http://doi.org/10.35784/iapgos.7555

received: 10.04.2025 | revised: 23.09.2025 | accepted: 18.11.2025 | available online: 20.12.2025

THE MATHEMATICAL METHOD FOR ASSESSING THE CYBERSECURITY STATE OF CLOUD SERVICES

Yevheniia Ivanchenko[1], Volodymyr Shulha[2], Ihor Ivanchenko[1], Yevhenii Pedchenko[1], Mari Petrovska[3]

[1]State University of Information and Communication Technologies, Educational and Scientific Institute of Cybersecurity and Information Protection, Kyiv, Ukraine, [2]State University of Information and Communication Technologies, Kyiv, Ukraine, [3]State Non-Commercial Company State University "Kyiv Aviation Institute", Technical Information Protection Department, Kyiv, Ukraine

Abstract. *This study presents the developed mathematical method for assessing the cybersecurity state of cloud services of information infrastructure facilities. The developed assessment method consists of 11 assessment stages, which provide a comprehensive assessment of 5 types of cloud services. The developed approach to assessing the cybersecurity state of cloud services can become the basis for further research in the field of cybersecurity by expanding tools for analyzing risks in the cloud environment and will help increase confidence in the use of cloud services in the face of modern information challenges.*

Keywords: cybersecurity, cloud security, scoring metric, decision coefficient, risk assessment, container security

MATEMATYCZNA METODA OCENY STANU CYBERBEZPIECZEŃSTWA USŁUG CHMUROWYCH

Streszczenie. *Niniejszy artykuł przedstawia opracowaną metodę matematyczną do oceny stanu cyberbezpieczeństwa usług chmurowych obiektów infrastruktury informacyjnej. Opracowana metoda oceny składa się z 11 etapów, które zapewniają kompleksową ocenę 5 typów usług w chmurze. Opracowane podejście do oceny stanu cyberbezpieczeństwa usług chmurowych może stać się podstawą dla dalszych badań w dziedzinie cyberbezpieczeństwa poprzez rozszerzenie narzędzi do analizy ryzyk w środowisku chmurowym i pomoże zwiększyć zaufanie do korzystania z usług chmurowych w obliczu współczesnych wyzwań informacyjnych.*

Słowa kluczowe: cyberbezpieczeństwo, bezpieczeństwo w chmurze, metryka punktacji, współczynnik decyzyjny, ocena ryzyka, bezpieczeństwo kontenerów

Introduction

Assessing the security of cloud service providers is a critical aspect for any organization that is planning or has already migrated its information assets to cloud computing. Despite the significant advantages of cloud computing, such as scalability, flexibility, and cost optimization, a lack of full understanding of the cloud service's cybersecurity can pose significant risks to the confidentiality, integrity, and availability of company data.

According to analytical reports of the world's leading cybersecurity companies, including Proofpoint [2], CrowdStrike [1], and Check Point [12], ensuring the security of cloud services is one of the main challenges for modern enterprises. The use of cloud services not only changes the traditional approach to risk management, but also creates new threats related to unauthorized access, data leaks, breaches of security configurations, and exploitation of vulnerabilities in the provider's services. These companies outline the main problems related to the security of cloud services:

- Incorrect configuration of security systems, which can lead to leakage of business data beyond the cloud service resources.
- Possibility of unauthorized access to environments deployed on the resources of cloud service providers that are connected to the Internet due to the lack of proper security systems, access control, compromised credentials, or incorrect settings.
- Insufficient protection of APIs, which allows CLI requests to be performed to configure cloud services without the need to enter a token or login and password, giving an attacker full control over the services.

Lack of protection systems against cyberattacks, which allows attackers to make successful requests to cloud services and interfere with business processes.

In this case, security vendors only describe the security problems faced by businesses using cloud service providers but do not provide an opportunity to audit the security systems of such services as IaaS, CaaS, PaaS, FaaS, and SaaS.

1. Purpose and objectives of the study

The main purpose of this study is to develop a mathematical method for assessing the cybersecurity state of cloud services of information infrastructure facilities based on the described model for evaluating cloud services.

To achieve this goal, it is necessary to develop an evaluation system based on 120 questions with various answer options and recommendations for improving the security of cloud services for information infrastructure. The proposed method for assessing the cybersecurity state of cloud services will allow an objective and comprehensive determination of the level of security by calculating the appropriate number of points when answering questions for each parameter being assessed. In addition, this method will provide a differentiated scoring scale depending on the characteristics of different types of cloud services, which will ensure the accuracy and completeness of the assessment by auditors [9].

