=M\left(q_2,q_1\right),\ \forall q_1,q_2\in Q\ \text{(symmetry)};$$

$$M\left(q_1,q_3\right)\langle M\left(q_1,q_2\right)+M\left(q_2,q_3\right),$$
$$\forall q_1,q_2,q_3\in Q\ \text{(triangle inequality)}.$$

Thus, the metrics allow you to determine the quantitative characteristics of individual components of the security level and/or the level of a possible implementation of a targeted attack, as well as to compare identical systems in terms of security. When considering the classification of security metrics, we use the following concepts: minimum (single attack, minimum cost, minimum time), average probable, realistic and maximum.

Each element of information resources $I_{A_i}\in\{I_A\}$ can be described by the vector $I_{A_i}=(Type_i,A_i^C,A_i^I A_i^A,A_i^{Au},A_i^{Inv},\beta_i)$. $Type_i$ is the type of information asset, described by a set of basic values: $Type_i=\{CI_i, PD_i, CD_i, TS_i, StR_i, PubI_i, ContI_i, PI_i\}$, where CI_i is confidential information, PD_i is payment documents, CD_i is credit documents , TS_i is trade secret, StR_i is statistical reports, $PubI_i$ is public information, $ContI_i$ is control information, PI_i is personal information. A_i^C, $A_i^I A_i^A$, A_i^{Au}, $A_i^{Inv} A_i^{Au}$, A_i^{Inv} are security services (A_i^C – confidentiality, A_i^I – integrity, A_i^A – availability, A_i^{Au} – authenticity, A_i^{Inv} – involvement); β_i is a metric of the ratio of time and degree of information secrecy for an asset (critical 1.0, high 0.75, medium 0.5, low 0.25, very low 0.01).

We introduce the following definitions:

– the number of attacks (W_{att}) – a metric of the number of attacks on the CPSS, which allows evaluating the results of penetration and determining the system security based on the simplest graph analysis;

– the minimum cost of an attack ($C_{att}^{\min}$) – a metric of financial costs/computing resources (time costs), which allows estimating the «cost» of an attack. Based on [1], determining the «possibility» to implement a cyberattack on the CPSS;

– the cost of an attack (C_{att}) – a metric of the cost of detecting the possibility of an attack (vulnerability detection) and the cost of performing an attack (implementation of attack targets) on the CPSS.

Attack, detection and blocking/removal costs can be defined as follows:

1) minimum costs for detection, blocking/removal (protection cost) ($E_{det\,att}^{\min}$) – a metric of financial costs/computing resources (time costs), which allows estimating the «cost» of CPSS preventive protection measures;

2) minimum costs for declining attacks ($E_{decl\ att}^{\min}$) – a metric that determines the minimum costs of the defense side necessary to achieve the maximum level of CPSS counteraction;

3) the minimum cost of reducing all attacks ($C_{red}^{\min}$) – a metric that allows determining the minimum cost of implementing CPSS preventive protection measures;

4) the minimum duration of an attack ($T_{att}^{\min}$) – a metric that determines the shortest time to implement an attack, and the less protected is the CPSS;

– the duration of attacks (T_{att}) – a metric that evaluates the duration of an attack, which allows assessing the system's ability to form CPSS preventive protection measures;

– the probability of an attack (P_{att}) – a metric that determines the probability of reaching the target of an attack on the CPSS;

– the maximum probability of an attack ($P_{att}^{\max}$) – a metric that determines the probability of reaching the target of an attack with $T_{att}^{\min}$;

– the overall probability of hacking ($P_{hacking}^{overall}$) – a metric for determining the maximum level of security in case of implementing $P_{att}^{\max}$.

The resulting value can be considered as the probability that an attacker, having performed all attacks one after another, will be able to compromise/crack the CPSS;

– the average probability of system compromise ($P_{hacking}^{average}$) – a metric that takes into account the frequency of various attacks on the CPSS;

– compliance percentage – a metric for managers who need to be sure that the system security complies with some rules or laws. The metric allows you to estimate the optimal number of security measures and shows that adding more proposed security measures does not necessarily improve security, as the proposed security measures are not specific to the needs of a particular system.

The choice of an appropriate metric depends on what continuous business processes circulate in the system and the secrecy level of CPSS information resources. This should take into account the priorities defined by the security policy and the security profiles implemented in the CPSS. The reduction cost provides information to those responsible for the security budget (security managers and financial managers). This metric can be useful when additional investment in security is required.

The minimum cost of an attack, the probabilities and the duration of attacks are more useful for analysts studying attackers. Once analyzed, these metrics can be provided to security personnel who can improve the system by knowing the weakest points. Of course, these values are of interest to an attacker who wants to carry out an attack as efficiently as possible.

Considering the security level, it is also necessary to take into account the financial and computing resources of attackers, their qualifications and goals. In [1, 2, 12], a classification of attackers is proposed taking into account these indicators, as well as the hybridity and synergy of modern targeted attacks. Thus, it is proposed to consider two models of an attacker.

The «worst attacker» has a complete understanding of the system: he knows all possible attacks, the cost of each attack, and the probability that the attack will be successful. With all this knowledge, the attacker will always choose the «least expensive or most likely» way to implement a targeted attack. Thus, the minimum cost of an attack and/or the most probable attack metrics are used to assess the level of security.

Although such attackers are popular in the literature, they are not suitable for the «blind attacker» who knows nothing about the system. The attacker finds the first possible attack and tries to execute it, because it is not known how easy the attack will be. In other words, the attacker chooses attacks randomly. Thus, the C_{att} and P_{att} metrics are used to assess the level of security.

Of course, neither the first nor the second model is suitable for describing the attacker's behavior, since the attacker always has some knowledge about the system, but this knowledge is not complete. Therefore, new and more realistic attacker models are required. On the other hand, the two extreme models already presented show that different conclusions can be drawn regarding the attacker's behavior under consideration.

