

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
ODESA I.I. MECHNIKOV NATIONAL UNIVERSITY
Department of Computer Systems and Technologies



SYLLABUS OF THE ACADEMIC DISCIPLINE

«Cloud Technology Security»

Higher education level: **second (master's)**

Field of knowledge: **F – Information Technology**

Specialty: **F7 - Computer Engineering**

Specialization:

Educational and professional program: **Computer Engineering**

ONU
2026

Syllabus of the academic discipline "Cloud Technology Security". Odesa: ONU, 2026. – 16 p.

Developer: Larysa Yaroslavivna Martynovych, Senior Lecturer of the Department of Computer Systems and Technologies

The syllabus was approved at the department meeting

Protocol No. 1 dated «25» 08 2026 y

Head of the Department _____ (Yurii GUNCHENKO)
(signature) (Name SURNAME)

Agreed with the guarantor of the EPP/ESP

_____ (Yurii GUNCHENKO)
(signature)

Approved by the Educational and Methodological Commission (EMC) for IT specialties of the Faculty of Mathematics, Physics and Information Technologies

Protocol No. 1 dated «28» 08 2026 y

Head of the EMC _____ (Larysa MARTYNOVYCH)
(signature)

Reviewed and approved at the department meeting _____

Protocol No. ____ dated « ____ » _____ 20 ____ y

Head of the Department _____ (_____) (_____) (signature) (Name SURNAME)

Reviewed and approved at the department meeting _____

Protocol No. ____ dated « ____ » _____ 20 ____ y

Head of the Department _____ (_____) (_____) (signature) (Name SURNAME)

1. Description of the academic discipline

Name of indicators	Field of knowledge, specialty, specialization, higher education level	Characteristics of the academic discipline	
		<i>Full-time study</i>	<i>Part-time study</i>
Total amount: credits– 3 hours– 90 content modules – 2	Field of knowledge F – Information Technology Specialty F7 Computer Engineering EPP Computer Engineering Higher education level: Second (master's)	Elective	
		<i>Year of study:</i>	
		1-st	
		Semester	
		2-nd	
		Lectures	
		16 hours	hours
		Practical, seminars	
		14 hours	hours
		Laboratory	
		-	-
		Self-study	
		60 hours	hours
		Form of final control: pass/fail test	

2. Course Goals and Objectives

Goal of the Course: The goal of teaching this discipline is to study the principles, technologies, and tools related to the use of cloud services to ensure high availability, scalability, and efficiency of computing systems.

Objectives:

- Developing students' comprehensive knowledge of key cloud computing concepts and models;
- Studying the operating principles of cloud services and their capabilities;
- Studying cloud computing architecture and infrastructure that implements cloud security;
- Studying tools and technologies for deploying and managing cloud resources.

Upon completion of the course, the higher education student should:

Know:

- Key cloud services;
- Cloud infrastructure architecture and its components;
- * Fundamental cloud computing concepts and models;
- Operating principles of cloud services and their functional capabilities;
- Technologies for deploying and managing cloud resources;
- Major cloud computing security threats along with methods for their prevention and detection;

Be able to:

- Critically analyze the subject domain;
- Learn and master modern knowledge independently;
- Automate infrastructure management in cloud environments;
- Manage identity and access in the cloud;
- Utilize tools for providing network access to cloud resources;
- Apply available data encryption methods for data at rest and in transit;

Possess the competency to:

- Select effective models and methods for building, deploying, and managing cloud resources;
- Collect data on network activity and events;
- Solve complex problems related to access control for cloud resources;
- Automate infrastructure management across cloud environments;
- Provide varying levels of network access to cloud resources;
- Establish and maintain an appropriate level of cloud resource security.

Mastering this course enables students to acquire skills and competencies aimed at achieving the global Sustainable Development Goals (SDGs) through 2030, proclaimed by United Nations General Assembly Resolution No. 70/1 of September 25, 2015, and defined by Decree of the President of Ukraine No. 722 of September 30, 2019, specifically:

- **SDG 4: Quality Education** (*Ensure inclusive and equitable quality education and promote lifelong learning opportunities for all*)

The "Cloud Technology Security" course provides access to modern knowledge and technologies by facilitating the professional development of specialists in scientific research, experimentation, and academic inquiry. This promotes equal opportunities for learning and professional growth. Engaging in scientific and practical activities helps students acquire highly competitive skills.