2. Description of the developed mathematical method

The developed method for assessing the cybersecurity state of cloud services is based on a structured list of questions included in the assessment model, which is the main one for determining the level of criticality of each of the assessed cloud services. This model is the basis for building an assessment system that makes it possible to obtain of the security and safety of cloud environments.

The method of assessing the cybersecurity state of cloud services involves the use of a scale of points ranging from 0 to 5, where 5 is the maximum point, indicating the highest level of security, and 0 is the minimum point, indicating the absence of the necessary protection measures. This scale allows for a clearly define the level of security for each parameter being evaluated and is easy for the auditor to navigate after completing the evaluation of the cloud service modules.

To conduct an effective assessment, we have identified 10 key stages that are key to evaluating cloud services. These stages include:

- Description of general information about the cloud service.
- Network maintenance.
- Data storage.
- Maintenance of server hardware.
- Maintenance of the virtualization system (VS).
- Operation system (OS) maintenance.
- Container management.
- Service continuity.
- Application management.
- Data processing.

The above stages form the basis for assessing the cybersecurity state of cloud services and allow determination the level of security of each of the modules of the cloud service under assessment.

In addition, the developed mathematical method for assessing the cybersecurity state of cloud services will be used to evaluate different types of cloud services, namely:

- IaaS (Infrastructure-as-a-Service).
- CaaS (Container-as-a-Service).
- PaaS (Platform-as-a-Service).
- FaaS (Function-as-a-Service).
- SaaS (Software-as-a-Service) [10].

The types of cloud services described above require different approaches to assessing the state of cybersecurity, as they have their specific characteristics and risks that affect their security and are differently affected by automation and human factors on the configuration and implementation of security systems. The proposed assessment system can effectively determine the level of security of each of these types of services and ensure their compliance with modern cybersecurity requirements.

2.1. Modules of the developed mathematical method

The developed mathematical method for assessing the cybersecurity state of cloud services is based on 11 developed assessment parameters. These assessment parameters include one parameter responsible for collecting general information about the assessed cloud service, nine assessment parameters responsible for directly assessing the cybersecurity state of cloud services, and one assessment parameter that provides a list of recommendations for each of the answer options provided by the auditor. These 11 assessment parameters are summarized as follows:

- ***CSP_1 = GP = "General Points module"*** is a module to obtain a description of the general terms and conditions of the cloud service provider. This module applies to such types of cloud services as IaaS, CaaS, PaaS, FaaS, and SaaS.
- ***CSP_2 = N = "Network module"*** is a module for assessing the level of security of the cloud service provider's network. This module applies to such types of cloud services as IaaS, CaaS, PaaS, FaaS, and SaaS.
- ***CSP_3 = S = "Storage module"*** is a module for assessing the security level of drives (HDD/SSD/M2, etc.). This module applies to such types of cloud services as IaaS, CaaS, PaaS, FaaS, and SaaS.
- ***CSP_4 = SR = "Server module"*** is a module for assessing the security of server hardware. This module applies to such types of cloud services as IaaS, CaaS, PaaS, FaaS, and SaaS.
- ***CSP_5 = V = "Virtualization module"*** is a module for assessing the virtualization environment used. This module applies to such types of cloud services as IaaS, CaaS, PaaS, FaaS, and SaaS.
- ***CSP_6 = OS = "Operation System module"*** is a module for assessing the security of OSs used. This module applies to such types of cloud services as CaaS, PaaS etc.
- ***CSP_7 = CT = "Container Technology module"*** is a module for assessing the security of container management software. This module applies to the following types of cloud services: CaaS, PaaS, FaaS, and SaaS.
- ***CSP_8 = R = "Runtime module"*** is a module for evaluating monitoring systems to detect anomalies, vulnerabilities, system events, etc. This module applies to such types of cloud services as PaaS, FaaS, and SaaS.
- ***CSP_9 = A = "Application module"*** is a module for assessing the security of software supplied to customers. This module applies to the following types of cloud services FaaS, and SaaS.
- ***CSP_{10} = D = "Data module"*** is a module for assessing the level of security of data processed by the cloud service provider's systems. This module applies only to the type of cloud service SaaS.
- ***CSP_{11} = RE = "Recommendations' module"*** generates recommendations on all possible options for choosing an auditor. This module applies to such types of cloud services as IaaS, CaaS, PaaS, FaaS, and SaaS [9].