Thus, the introduced metrics allow introducing a systematic approach to analyzing the results and obtaining an objective assessment of the current level of CPSS security. The results also provide a «rough» estimation of system compromise/hacking (Table 1).

Table 1

Systematization of the results of quantitative assessments of security metrics

Metric	Min	Average	Real	Max
W_{att}	$W_{att}^{\min}$	W_{att}^{Av}	W_{att}^{Re}	$W_{att}^{\max}$
C_{att}	$C_{att}^{\min}$	C_{att}^{Av}	C_{att}^{Re}	$C_{att}^{\max}$
$E_{det\,att}$	$E_{det\,att}^{\min}$	$E_{det\,att}^{Av}$	$E_{det\,att}^{\mathrm{Re}}$	$E_{det\,att}^{\max}$
$E_{decl\,att}$	$E_{decl\;att}^{\min}$	$E_{decl\;att}^{Av}$	$E_{decl\;att}^{\mathrm{Re}}$	$E_{decl\;att}^{\max}$
C_{red}	$C_{red}^{\min}$	C_{red}^{Av}	C_{red}^{Re}	$C_{red}^{\max}$
T_{att}	$T_{att}^{\min}$	T_{att}^{Av}	T_{att}^{Re}	$T_{att}^{\max}$
P_{att}	$P_{att}^{\min}$	P_{att}^{Av}	P_{att}^{Re}	$P_{att}^{\max}$

The analysis of Table 1 provides the formation of an objective assessment of the CPSS security level based on $P_{hacking}^{average}$:

$$P_{hacking}^{average} = \left(W_{att}, C_{att}, E_{det\,att}, E_{decl\;att}, C_{red}, T_{att}, P_{att}\right),$$

or

$$P_{hacking}^{average} \approx P_{att}^{\max}. \tag{1}$$

At the same time, it is necessary to consider the weighting factors of both security services and secrecy level, which will reduce the computational and economic costs of preventive measures to protect/counter targeted/cyberattacks. In [49], to calculate the weighting factors of criteria, it is proposed to use the method of pairwise comparison of criteria based on floating preference forming the basis of the analytic hierarchy process. By this method, the decision maker (DM) first forms his logical judgments about the qualitative level of criteria preference in relation to each other, according to Table 2, column 2. Then, using a verbal-numerical scale, he translates the qualitative values of preference into quantitative values, Table 2, column 3.

Table 2

Fundamental verbal-numerical scale of the relative preference of criteria proposed by Saaty

No.	Qualitative determination of criteria preference level	Quantitative value of criteria preference level, (k_{ij})
1	Equal preference	1
2	Weak degree of preference	2
3	Medium degree of preference	3
4	Above average preference	4
5	Moderately strong preference	5
6	Strong preference	6
7	Very strong preference	7
8	Very, very strong preference	8
9	Absolute preference	9

If in the pairwise comparison matrix of criteria, the criterion of row (i) is superior to the criterion of column (j), then this matrix element is assigned the corresponding number k_{ij} from Table 2, column 3. If the criterion specified in the row is not dominant in relation to the criterion indicated in the column, then the reciprocal of the preference coefficient, i.e. $1/k_{ij}$, is always written into the corresponding matrix element. The diagonal elements of the pairwise comparison matrix of criteria are always equal to one.

In order for the results obtained using this method to be correct, it is necessary that the matrix be fully consistent with the decision maker's judgments. For this, the following conditions must be met for any elements k_{ik}, k_{ij}, k_{jk} [49]:

– the condition of consistency of the matrix elements as follows:

$$k_{ik}=k_{ij}\times k_{jk}; \tag{2}$$

– the condition of transitivity of the matrix elements, according to which we have if:

$$k_{ik}>k_{ij}, \text{ and } k_{ij}>k_{jk}, \text{ then } k_{ik}>k_{jk}. \tag{3}$$

The eigenvectors of the criteria are calculated by the formula:

$$C_i = \left(k_{i1} \times k_{i2} \cdots k_{in}\right)^{1/n}, \quad (4)$$

where k_{ij} is the quantitative value of the criterion preference level (Table 2).

Next, the importance factors α_i, i.e., the weighting factors of these criteria, are determined by the following formula:

$$\alpha_i = \frac{C_i}{\sum_{i=1}^{n} C_i}. \quad (5)$$

When using the security services of the practical integrity-confidentiality-availability (ICA) model, the indicators of a comparative analysis of the three security services for the proposed floating preference method have the form presented in Table 3.

Table 3

Preference analysis of three criteria by the floating preference method

Security service	K_1	K_2	K_3	C_i	α_i
K_1	1	2	3	1.817	0.540
K_2	1/2	1	2	1	0.297
K_3	1/3	1/2	1	0.551	0.163

To assess the current level of security, the model [45] was taken as a basis.

Let CPSS, {*N*} and, {*Pr*} be the sets of vulnerabilities/threats and elements of the protection system. $P_{\{N\}}(\{Pr\})$ – the probability of vulnerabilities/threats covered by the elements of the information protection system (IPS), and $P_{\{N\}}^{unprotected}(\{\mathrm{Pr}\})$ – the probability of uncovered vulnerabilities/threats of the IPS.

Then,

$$P_{\{N\}}\left(\{\mathrm{Pr}\}\right) \cap P_{\{N\}}^{unprotected}\left(\{\mathrm{Pr}\}\right) = \varnothing, \quad (6)$$

$$P_{\{N\}}\left(\{\mathrm{Pr}\}\right) \cup \sum P_{\{N\}}^{unprotected}\left(\{\mathrm{Pr}\}\right) = \{N\}. \quad (7)$$

Thus, an absolutely secure system must satisfy the following conditions: $\{N\}=\varnothing$, i.e. there are no threats, there is no relation ρ such that $P_{\{N\}}^{unprotected}(\{\mathrm{Pr}\})\rho\{N\}$.