- **SDG 8: Decent Work and Economic Growth** (*Promote sustained, inclusive and sustainable economic growth, full and productive employment and decent work for all*)

Knowledge and skills in critically analyzing the subject domain, conducting applied research, acquiring modern knowledge, and implementing cutting-edge data processing and security technologies are in high demand in the labor market. This fosters job creation in IT and high-tech sectors. Specialists equipped with these competencies can work across various industries, driving broader economic development.

- **SDG 9: Industry, Innovation and Infrastructure** (*Build resilient infrastructure, promote inclusive and sustainable industrialization and foster innovation*)

Applying knowledge in cloud deployment, implementation, and data security contributes to the efficient use of existing computing resources, data protection, and the development of various data storage and processing systems, smart cities, transport, and modern infrastructure.

- **SDG 12: Responsible Consumption and Production** (*Ensure sustainable consumption and production patterns*)

Utilizing knowledge of cloud deployment, execution, and security promotes the rational use of available computing power, robust data protection, reduction of production and data storage costs, and the efficient utilization of all available technological resources.

3. Content of the academic discipline

CONTENT MODULE 1. Standards, architecture, and principles of building distributed systems based on service models and cloud platform technologies

Topic 1. Basic concepts and classification of cloud computing systems. Definition and key characteristics of cloud computing. Evolution of cloud technologies: from Grid and Utility computing to modern hyperscalers. Classification of cloud systems by models and types of computing. Standardization in the field of cloud technologies: the role of NIST SP 800-145 and the work of ISO/IEC JTC 1/SC 38.

Topic 2. Basic architectures and components of cloud platforms. Cloud data center architecture: distributed nature, virtualization (the role of hypervisor and containerization). Key components of cloud infrastructure. Principles of Multi-tenancy. The concept of Software-Defined Networking (SDN) and Software-Defined Infrastructure (SDI) in the context of security.

Topic 3. Service models of cloud platforms (IaaS, PaaS, SaaS) and their security aspects. IaaS (Infrastructure as a Service): management, host- and network-level security, virtualization risks. PaaS (Platform as a Service): application-level security, runtime environment, platform-level identity and access management (IAM). SaaS (Software as a Service): data security, access configuration, risks associated with vendor trust. Function as a Service (FaaS/Serverless Computing): unique security challenges of "cold start", secrets management, and injection attacks.

Topic 4. Deployment models of cloud platforms and risks. Private cloud: architecture, management, and compliance with corporate security standards. Public cloud: high availability, scalability, but vendor dependence and the need for enhanced configuration control. Hybrid cloud: ensuring security continuity during the transition between private and public environments (Cloud Bursting). Multi-cloud environment: unified security policy management, provider interoperability, and tool unification.

CONTENT MODULE 2. Cloud platforms: principles of operation and architecture. Advantages of different providers and their combination. Protection methods and models in the cloud, different types of responsibility.

Topic 5. General overview of modern platforms. Google Cloud Platform (GCP) cloud platform. Shared Responsibility Model: detailed analysis of the boundaries of responsibility between customer and provider. GCP Security: "Zero Trust" (BeyondCorp) philosophy from Google. Key GCP security components: Cloud Identity and Access Management (IAM), Cloud Armor (WAF/DDoS), VPC Service Controls, Security Command Center (SCC). Overview of tools for data security in GCP: KMS, Secret Manager, Cloud Data Loss Prevention (DLP).

Topic 6. Amazon Web Services (AWS) cloud computing platform. AWS security architecture: multi-layered defense. AWS Security Tools: detailed consideration of IAM (Policies, Roles, Users), Security Hub, GuardDuty (Threat Detection), Inspector (Vulnerability Management). Network security in AWS: VPC (Virtual Private Cloud), Security Groups, Network ACLs, Transit Gateway. S3 object storage security: access policies (Bucket Policies), encryption, and access logging.