To understand how the above 11 evaluation parameters will be applied to the 5 types of cloud services, it is necessary to look at Table 1, which will show which evaluation parameter will be applied to each of the cloud services.

Table 1. Dependency parameters for modules and types of cloud services

No.	Parameters	IaaS	CaaS	PaaS	FaaS	SaaS
1	*CSP_1 = GP = "General Points module"*	✓	✓	✓	✓	✓
2	*CSP_2 = N = "Network module"*	✓	✓	✓	✓	✓
3	*CSP_3 = S = "Storage module"*	✓	✓	✓	✓	✓
4	*CSP_4 = SR = "Server module"*	✓	✓	✓	✓	✓
5	*CSP_5 = V = "Virtualization module"*	✓	✓	✓	✓	✓
6	*CSP_6 = OS = "Operation System module"*	✗	✓	✓	✓	✓
7	*CSP_7 = CT = "Container Technology module"*	✗	✓	✓	✓	✓
8	*CSP_8 = R = "Runtime module"*	✗	✗	✓	✓	✓
9	*CSP_9 = A = "Application module"*	✗	✗	✗	✓	✓
10	*CSP_{10} = D = "Data module"*	✗	✗	✗	✗	✓
11	*CSP_{11} = RE = "Recommendations' module"*	✓	✓	✓	✓	✓

2.2. Comparative analysis of the developed mathematical method

The developed method will be compared against such standards as HIPAA, PCI-DSS, SOC 2, ISO 27001, NIST 800-145, and GDPR. To detailed comparison, information on each of these standards is provided below in relation to the cloud service modules specified in Section 2.1., with the overall comparison presented in Table 2:

- HIPAA: Assesses – General, Network, Storage, Server, Operation, Container, Application, and Data modules through the requirements for the protection of Protected Health Information (PHI), including encryption and access control. It does not cover Virtualization, Technology, Runtime, and Recommendation, since these aspects are not prioritized within specific healthcare standards and do not require detailed regulation [4].
- PCI-DSS: Assesses – General, Network, Storage, Server, Operation, Container, Application, and Data modules in accordance with payment card data protection standards, focusing on encryption and monitoring. It does not cover

Virtualization, Technology, Runtime, and Recommendation, as these modules are less significant for ensuring transaction security and are not central to the standard [8].
- SOC-2: Assesses – General, Network, Storage, Server, Virtualization, Operation, and Application modules based on trust principles (security, availability), including infrastructure and operational controls. It does not cover Container, Technology, Runtime, Data, and Recommendation, as these aspects are less relevant for evaluating the effectiveness of trust systems [11].
- ISO/IEC 27001: Assesses – General, Network, Storage, Server, Virtualization, Container, Technology, Runtime, Application, and Data modules through the Information Security Management System (ISMS) and risk management framework, encompassing encryption and auditing. It does not cover Operation and Recommendation, as the standard is focused on strategic management rather than detailed operational processes or recommendations [5].
- NIST 800-145: Assesses – Server, Virtualization, Container, and Technology modules through the definitions of cloud service models, which serve as a foundation for adapting controls. It does not cover General, Network, Storage, Operation, Runtime, Application, Data, and Recommendation, since the standard does not specify detailed requirements for these modules, leaving them to other NIST frameworks [8].
- GDPR: Assesses – General, Network, Storage, Server, Virtualization, Operation, Application, Data, and Technology modules in terms of personal data protection, including encryption and Data Protection Impact Assessments (DPIA). It does not cover Container, Runtime, and Recommendation, as these modules are of lower priority for ensuring data subject rights and compliance [3].

Table 2. Comparison of the developed modules with standards

Parameters	HIPPA	PCI-DSS	SOC-2	ISO 27001	NIST 800-145	GDPR
"General Poinxts module"	✓	✓	✓	✓	✓	✓
"Network module"	✓	✓	✓	✓	✗	✓
"Storage module"	✓	✓	✓	✓	✗	✓
"Server module"	✓	✓	✓	✓	✓	✓
"Virtualization module"	✗	✗	✗	✓	✓	✓
"Operation System module"	✓	✓	✓	✗	✗	✗
"Container Technology module"	✗	✗	✗	✓	✓	✓
"Runtime module"	✗	✗	✗	✓	✓	✗
"Application module"	✓	✓	✓	✓	✗	✓
"Data module"	✓	✓	✗	✓	✗	✓
"Recommendations' module"	✗	✗	✗	✗	✗	✗

2.3. Stages of the developed mathematical method

Stage 1 – obtaining general information about the cloud service being evaluated.