The second condition means that vulnerabilities and threats exist, but there are no pairs that can harm the system. In other words, there are vulnerabilities without corresponding threats and threats without corresponding vulnerabilities.

Then, $I_{A_i} \in \{I_A\}$ is information resources. Let s_{ij} be the j^{th} value of the security service of the i^{th} asset. The security matrix *S* is defined as follows:

$$S = \begin{bmatrix} s_{11} & s_{12} & \cdots & s_{1n} \\ s_{21} & s_{22} & \cdots & s_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ s_{m1} & s_{m2} & \cdots & s_{mn} \end{bmatrix}, \quad (8)$$

where

$$0 < a_{ij} < 1 \text{ for } i=1, 2, ,...,n; j=1, 2, ..., m. \quad (9)$$

Therefore, a completely unprotected system would have the following threat matrix:

$$S_{att}^{\max} = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 \\ \cdots & \cdots & \cdots & \cdots \\ 1 & 1 & \cdots & 1 \end{bmatrix}, \quad (10)$$

where $s_{ij}=1$, $\left\|S_{att}^{\max}\right\|$ is a stochastic matrix.

For the matrix $S^{real} = \left\|s_{ij}\right\|_{m\times n}$, we denote the Frobenius norm of the matrix $\left\|S^{real}\right\|_{Fn}$ by:

$$\left\|S^{real}\right\|_{Fn} = \sqrt{\frac{\sum_i \sum_j s_{ij}^2}{mn}}, \quad (11)$$

then the security level (performing security services A_i^C, A_i^I, A_i^A):

$$S_{att}^{\max} - S = \begin{bmatrix} 1-s_{11} & 1-s_{12} & \cdots & 1-s_{1n} \\ 1-s_{21} & 1-s_{22} & \cdots & 1-s_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ 1-s_{m1} & 1-s_{m2} & \cdots & 1-s_{mn} \end{bmatrix}. \quad (12)$$

This can be used to determine the penetration/hacking probability as follows:

$$\text{Security} = \left\|S_{att}^{\max} - S\right\|_{Fn} = \sqrt{\frac{\sum_i \sum_j \left(1-s_{ij}^2\right)}{mn}} \times 100\,\%, \quad (13)$$

then, an estimate of the current state of CPSS security is defined by:

$$\text{Insecurity} = \left(1 - \left\|S_{att}^{\max} - S\right\|_{Fn}\right) \times 100\,\%. \quad (14)$$

Thus, if $s_{ij}=1$ for all *i*, *j*, then *Insecurity*=0 %, i.e. the system is absolutely secure; on the other hand, if $s_{ij}=0$ for all *i*, *j*, then *Insecurity*=100 %, i.e. the system is absolutely insecure.

5. Results of the development of methodological foundations for constructing a classifier of security metrics

5. 1. Development of a classifier of security metrics

To form a classifier of security metrics, it is proposed to use the approach proposed in [1, 12], i.e., to use the division of metrics into platforms according to belonging to the obtained comparative parameters. This approach provides the scalability of the classifier and objective assessment of the current security level, taking into account the selected priorities. The proposed classifier is shown in Fig. 1.

At the first stage, based on the expert evaluation of security metrics, a base of security metrics and classification tuples of metrics are formed. Thus, an objective assessment of possible «patterns» of security metrics is formed, taking into account not only the priorities of CPSS continuous business processes, but also the attacker's capabilities.

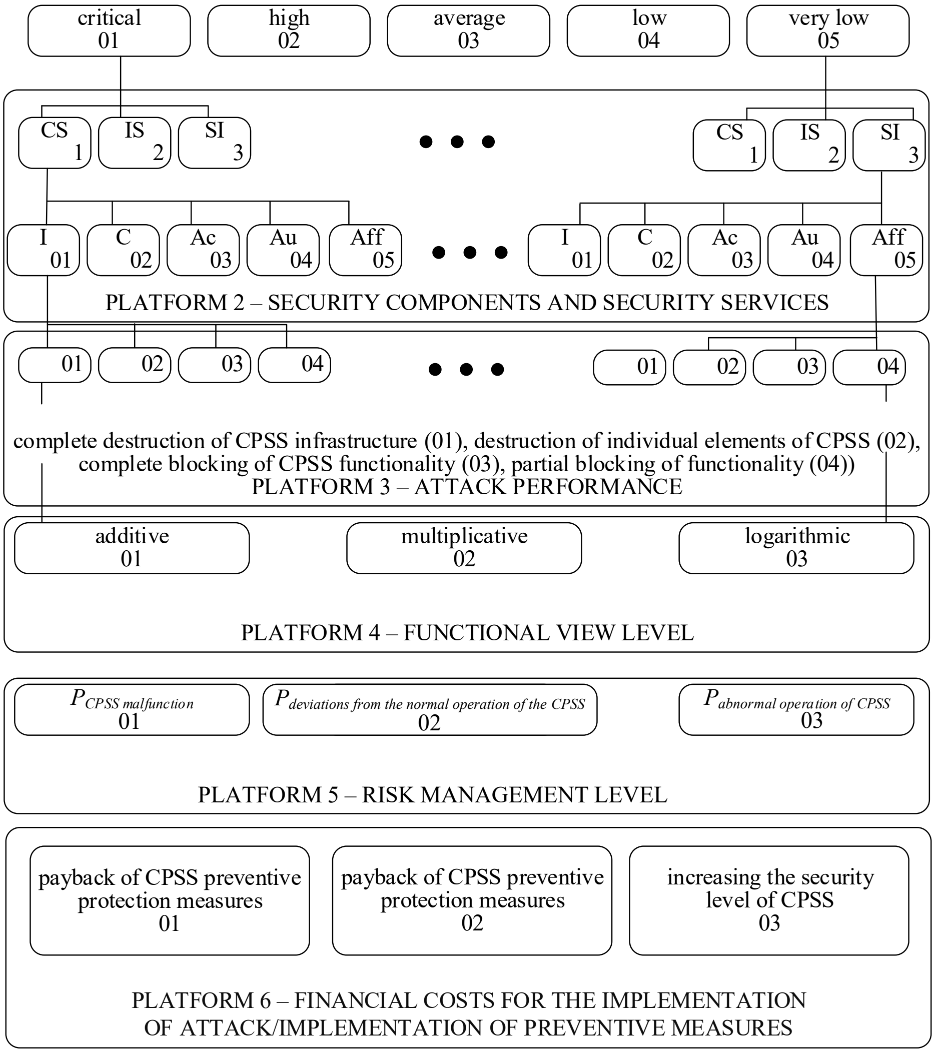
critical 01
high 02
average 03
low 04
very low 05
CS 1
IS 2
SI 3
CS 1
IS 2
SI 3
I 01
C 02
Ac 03
Au 04
Aff 05
I 01
C 02
Ac 03
Au 04
Aff 05
PLATFORM 2 – SECURITY COMPONENTS AND SECURITY SERVICES
01
02
03
04
01
02
03
04
complete destruction of CPSS infrastructure (01), destruction of individual elements of CPSS (02), complete blocking of CPSS functionality (03), partial blocking of functionality (04))
PLATFORM 3 – ATTACK PERFORMANCE
additive 01
multiplicative 02
logarithmic 03
PLATFORM 4 – FUNCTIONAL VIEW LEVEL
P CPSS malfunction 01
P deviations from the normal operation of the CPSS 02
P abnormal operation of CPSS 03
PLATFORM 5 – RISK MANAGEMENT LEVEL
payback of CPSS preventive protection measures 01
payback of CPSS preventive protection measures 02
increasing the security level of CPSS 03
PLATFORM 6 – FINANCIAL COSTS FOR THE IMPLEMENTATION OF ATTACK/IMPLEMENTATION OF PREVENTIVE MEASURES