Topic 7. Capabilities of Microsoft Azure cloud services. Azure Security Strategy: Defense in Depth concept and integration with Microsoft enterprise solutions. Key Azure security services: Azure Active Directory (Azure AD), Azure Security Center (Defender for Cloud), Azure Key Vault (Secrets Management). Azure Sentinel (SIEM/SOAR): incident response automation and security information management. Ensuring compliance and regulatory requirements in Azure (e.g., GDPR, HIPAA) via Azure Policy.

Topic 8. Access security and cloud resources. Identity and Access Management (IAM): implementation of the Principle of Least Privilege, Role-Based Access Control (RBAC), conditional access. Multi-Factor Authentication (MFA) and risk-based adaptive authentication. Secrets Management: use of Key Management Services (KMS) and specialized secret stores. API security: protection of cloud API interfaces, API Gateway, token management, and request rate limiting.

4. Structure of the academic discipline

Topics	Number of Hours									
	Full-time study					Part-time study				
	Total	including				Total	including			
		lec	prac	lab	selfst		lec	prac	lab	selfst
1	2	3	4	5	6	7	8	9	10	11
Content Module 1. Standards, architecture, and principles of building distributed systems based on service models and cloud platform technologies										
Topic 1. Basic concepts and classification of cloud computing systems.	10	2			8					
Topic 2. Basic architectures and components of cloud platforms.	10	2	2		6					
Topic 3. Service models of cloud platforms.	10	2	2		6					
Topic 4. Deployment models of cloud platforms	10	2	2		6					
Total for Content Module 1	40	8	6		26					
Content Module 2. Cloud platforms: principles of functioning and construction. advantages of different providers and their combination. Methods and models of protection in the cloud, different types of responsibility.										
Topic 5. General overview of modern platforms. Google Cloud Platform. Key components and their purpose.	12	2	2		8					
Topic 6. Amazon Web Services (AWS) cloud computing platform.	12	2	2		8					
Topic 7. Capabilities of Microsoft Azure cloud services.	12	2	2		8					
Topic 8. Access security and cloud resources.	14	2	2		10					
Total for Content Module 2	50	8	8		34					
Total Hours	90	16	14		60					

5. Seminar Topics

Seminar classes are **not** provided for by the curriculum.

6. Practical Class Topics

No.	Topic Name	Number of Hours	
		Full-time study	Part-time study
1	Conduct a comparative analysis of the distribution of responsibility for the security of data, operating system, network, and applications between the client and the provider in the IaaS, PaaS, and Serverless (FaaS) models.	2	
2	Investigate the implementation of the Zero Trust model in cloud environments.	2	
3	IAM account lifecycle and the use of temporary credentials.	2	
4	Investigate the principles of Key Management Service (KMS) and compare the BYOK (Bring Your Own Key) and HYOK (Hold Your Own Key) approaches from the perspective of control and compliance.	2	
5	Implement Identity and Access Management (IAM) based on the principle of least privilege.	2	
6	Implement secrets management using Key Management Services (KMS) and specialized secret stores.	2	
7	Develop a response procedure for a typical cloud incident (e.g., a compromised administrator account).	2	
Total		14	

7. Laboratory Work Topics

Laboratory classes are **not** provided for by the curriculum.

8. Self-Study

No.	Topic Name/Question for Preparation	Number of Hours	
		Full-time study	Full-time study
1	In-depth analysis of the shared responsibility model and risks of service models	6	
2	Zero Trust architecture and cryptographic isolation	6	
3	Comprehensive Identity and Access Management (IAM)	6	
4	Data Protection: KMS, BYOK, HYOK and Confidential Computing	6	
5	DevSecOps and security automation in CI/CD	6	
6	Security of Container and Serverless environments	6	
7	Cloud Security Posture Management (CSPM) and prevention of Misconfiguration	6	

8	Cloud Access Security Brokers (CASB) and Data Loss Prevention (DLP)	6	
9	Regulatory Compliance, Data Sovereignty and cloud standards	6	
10	Incident Response and Cloud Forensics	6	
Total		60	

Self-Study work includes:

- [1] – preparation for lectures and practical classes;
- [2] – non-formal and/or informal education, etc.