At this stage, the **GP** parameter is filled in, which contains the data entered by the client before the assessment begins. This parameter is not used at the first stage of the assessment as it only has an informative function. For example, the data that the auditor enters as part of this stage may include the type of SaaS cloud service called "Cloud Service" and the determination that this service does not cooperate with aggressor countries.

Stage 2 – assessing the cybersecurity of the network maintenance module.

At this stage, the values of the **N** parameter are used to assess the security status of the network module, which includes checking the system for resistance to DDoS attacks, analyzing network bandwidth, and other aspects.

Stage 3 – assessing the cybersecurity of the storage module.

At this stage, the values of the **S** parameter are used to assess the security status of the storage module for data processed on the cloud service. The possibility of data recovery, the stability of data arrays, and other aspects are assessed.

Stage 4 – assessing the cybersecurity of the server hardware maintenance module.

At this stage, the values of the **SR** parameter are used to assess the security status of the cloud hardware service module that processes data on the cloud service. The system's ability to counteract physical attacks on the equipment and other possible threats is assessed.

Stage 5 – assessing the cybersecurity of the VS maintenance module.

At this stage, the values of the **V** parameter are used to assess the security status of the module for ensuring the functioning of the cloud provider's virtual environment. The VS used, its level of security, and other critical aspects are assessed.

Stage 6 – assessing the cybersecurity of the OS.

At this stage, the values of the **OS** parameter are used to assess the security status of the module to ensure the functioning of the OSs used. The selected OS is evaluated for its security level.

Stage 7 – assessing the cybersecurity of the container management module.

At this stage, the values of the **CT** parameter are used to assess the security status of the containerization environment management module. The security of all deployed containers running on the cloud provider's resources is assessed.

Stage 8 – assessing the cybersecurity of the service continuity module.

At this stage, the values of the **R** parameter are used to assess the security status of the cloud provider's service continuity module. The goal is to ensure the maximum availability of these services.

Stage 9 – assessing the cybersecurity of the application management module.

At this stage, the values of parameter **A** are used to assess the security status of the security module of the deployed application as a service on the resources of the cloud provider. The goal is to assess the security status of the proposed application and its ability to counteract cyber attacks.

Stage 10 – assessing the cybersecurity of the data processing module.

At this stage, the values of the **D** parameter are used to assess the security status of the company's data processing module on the cloud provider's resources. The goal is to identify potential sources of information leakage and determine the need to eliminate them.

Stage 11 – calculation of the evaluation results.

To perform the calculations for the 11 evaluation steps described above, the maximum number of scores for each of the evaluation parameters described in Table 3 is determined.

Table 3. Maximum scores for all assessment parameters

No.	Parameters	Maximum scores
1	CSP1 = GP	0
2	CSP2 = N	110
3	CSP3 = S	95
4	CSP4 = SR	60
5	CSP5 = V	65
6	CSP6 = OS	60
7	CSP7 = CT	50
8	CSP8 = R	65
9	CSP9 = A	50
10	CSP10 = D	60
Summary:		615 scores

The maximum score of 615 points will only be applied when all 10 evaluation parameters are applied to the evaluated cloud service. However, the following is a list of cloud service types and their respective scores:

- for IaaS – 330 scores,
- for CaaS – 440 scores,
- for PaaS – 505 scores,
- for FaaS – 555 scores,
- for SaaS – 615 scores.

A new parameter, ***CSP***$\boldsymbol{CSP_i}$, will be used to calculate the total number of points, which will contain the sum of all scores. That is why the calculation of this parameter will be based on formula (1), which will add all the identifiers:

$$\sum_{i=1}^{10} CSP_i = CSP_1 + CSP_2 + CSP_3 + CSP_4 + CSP_5 +$$

$$+ CSP_6 + CSP_7 + CSP_8 + CSP_9 + CSP_{10} = \qquad (1)$$

$$\mathbf{GP} + \mathbf{N} + \mathbf{S} + \mathbf{SR} + \mathbf{V} + \mathbf{OS} + \mathbf{CT} + \mathbf{R} + \mathbf{A} + \mathbf{D}$$

where: $CSP_i \subseteq CSP \quad (i = \overline{1,10})$ – the sum of all calculated identifier scores obtained based on the auditor's responses during the assessment of the state of cybersecurity of cloud services of information infrastructure facilities.