Fig. 1. Structure of the threat classifier (expert evaluation)

At the second stage, using the proposed expressions, the probabilities of the implementation of threats, the possibility of their synergistic and/or hybrid impact on infrastructure elements are calculated. This approach significantly simplifies the classification of security metrics, and allows the average person to intuitively use it in practice. The classifier consists of 6 platforms.

The first platform defines security metrics as critical, high, medium, low, very low. The second platform considers the metrics for assessing the provision of security services, taking into account the security component: cybersecurity (CS), information security (IS), security of information (SI). The third platform defines the metrics for evaluating the effectiveness of cyberattacks – complete destruction of the CPSS infrastructure (01), destruction of individual CPSS elements (02), complete blocking of the CPSS functionality (03), partial blocking of the functionality (04). The fourth platform is a functional view: additive, multiplicative, logarithmic. The fifth platform determines the direction of metrics in risk management, based on the assessment of the probability of failures (01), the probability of deviation from normal operation (02), the probability of abnormal operation (03).

The sixth platform allows you to determine the level of financial costs for the implementation of an attack/implementation of preventive measures. It is proposed to use the metrics for assessing the payback of CPSS preventive protection measures (01), the volume of investments in the creation/modification of the IPS (02), and increasing the level of CPSS security (03).

5. 2. Development of a stochastic model of the current security level of CPSS information assets (resources)

To form a stochastic model for assessing the security level of information assets, it is necessary to consider the implementation of all security services by the IPS: *C*, *I*, *A*, *Au*, *Aff* for all information resources CI_i, PD_i, CD_i, TS_i, StR_i, $PubI_i$, $ContI_i$, PI_i. To assess the hybrid and synergistic components of threats, we use the procedure in [12], which is determined by an expert. To verify the experts' assessment, we use the approach proposed in [12]. To form the threat coefficients (proposed in [1]), the values given in Table 4 were used:

$$\alpha_i^{CPSS}, i \in [0.067;\ 0.133;\ 0.2;\ 0.267;\ 0.333]. \qquad (15)$$

To determine the dependency of security services for information resources, we use the results in Table 5 [49], where K_1 is the confidentiality service, K_2 is the integrity service, K_3 is the authenticity service, K_4 is the availability service, and K_5 is the affiliation service.

Table 4

Selection of weighting factors α_i of manifestations of the ith vulnerability/threat depending on the conditions of their manifestation

Weighting factor, α_i	Vulnerability/attack manifestation conditions
0.067	occurs no more than once every 5 years
0.133	occurs no more than once a year
0.2	occurs no more than once a month
0.267	occurs no more than once a week
0.333	occurs daily

Table 5

Preference analysis of five criteria by the floating preference method

Security service	K_1	K_2	K_3	K_4	K_5	C_i	s_i
K_1	1	2	3	4	5	2.605	0.417
K_2	1/2	1	2	3	4	1.644	0.263
K_3	1/3	1/2	1	2	3	1	0.160
K_4	1/4	1/3	1/2	1	2	0.608	0.098
K_5	1/5	1/4	1/3	1/2	1	0.384	0.062

To take into account the secrecy level of information resources (CI_i, PD_i, CD_i, TS_i, StR_i, $PubI_i$, $ContI_i$, PI_i), we use the indicators β_i presented in Table 6.

Table 6

Ratio of time and degree of information secrecy

Degree of information secrecy	Time
critical	up to 1 year
high	up to 1 month
medium	up to 1 hour
low	up to 10 minutes
very low	up to 1 minute

Table 7 shows the secrecy levels of the main elements of information assets.