Acceptance of results obtained in the system of non-formal/informal education

Name of the educational platform	Name of the course	Link
Google Cloud Platform;	Google Cloud Skills Boost	https://www.cloudskillsboost.google/
Amazon Web Services (AWS);	Amazon Web Services	https://aws.amazon.com/training/?intClick=gsrc_navbar
Microsoft Azure;	Microsoft Azure	https://learn.microsoft.com/uk-ua/training/browse/?products=azure

HYPERLINK

"

h

t

t

p

s

:

/

/

o

n

u

.

e

d

u

.

u

a

/

p

9. Teaching methods

The following teaching methods are used in the process of studying the academic discipline:

verbal methods: lectures (problem-based, visualization lectures, case study lectures, etc.), narration, explanation, conversation, discussion, debate, discussion of problem situations, situational learning;

visual methods: illustration (including multimedia presentations), demonstration, method of direct observation, presentation of own research results;

practical methods: exercises; training exercises; solving calculation problems; practical works; laboratory works; project method (designing); individual tasks performance.

10. Forms of control and evaluation methods (including criteria for evaluating learning outcomes)

Control is carried out in compliance with the requirements of objectivity, an individual approach, systematicity and consistency, and comprehensiveness.

Current control: Questioning during practical classes and Execution and defense of practical works.

Periodic control: control work (testing) by content module (CM).

Final control – a pass/fail test is graded on a 100-point scale using a cumulative system.

Evaluation criteria for various types of work

Type of control	Number of points
Questioning during classes	From 0 to 10 points
Execution and defense of practical works	From 0 to 10 points
Control work (testing) by CM	From 0 to 10 points

Type of control	Points	Criteria
Questioning during practical classes	1	1 point for each correct answer to one question.
Execution and defense of practical works	0-2	Work is not completed, completed with errors, the task is not fulfilled.
	3-5	Work is incomplete, completed with errors; the higher education applicant does not understand the principles of operation and cannot explain them, and does not answer all questions.
	6-8	Work is completed with some inaccuracies; the applicant does not answer all control questions.
	9-10	Work is completed fully and correctly; the applicant exhaustively explains the ways of solving the task and gives complete answers to control questions.
Control work (testing) by CM	1	1 point for each correct answer to one question.

Policy on deadlines and retakes: In case of missing a class for valid reasons, the applicant is obliged to complete the test on the relevant topic in extracurricular time as agreed with the teacher. Retaking takes place with the permission of the dean's office in the presence of valid reasons.

Academic integrity policy: during the mastering of the academic discipline, any types of academic integrity violations by both higher education applicants and the teacher are strictly prohibited. In case of detection and recording of any type of academic integrity violation, sanctions provided by the Law of Ukraine "On Academic Integrity" and internal regulatory documents of Odesa I. I. Mechnikov National University will be applied to the violator.

Policy on the use of artificial intelligence: during the mastering of this academic discipline, it is prohibited to publish texts, images, models, data, and other results generated by artificial intelligence as the results of one's own academic and educational activities unless allowed by the conditions of the educational task, and this fact itself is indicated in the educational task or accompanying materials. The use of artificial intelligence resources is prohibited during the final assessment.

11. Questions for final control

Part I: Basics and Architecture (Questions 1-10)