At this stage, the final calculation of the assessment results of the cloud service assessment modules is performed and calculated by the formula (2):

$$CC = \frac{\sum_{i=1}^{10} CSP_i}{< CSP\ type\ selected >} \cdot 100\% \qquad (2)$$

where: CC – cybersecurity coefficient of cloud services; $\sum_{i=1}^{10} CSP_i$ – the sum of all calculated points for each evaluation parameter; $< CSP\ type\ selected >$ – substituting the maximum number of points that each type of cloud service can potentially receive.

Based on the results of all 11 stages of the assessment, a new variable called RC is introduced to calculate the cloud service cybersecurity coefficient, which will provide an understanding for both the system and the user of whether the cloud service is recommended for use or not. As a result, after completing the assessment of the cloud service cybersecurity, the auditor is provided with one of the following recommendations:

- "Recommended for use (**Recommended**)" – the cloud service is fully recommended for the use and deployment of the company's business services and applications. This applies if the value of the CC variable is from 76% to 100%.
- "Maybe for use (**Maybe**)" – the cloud service can be used to deploy business services and applications, but it is recommended to review the security of the solution used. This applies if the value of the CC variable is from 26% to 75%.
- "Don`t recommend for use (**No Recommended**)" – the cloud service is not recommended for deploying the company's business services and applications, as it has a low level of security, both for its infrastructure and for the resources used by the customer. This applies if the value of the CC variable is from 0% to 25% [9].

In the context of each tuple parameter, the above results of the criterion evaluation will be presented by Table 4, which will allow to determine the weight of each of the evaluation parameters, leveling the influence of the subjective opinion of any of the auditors or errors in providing answers during the evaluation.

In the context of each type of cloud service, the above-described results of the criterion assessment will be set out by Table 5, which will allow to determine the number of points scored by type of cloud service, leveling the influence of the subjective opinion of any of the auditors or errors in providing answers during the assessment for each of the identified types of cloud services.

Table 4. Defining the value of the RC variable in terms of evaluation parameters

No.	Parameters	No Recommended	Maybe	Recommended
1	$CSP_1 = GP$	*0*	*0*	*0*
2	$CSP_2 = N$	*to 28 scores*	*29–83 scores*	*from 84 scores*
3	$CSP_3 = S$	*to 24 scores*	*25–72 scores*	*from 73 scores*
4	$CSP_4 = SR$	*to 15 scores*	*16–45 scores*	*from 46 scores*
5	$CSP_5 = V$	*to 16 scores*	*17–49 scores*	*from 50 scores*
6	$CSP_6 = OS$	*to 15 scores*	*16–45 scores*	*from 46 scores*
7	$CSP_7 = CT$	*to 13 scores*	*14–38 scores*	*from 39 scores*
8	$CSP_8 = R$	*to 16 scores*	*17–49 scores*	*from 50 scores*
9	$CSP_9 = A$	*to 13 marks*	*14–38 marks*	*from 39 marks*
10	$CSP_{10} = D$	*to 15 scores*	*16–45 scores*	*from 46 scores*

Table 5. Defining the value of the RC variable by type of cloud service

No.	Cloud Service	No Recommended	Maybe	Recommended
1	IaaS	to 83 scores	84–248 scores	from 249 scores
2	CaaS	to 110 scores	111–330 scoress	from 331 scores
3	PaaS	to 126 scores	127–379 scores	from 380 scores
4	FaaS	to 139 scores	140–416 scores	from 417 scores
5	SaaS	to 154 scores	155–461 scores	from 462 scores

3. Conclusion

This study presents a method based on a mathematical model, which is presented in [6], designed to mathematically calculate the assessment of the cybersecurity state of cloud services of information infrastructure facilities. To build the evaluation method, the results of the model development, the criteria for evaluating cloud services, and the answer options for which the number of points for each answer option was determined were used. The evaluation method consists of 11 stages, where the last one is the direct calculation of the criticality of the cloud service, which results in a recommendation to use/not use the cloud service. Due to the described method of assessing the cybersecurity of cloud services, the mathematical model of the study was finalized for implementation in the developed network application, which will be useful for auditors when assessing the security of the cloud service used in the customer company or before purchasing/using it.

References

[1] Baker K.: What is Cyber Espionage? Crowdstrike, 2025 [https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/cyber-espionage/].

[2] Cloud Security, Proofpoint, 2019 [https://www.proofpoint.com/us/threat-reference/cloud-security].

[3] GDPR. GDPR.EU. 2022 [https://gdpr.eu/].

[4] Health Information Privacy. U.S. Department of Health and Human Services, 2024 [https://www.hhs.gov/hipaa/index.html].