Table 7

Ratio of time and degree of secrecy of information assets

Information asset	Degree of information secrecy	Time	β_i
CI_i	critical	up to 1 year	1.0
PD_i	high	up to 1 month	0.75
CD_i	high	up to 1 month	0.75
TS_i	critical	up to 1 year	1.0
StR_i	medium	up to 1 hour	0.5
$PubI_i$	very low	up to 1 minute	0.25
$ContI_i$	low	up to 10 minutes	0.5
PI_i	critical	up to 1 year	1.0

Note: CI_i – confidential information, PD_i – payment documents, CD_i – credit documents, TS_i – trade secret, StR_i – statistical reports, $PubI_i$ – public information, $ContI_i$ – control information, PI_i – personal information

Table 8 shows the initial data of the criteria and indicators of expert evaluation, which corresponds to the proposed models: «Worst attacker» and «Blind attacker».

Table 8

Initial data of the criteria and indicators of expert evaluation of the weighting factor of the attacker's computing capabilities

Category	weighting factors						
	$P^{overall}_{hacking}$					P_{att}	T_{att}
	W_{att}	C_{att}	$E_{det\ att}$	$E_{decl\ att}$	C_{red}		
critical	1	0.001	1	0.001	0.001	1	0.001
high	0.75	0.25	0.75	0.25	0.25	0.75	0.25
medium	0.5	0.5	0.5	0.5	0.5	0.5	0.5
low	0.25	0.75	0.25	0.75	0.75	0.25	0.75
very low	0.001	1	0.001	1	1	0.001	1

Let CPSS, {N} and {Pr} be the sets of vulnerabilities/threats and elements of the protection system. $P_{\{N\}}(\{Pr\})$ is the probability of vulnerabilities/threats covered by the elements of the information security system (IPS), and $P^{unprotected}_{\{N\}}(\{\mathrm{Pr}\})$ is the probability of uncovered vulnerabilities/threats of the IPS based on (6) and (7).

The security matrix S is determined by formulas (8) and (9).

Therefore, an absolutely protected system is determined by formula (10). However, all security services are taken into account: C, I, A, Au, Aff.

Then the level of security (performance of security services: $A_i^C, A_i^I A_i^A, A_i^{Au}, A_i^{Inv}$) taking into account the secrecy of information resources (CI_i, PD_i, CD_i, TS_i, StR_i, $PubI_i$, $ContI_i$, PI_i) can be represented in a matrix form:

$$S_{att}^{\max} - S \otimes \beta_i = \\ = \begin{bmatrix} 1 - s_{11} \cdot \beta_1 & 1 - s_{12} \cdot \beta_2 & \dots & 1 - s_{1n} \cdot \beta_n \\ 1 - s_{21} \cdot \beta_1 & 1 - s_{22} \cdot \beta_2 & \dots & 1 - s_{2n} \cdot \beta_n \\ \dots & \dots & \dots & \dots \\ 1 - s_{m1} \cdot \beta_1 & 1 - s_{m2} \cdot \beta_2 & \dots & 1 - s_{mn} \cdot \beta_n \end{bmatrix}, \quad (16)$$

where ⊗ is the element-wise multiplication of the secrecy level metric of the information resource, β_i is the degree of information secrecy for the asset.

An estimate of the current state of CPSS security is then defined as:

$$\text{Security} = \left\| S_{att}^{\max} - S \otimes \beta_i \right\|_{Fn} = \\ = \sqrt{\frac{\sum_i \sum_j \left(1 - \left(s_{ij} \times \beta_i\right)^2\right)}{mn}} \times 100\,\%, \quad (17)$$

and the probability of penetration/hacking as:

$$\text{Insecurity} = \left(1 - \left\| S_{att}^{\max} - S \otimes \beta_i \right\|_{Fn}\right) \times 100\,\%. \quad (18)$$

Thus, the proposed approach makes it possible to dynamically assess the current state of the security level, taking into account the secrecy level of the information resource, as well as the absolute capabilities of an attacker with unlimited financial and computing resources.

Using the values obtained from Tables 5, 7, it is possible to form a matrix of resource security levels by type of service. The values of the matrix elements have the form where the row corresponds to the security service, and the column to the protected asset:

$$S_{att}^{\max} - S \otimes \beta =$$

$$= \begin{bmatrix} 0.8261 & 0.9022 & 0.9022 & 0.8261 & 0.9565 & 0.9891 & 0.9565 & 0.8261 \\ 0.9308 & 0.9611 & 0.9611 & 0.9308 & 0.9827 & 0.9957 & 0.9827 & 0.9308 \\ 0.9744 & 0.9856 & 0.9856 & 0.9744 & 0.9936 & 0.9984 & 0.9936 & 0.9744 \\ 0.9904 & 0.9946 & 0.9946 & 0.9904 & 0.9976 & 0.9994 & 0.9976 & 0.9904 \\ 0.9962 & 0.9978 & 0.9978 & 0.9962 & 0.9990 & 0.9998 & 0.9990 & 0.9962 \end{bmatrix}.$$

Performing calculations by formula (17), the value of *Insecurity* equal to 1.7 % is obtained. Accordingly, the *Security* value is 98.33 %.

The average value of the provision of security services for each asset is calculated by the formula:

$$P_{I_{A_j}}^{av.pr} = \sqrt{\frac{\sum_{i=1}^{7} \left(s_{ij} \cdot \beta_i \right)^2}{m}}. \qquad (19)$$

Table 9 shows the results of the average indicator of security service provision for each information asset at the corresponding secrecy level of the asset.

The average value of security service provision to CPSS information resources is calculated by the formula:

$$P_{A_i^C, A_i^I A_i^A, A_i^{Au}, A_i^{Inv}}^{av.pr} = \sqrt{\frac{\sum_{j=1}^{5} \left(s_{ij} \cdot \beta_i \right)^2}{n}}. \qquad (20)$$

Table 10 shows the results of the average indicator of security service provision to CPSS information resources at the corresponding secrecy level of the asset.