1. Explain the essence of the Shared Responsibility Model. Provide an example of a specific risk for which the client is responsible in the PaaS model, and a risk for which the provider is responsible.
2. Describe the architectural role and main functions of CASB (Cloud Access Security Broker). How does CASB help in implementing the DLP (Data Loss Prevention) policy between the local network and SaaS cloud services?
3. Analyze the Zero Trust principle in the context of cloud microservice architectures. How does the concept of an "identity-defined perimeter" replace the traditional network perimeter?
4. What is the critical difference between Attribute-Based Access Control (ABAC) and Role-Based Access Control (RBAC)?
5. Provide a scenario in the cloud (e.g., AWS, Azure) where using ABAC is more advantageous.
6. What is Confidential Computing and what key limitation of traditional encryption (data at rest and in transit) is it designed to solve using hardware enclaves (TEE)?
7. Justify why Cloud Misconfiguration is considered the greatest threat to cloud security. What tool approach (e.g., CSPM) is used to prevent and monitor it?
8. Explain the concept of Data Sovereignty and Data Residence. What impact does this have on the placement strategy of confidential data (e.g., personal data regulated by GDPR)?
9. Describe the mechanism of Federated Identity (e.g., using SAML or OIDC) and its importance for implementing Single Sign-On (SSO) in a hybrid cloud environment. What is the difference between Security Groups and Network Access Control Lists (NACLs) network control mechanisms in the cloud? Provide key differences regarding stateful/stateless operation.
10. How does Infrastructure as Code (IaC), in particular the use of tools like Terraform or CloudFormation, contribute to the implementation of the Shift Left approach in security?

Part II: Workload and Data Security (Questions 11-20)

11. Detail the difference between BYOK (Bring Your Own Key) and HYOK (Hold Your Own Key) in the context of Key Management Services (KMS). Which approach provides a higher level of control for the client?
12. What unique security issues arise in Serverless (FaaS) environments compared to traditional VMs? Focus on function IAM permissions and Cold Start risks.
13. What is Container Image Scanning and at what stage of the CI/CD pipeline should it be integrated to effectively prevent Supply Chain Attacks?
14. Describe the purpose and principle of operation of DAST (Dynamic Application Security Testing). Why is DAST more important for cloud security than SAST when identifying vulnerabilities related to execution logic?
15. What function does a Web Application Firewall (WAF) perform in cloud architecture? Provide examples of three types of attacks from the OWASP Top 10 list that WAF protects against.
16. Explain the risk of Over-Privileging and its consequences. How do CIEM (Cloud Infrastructure Entitlement Management) tools help solve this problem?
17. What is the risk of Lateral Movement in a cloud network? How does Microsegmentation help minimize the potential damage from such an attack?
18. Justify the need to use Secret Management (e.g., AWS Secrets Manager, Azure Key Vault) in the cloud. What risks arise when storing secrets in code or environment variables?
19. What is the role of Hardware Security Modules (HSMs) in cloud KMS? How do they enhance the security of encryption keys compared to software solutions?
20. What security measures should be taken to protect API interfaces in the cloud (e.g., API Gateway) to prevent unauthorized access and excessive usage (rate limiting)?

Part III: Compliance, Audit, and Risk Management (Questions 21-30)

21. What are the main stages of the Cloud Risk Assessment process? What should be focused on when analyzing threats related to external integrations?
22. Explain how logging and auditing mechanisms (CloudTrail, Azure Monitor) are used in the Incident Response process. What information is most important for conducting cloud forensics?
23. Describe the principle of Immutable Infrastructure and how it affects security and patch management.
24. How does applying security policies as code (Security-as-Code) help ensure Compliance and prevent Configuration Drift?
25. Reveal the concept of Vendor Lock-in in the context of cloud security. What strategies can be used to minimize it?
26. What risks are associated with using public repositories (e.g., Docker Hub, PyPI) to obtain base images/libraries? How can these risks be mitigated?
27. What are Cloud Security Alliance (CSA) Star and CIS Benchmarks? Explain their importance for clients when selecting and configuring cloud services.
28. Explain the importance of Secret Rotation and Temporary Credentials in the cloud. How does this reduce the risk associated with the compromise of long-term access keys?
29. What is the difference between hypervisor-level isolation and container-level isolation (e.g., in Kubernetes)? What are the security consequences of an isolation breach in both cases?
30. Which international security standard (e.g., ISO/IEC 27017) is most relevant for auditing and evaluating the security of cloud services and why?