[5] ISO/IEC 27001:2022. ISO. 2022 [https://www.iso.org/standard/27001].

[6] Ivanchenko I., Pedchenko Y.: Secure web application model for cybersecurity assessment of cloud service providers. Scientific Notes of the State University of Information and Communication Technology 2, 2024, 116–134 [https://doi.org/10.31673/2518-7678.2024.025842].

[7] NIST SP 800–145. NIST: Computer Security Resource Center. 2011 [https://csrc.nist.gov/pubs/sp/800/145/final].

[8] PCI Data Security Standard (PCI DSS). PCI Security Standards Council, 2024 [https://www.pcisecuritystandards.org/standards/pci-dss/].

[9] Pedchenko Y. et al.: Mathematical model of security cloud services assessment, Problems of scientific, technical and legal support for cybersecurity in the modern world, 2024, 13–21 [https://doi.org/10.24917/9788668020861].

[10] Roger S.: IaaS vs. CaaS vs. PaaS vs. FaaS vs. SaaS –What's the difference?, Medium 2021 [https://stample.com/link/stamples/5ff3d43b60b2acfb9eb5ceb6/iaas-vs-caas-vs-paas-vs-faas-vs-saas-whats-the-difference].

[11] SOC2. SOC: System and Organization Controls. 2024 [https://soc2.co.uk/].

[12] Top 15 Cloud Security Issues, Threats and Concerns, Check Point, 2024 [https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/top-cloud-security-issues-threats-and-concerns/].

Prof. Yevheniia Ivanchenko
e-mail: e.ivanchenko@duikt.edu.ua

Doctor of Technical Sciences, professor, Laureate of the Borys Paton National Prize of Ukraine. She has been working as the Director of the Educational and Research Institute of Cybersecurity and Information Protection of the State University of Information and Communication Technologies since 2024. She is the author and co-author of 136 scientific and educational works, including 103 scientific works, 8 patents, 3 copyright certificates, and 21 educational works.
Research interests: cybersecurity, information security, cloud technologies, and methods and models for assessing the security of critical infrastructure facilities.

https://orcid.org/0000-0003-3017-5752

Prof. Volodymyr Shulha
e-mail: v.shulha@duikt.edu.ua

Doctor of History, senior researcher. He has been serving as the Rector of the State University of Information and Communication Technologies since 2024. He is the author and co-author of more than 50 scientific and educational works, 42 of which are scientific.
Research interests: cybersecurity, cyber attacks in cyberspace, cloud technologies, methods and models of organizing cyber defense systems in cyber diplomacy.

https://orcid.org/0000-0003-4356-7288

D.Sc. Ihor Ivanchenko
e-mail: igor-p-l@ukr.net

Candidate of Sciences in Technology. He works as an associate professor at the State University of Information and Communication Technologies. He has more than 50 published scientific works, including collective monographs, an encyclopedia, manuals, laboratory workshops, articles in national and international professional journals, teaching and methodological complexes of disciplines, materials and abstracts of conference reports, patents, and copyright certificates for computer programs.
Research interests: information and aviation security, access control methods and models, risk and security assessment, construction of integrated information security systems, cloud service security, and cybersecurity.

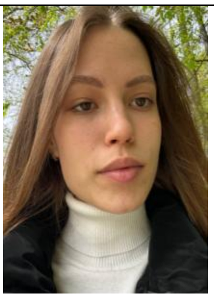
https://orcid.org/0000-0003-3415-9039

Ph.D. Yevhenii Pedchenko
e-mail: ympedchenko@gmail.com

He received a master's degree from the National Aviation University in 2021 and a Ph.D. in 2025. Since 2022, he has also been working at SITON GROUP LLC as Head of the Information Security Department. Starting from 2025, he has been working at the State University of Information and Communication Technologies. He is the author or co-author of 10 papers, 10 abstracts, 2 monographs, and 1 patent.
Research interests: cybersecurity, cloud security, nonlinear cybersecurity parameters, cyber threats, assessment.

https://orcid.org/0000-0001-8436-5792

Mari Petrovska
e-mail: pmarisha2004@gmail.com



She is a 4th-year bachelor's student majoring in Cybersecurity at the State Non-Profit Enterprise "State University" Kyiv Aviation Institute. She is interested in web programming with backend website development and sports. She is the author or co-author of 1 paper, 4 abstracts, and 2 monographs.
Research interests: cybersecurity, information security, websites, web programming, and cryptography.

https://orcid.org/0009-0005-2150-2194