Table 9

Average indicator of security service provision for each information asset

Information asset	$P_{I_{A_j}}^{av.pr}$	Time	β_i
CI_i	0.94	up to 1 year	1.0
PD_i	0.97	up to 1 month	0.75
CD_i	0.97	up to 1 month	0.75
TS_i	0.94	up to 1 year	1.0
StR_i	0.99	up to 1 hour	0.5
$PubI_i$	1.0	up to 1 mimute	0.25
$ContI_i$	0.99	up to 10 minutes	0.5
PI_i	0.94	up to 1 year	1.0

Table 10

Average value of security service provision to CPSS information resources

Security service	$P_{A_i^C, A_i^I A_i^A, A_i^{Au}, A_i^{Inv}}^{av.pr}$	Time	β_i
A_i^C	0.96	up to 1 year	1.0
A_i^I	1.0	up to 1 month	0.75
A_i^A	1.0	up to 1 month	0.75
A_i^{Au}	1.0	up to 1 year	1.0
A_i^{Inv}	1.0	up to 1 hour	0.5

The results presented in Tables 9, 10 confirm the need for both strict accounting of information resources and definition of the «cost» (level of secrecy) of information resources. This approach minimizes the cost of preventive measures, forms an objective assessment of the current level of CPSS security, and also allows you to timely select a set of measures ensuring the required level of security.

Thus, the proposed approach allows combining various metrics in order to obtain an objective assessment of the current state of the CPSS security level, taking into account not only the computational and financial costs of an attacker to implement a targeted attack, but also the secrecy level of information resources. This minimizes the computational and economic costs of the defense side, as well as the set of preventive measures.

6. Discussion of the results of modeling the assessment of the current state of CPSS security

To evaluate the results of modeling the assessment of the current state of the security level, the indicators of the occurrence of targeted cyberattacks, proposed in [1, 2, 12], are used, taking into account their hybridity and synergy, the level of secrecy of information resources, as well as the classification of possible attackers. This approach takes into account the degree of provision of security services, as well as minimizes the cost of preventive measures.

The proposed model makes it possible to assess the current state of the security level based on the proposed stochastic model and the initial data presented in Tables 5–8. The data of Tables 5–8 can be used or pre-adjusted depending on the secrecy level of CPSS information resources, the choice of a set of security profiles, as well as synergism and hybridity of threats (attacker capabilities). In addition, this model allows you to evaluate not only the current security level, but also to obtain average values for the provision of security services for each CPSS information asset. Estimates can also be obtained for the average value of security provision to each service for the entire set of assets. The disadvantage of security metrics is the inability to take into account the rapid growth of computing resources of quantum computers. In addition, the emergence of a full-scale quantum computer will allow hacking symmetric and asymmetric algorithms based on Shor's and Grover's quantum algorithms, and a significant reduction in the security level of modern information security systems based on them.

Table 11 shows the results of a comparative assessment of various approaches to the current state of information security of critical infrastructure objects (automated banking systems). In [1, 12], the results of the assessment based on the CRAMM and FAIR metrics are presented, providing both a quantitative and qualitative assessment of the current security level of information resources. The analysis of Table 11 showed that the proposed approach based on the Concept allows the interested user to obtain an objective assessment of the security level of critical infrastructure elements. In addition, aspects of both the threats themselves (hybridity and synergy) and the secrecy level of information resources are taken into account. All this makes it possible to minimize the costs (financial and computational) of preventive protection measures.

Table 11

Comparison of approaches (metrics) for assessing the current state of information security of critical infrastructure facilities

Method	evaluation metrics					
	$P^{av.pr}_{A_i^C, A_i^I A_i^A, A_i^{Au}, A_i^{Inv}}$	costs		compliance with regulatory requirements	β_i	W_{att}
		$E^{\min}_{det\,att}$	C_{att}			
CRAMM	+/–	+/–	+/–	–	–	–
FAIR	+/–	+/–	+/–	–	–	–
Proposed approach	+	+	+	+	+	+

A promising area of research is the formation of security profiles on the basis of the proposed approach based on post-quantum algorithms – McEliece and Niederreiter crypto-code structures based on algebrogeometric codes and/or flawed codes of multifactorial cryptography. A description of the construction of crypto-code structures on these error-correcting codes is given in [1, 2]. Taking into account the set of metrics based on the proposed classifier, and the «cost» (the required level of secrecy), it is possible to build multi-loop security systems, which are considered in [2, 50]. Combining the two approaches provides, on the basis of the classifier, the choice of the necessary metrics, the objectivity of assessing the current state of the security level. And the multi-loop security system forms the required preventive protection measures at all levels (environments, technologies) of the CPSS.

7. Conclusions

1. The initial model of the formal description and analysis of security metrics is presented. First of all, it is shown that in measurement theory, the term «metric» has a different meaning (distance) than that commonly used in the security community. A number of security metrics that can be found in the literature were formalized and evaluated by very simple empirical criteria. We also investigated relationships between the metrics and found that in the strict sense, all metrics are independent, but there are some correlations between them. It is shown that there is no strict definition of the concept of «more secure» and, therefore, there is no indicator that is good (or bad) for measuring security. Thus, security metrics should be used depending on the entity that requires a security assessment, i.e. the stakeholder. It is concluded that the metric must be formed not only depending on the attacker's model, but also take into account the synergy and hybridity of modern targeted threats and the computing capabilities of all parties to the cyber conflict. The metric should also be applicable to minimize the economic and energy components of the conflict.

2. The proposed stochastic model for assessing the current state allows for the objectivity and efficiency of obtaining information. In addition, it allows you to determine the level of provision of security services to various information assets, as well as assess the security of information resources, taking into account an individual security service. This approach makes it possible to take into account the level of secrecy (required security time) for various assets, as well as to form not only a set of security metrics to assess the current state, but also security profiles, taking into account the security of continuous business processes. The average value of the provision of security services to CPSS information resources is 0.99, with an average value of the security level of information resources of 0.8.

Conflict of interest

The authors declare that they have no conflict of interest in relation to this research, whether financial, personal, authorship or otherwise, that could affect the research and its results presented in this paper.

References

1. Yevseiev, S., Ponomarenko, V., Laptiev, O., Milov, O., Korol, O., Milevskyi, S. et. al.; Yevseiev, S., Ponomarenko, V., Laptiev, O., Milov, O. (Eds.) (2021). Synergy of building cybersecurity systems. Kharkiv: PC TECHNOLOGY CENTER, 188. doi: https://doi.org/10.15587/978-617-7319-31-2
2. Yevseiev, S., Pohasii, S., Milevskyi, S., Milov, O., Melenti, Y., Grod, I. et. al. (2021). Development of a method for assessing the security of cyber-physical systems based on the Lotka–Volterra model. Eastern-European Journal of Enterprise Technologies, 5 (9 (113)), 30–47. doi: https://doi.org/10.15587/1729-4061.2021.241638
3. INFOSEC Research Council. Hard Problem List (2005). Available at: https://www.infosec-research.org/docs_public/20051130-IRC-HPL-FINAL.pdf
4. A Roadmap for Cybersecurity Research (2009). Homeland Security. Available at: https://www.dhs.gov/sites/default/files/publications/CSD-DHS-Cybersecurity-Roadmap_0.pdf
5. ISO/IEC 27001:2005. Information technology – Security techniques – Information security management systems – Requirements. Available at: https://www.iso.org/standard/42103.html
6. ISO/IEC 27002:2005. Information technology – Security techniques – Code of practice for information security management. Available at: https://www.iso.org/standard/50297.html
7. Control Objectives for Information and related Technology (COBIT) 5 (2012). IT Governance Institute. Illinois.
8. Recommended Security Controls for Federal Information Systems and Organizations. NIST Special Publication 800-53 Revision 3. NIST. doi: https://doi.org/10.6028/nist.sp.800-53r3
9. ISO/IEC 27004:2009. Information technology – Security techniques – Information security management – Measurement. Available at: https://www.iso.org/standard/42106.html

10. Chew, E., Swanson, M., Stine, K. M., Bartol, N., Brown, A., Robinson, W. (2008). Performance measurement guide for information security. NIST. doi: https://doi.org/10.6028/nist.sp.800-55r1
11. Hayden, L. (2010). IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data. McGraw-Hill, 396.
12. Yevseiev, S., Melenti, Y., Voitko, O., Hrebeniuk, V., Korchenko, A., Mykus, S. et. al. (2021). Development of a concept for building a critical infrastructure facilities security system. Eastern-European Journal of Enterprise Technologies, 3 (9 (111)), 63–83. doi: https://doi.org/10.15587/1729-4061.2021.233533
13. Yevseiev, S., Laptiev, O., Lazarenko, S., Korchenko, A., Manzhul, I. (2021). Modeling the protection of personal data from trust and the amount of information on social networks. EUREKA: Physics and Engineering, 1, 24–31. doi: https://doi.org/10.21303/2461-4262.2021.001615
14. Yevseiev, S., Katsalap, V., Mikhieiev, Y., Savchuk, V., Pribyliev, Y., Milov, O. et. al. (2022). Development of a method for determining the indicators of manipulation based on morphological synthesis. Eastern-European Journal of Enterprise Technologies, 3 (9 (117)), 22–35. doi: https://doi.org/10.15587/1729-4061.2022.258675
15. Agyepong, E., Cherdantseva, Y., Reinecke, P., Burnap, P. (2019). Challenges and performance metrics for security operations center analysts: a systematic review. Journal of Cyber Security Technology, 4 (3), 125–152. doi: https://doi.org/10.1080/23742917.2019.1698178
16. Yee, G. (2012). The state and scientific basis of cyber security metrics. Including Canadian perspectives. Contract Report, DRDC Ottawa CR 2012-109. Available at: https://silo.tips/download/the-state-and-scientific-basis-of-cyber-security-metrics
17. Stolfo, S., Bellovin, S. M., Evans, D. (2011). Measuring Security. IEEE Security & Privacy Magazine, 9 (3), 60–65. doi: https://doi.org/10.1109/msp.2011.56
18. Ahmed, R. K. A. (2016). Overview of Security Metrics. Software Engineering, 4 (4), 59–64. Available at: https://www.researchgate.net/publication/311884003_Overview_of_Security_Metrics
19. Perpetus, J., Houngbo, P. J., Hounsou, J. T. (2015). Measuring Information Security: Understanding And Selecting Appropriate Metrics. International Journal of Computer Science and Security (IJCSS), 9 (2). Available at: https://www.researchgate.net/publication/281648626_Measuring_Information_Security_Understanding_And_Selecting_Appropriate_Metrics
20. Haque, M. A., Shetty, S., Krishnappa, B. (2019). Cyber-Physical System Resilience. Complexity Challenges in Cyber Physical Systems, 301–337. doi: https://doi.org/10.1002/9781119552482.ch12
21. Abbas Ahmed, R. K. (2016). Security Metrics and the Risks: An Overview. International Journal of Computer Trends and Technology, 41 (2), 106–112. doi: https://doi.org/10.14445/22312803/ijctt-v41p119
22. Jaquith, A. (2007). Security Metrics: Replacing Fear, Uncertainty, and Doubt. Addison-Wesley Professional.
23. Moshtari, S., Okutan, A., Mirakhorli, M. (2022). A grounded theory based approach to characterize software attack surfaces. Proceedings of the 44th International Conference on Software Engineering. doi: https://doi.org/10.1145/3510003.3510210
24. Munaiah, N., Meneely, A. (2016). Beyond the Attack Surface. Proceedings of the 2016 ACM Workshop on Software PROtection. doi: https://doi.org/10.1145/2995306.2995311
25. Lallie, H. S., Debattista, K., Bal, J. (2020). A review of attack graph and attack tree visual syntax in cyber security. Computer Science Review, 35, 100219. doi: https://doi.org/10.1016/j.cosrev.2019.100219
26. Noel, S., Wang, L., Singhal, A., Jajodia, S. (2010). Measuring security risk of networks using attack graphs. International Journal of Next-Generation Computing, 1 (1). Available at: https://www.researchgate.net/publication/220202986_Measuring_Security_Risk_of_Networks_Using_Attack_Graphs
27. Hou, S., Chen, X., Ma, J., Zhou, Z., Yu, H. (2022). An Ontology-Based Dynamic Attack Graph Generation Approach for the Internet of Vehicles. Frontiers in Energy Research, 10. doi: https://doi.org/10.3389/fenrg.2022.928919
28. Wang, L., Islam, T., Long, T., Singhal, A., Jajodia, S. (2008). An Attack Graph-Based Probabilistic Security Metric. Data and Applications Security XXII, 283–296. doi: https://doi.org/10.1007/978-3-540-70567-3_22
29. Żebrowski, P., Couce-Vieira, A., Mancuso, A. (2022). A Bayesian Framework for the Analysis and Optimal Mitigation of Cyber Threats to Cyber-Physical Systems. Risk Analysis. doi: https://doi.org/10.1111/risa.13900
30. Frigault, M., Wang, L. (008). Measuring Network Security Using Bayesian Network-Based Attack Graphs. 2008 32nd Annual IEEE International Computer Software and Applications Conference. doi: https://doi.org/10.1109/compsac.2008.88
31. Krautsevich, L., Martinelli, F., Yautsiukhin, A. (2010). Formal approach to security metrics. Proceedings of the Fourth European Conference on Software Architecture Companion Volume - ECSA '10. doi: https://doi.org/10.1145/1842752.1842787
32. Agyepong, E., Cherdantseva, Y., Reinecke, P., Burnap, P. (2020). Towards a Framework for Measuring the Performance of a Security Operations Center Analyst. 2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security). doi: https://doi.org/10.1109/cybersecurity49315.2020.9138872
33. Halonen, P., Hätönen, K. (2010). Towards holistic security management through coherent measuring. Proceedings of the Fourth European Conference on Software Architecture Companion Volume – ECSA'10. doi: https://doi.org/10.1145/1842752.1842786
34. Mellado, D., Fernández-Medina, E., Piattini, M. (2010). A comparison of software design security metrics. Proceedings of the Fourth European Conference on Software Architecture Companion Volume – ECSA'10. doi: https://doi.org/10.1145/1842752.1842797

35. Kevin N'DA, A. A., Matalonga, S., Dahal, K. (2021). Applicability of the Software Security Code Metrics for Ethereum Smart Contract. The International Conference on Deep Learning, Big Data and Blockchain (Deep-BDB 2021), 106–119. doi: https://doi.org/10.1007/978-3-030-84337-3_9
36. Bosire, A., Kimwele, M. (2015). Advances in Measuring and Preventing Software Security Weaknesses. International Journal of Advanced Research in Computer Science and Software Engineering. 5 (12). Available at: https://www.researchgate.net/publication/338402728_Advances_in_Measuring_and_Preventing_Software_Security_Weaknesses
37. Liu, Y., Traore, I., Hoole, A. M. (2008). A Service-Oriented Framework for Quantitative Security Analysis of Software Architectures. 2008 IEEE Asia-Pacific Services Computing Conference. doi: https://doi.org/10.1109/apscc.2008.17
38. Hariprasad, T., Vidhyagaran, G., Seenu, K., Thirumalai, C. (2017). Software complexity analysis using halstead metrics. 2017 International Conference on Trends in Electronics and Informatics (ICEI). doi: https://doi.org/10.1109/icoei.2017.8300883
39. Liu, Y., Traore, I. (2004). UML-based Security Measures of Software Products. Proceedings of International Workshop on Methodologies for Pervasive and Embedded Software (MOMPES'04).
40. Wang, L., Jajodia, S., Singhal, A., Noel, S. (2010). k-Zero Day Safety: Measuring the Security Risk of Networks against Unknown Attacks. Lecture Notes in Computer Science, 573–587. doi: https://doi.org/10.1007/978-3-642-15497-3_35
41. SP 800-55 Rev. 2 (2020). PRE-DRAFT Call for Comments: Performance Measurement Guide for Information Security. Available at: https://csrc.nist.gov/publications/detail/sp/800-55/rev-2/draft
42. Bernik, I., Prislan, K. (2016). Measuring Information Security Performance with 10 by 10 Model for Holistic State Evaluation. PLOS ONE, 11 (9), e0163050. doi: https://doi.org/10.1371/journal.pone.0163050
43. Hernandez-Ramos, J. L., Matheu, S. N., Skarmeta, A. (2021). The Challenges of Software Cybersecurity Certification [Building Security In]. IEEE Security & Privacy, 19 (1), 99–102. doi: https://doi.org/10.1109/msec.2020.3037845
44. Talbot, J., Jakeman, M. (2009). Security Risk Management. Wiley. doi: https://doi.org/10.1002/9780470494974
45. Phipps, J. (2022). IT Risk Management Guide for 2022. Available at: https://www.cioinsight.com/it-management/it-risk-management/
46. Lentz, R. F. (2010). Advanced Persistent Threats & Zero Day Attacks. Slide Presentation.
47. Lentz, R. F. (2011). Cyber Security Maturity Model. Slide Presentation.
48. Mohammad, S. M. (2020). Risk Management in Information Technology. SSRN Electronic Journal. doi: https://doi.org/10.2139/ssrn.3625242
49. Postnikov, V., Spiridonov, S. (2015). Selecting Methods of the Weighting Factors of Local Criteria. Science and Education of the Bauman MSTU. doi: https://doi.org/10.7463/0615.0780334
50. Yevseiev, S., Milevskyi, S., Bortnik, L., Alexey, V., Bondarenko, K., Pohasii, S. (2022). Socio-Cyber-Physical Systems Security Concept. 2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA). doi: https://doi.org/10.1109/hora55278.2022.9799957