12. Distribution of points received by higher education applicants

Current and periodic control								Total points
Content Module 1				Content Module 2				
T1	T2	T3	T4	T5	T6	T7	T8	100
10	10	10	10	10	10	10	10	
Control work for CM 1 – 10				Control work for CM 2 – 10				

T1, T2 ... T8 – topics

* Note: Control work for a content module is carried out in the form of written test tasks after completing the study of the educational material of each content module. Written test tasks consist of 10 test tasks and correspond to the content of the module's educational material. For each correct answer to one test task, the student receives 1 point.

Grading scale: national and ECTS

Total score for all types of educational activities	ECTS grade	Grade on the national scale	
		for an exam, course project (work), practical training	for a pass/fail test
90-100	A	excellent	passed
85-89	B	good	
75-84	C		
70-74	D	satisfactory	
60-69	E		
35-59	FX	unsatisfactory with the possibility of retaking	not passed with the possibility of retaking
0-34	F	unsatisfactory with mandatory retaking of the discipline	not passed with mandatory retaking of the discipline

Grade on the national scale	Theoretical preparation	Practical preparation
	Education applicant	
90-100/ passed	Fully masters the educational material, presents it fluently, independently, and argumentatively during oral presentations and written responses; deeply and comprehensively covers the content of theoretical questions, using regulatory, mandatory, and supplementary literature; draws independent conclusions and identifies cause-and-effect relationships; independently finds additional information and uses it to accomplish the tasks set before them. The higher education applicant is able to highlight essential features of the studied material through synthesis and analysis operations, identify cause-and-effect relationships, form conclusions and generalizations, and fluently operate with facts and data.	Deeply and comprehensively reveals the essence of practical tasks, using regulatory, mandatory, and supplementary literature; can argumentatively choose a rational method for completing a task and evaluate the results of their own practical activity; performs creative tasks and initiates new ways of completing them; fluently uses acquired theoretical knowledge when analyzing practical material; demonstrates a creative approach to completing individual and collective tasks during independent work.

75-89 / passed	sufficiently fully masters the educational material, reasonably presents it during oral presentations and written answers, using normative and mandatory literature; when presenting some questions, there is a lack of sufficient depth and argumentation, applies knowledge to solve standard situations; independently analyzes, generalizes and systematizes educational information, but isolated insignificant inaccuracies and minor errors are allowed.	correctly solved most practical tasks according to the model; has stable skills in completing the task
60-74 / passed	masters the educational material at the reproductive level or reproduces a certain part of the educational material with elements of logical connections, knows the basic concepts of the educational material; has difficulties during highlighting essential features of the studied; during identifying cause-and-effect relationships and formulating conclusions.	can use knowledge in standard situations, has elementary, unstable skills in completing the task. Correctly solved half of the practical tasks. The applicant has difficulties during highlighting essential features of the studied; during identifying cause-and-effect relationships and formulating conclusions.
35-59 / not passed with the possibility of retaking	masters the educational material superficially and fragmentarily (without argumentation and justification); unsystematically highlights random features of the studied; does not know how to do the simplest analysis and synthesis operations; making generalizations and conclusions is difficult; significant mistakes are made during the answer.	insufficiently reveals the essence of practical tasks, allowing significant inaccuracies, correctly solved isolated practical tasks with the help of a teacher, formed abilities and skills are absent.
0-34/ not passed with mandatory retaking of the discipline	does not master the educational material	completes only elements of the task, requires constant help of a teacher

Note: the maximum number of points for each topic is specified in paragraph 12.

13. Educational and methodological support

1. Syllabus of the discipline;
2. Educational and methodological materials for lectures, lecture notes (texts, diagrams);
3. Multimedia presentations;
4. Plans of practical classes;

14. Recommended literature

Basic

1. John Culkin, Mike Zazon. AWS Cookbook: Recipes for Success on AWS. — 1st Edition — O'Reilly Media, 2022 — 356 p.
2. Reza Salehi. Azure Cookbook: Recipes to Create and Maintain Cloud Solutions in Azure. — 1st Edition — O'Reilly Media, 2023 — 332 p.
3. Rui Costa, Drew Hodun. Google Cloud Cookbook: Practical Solutions for Building and Deploying Cloud Services. — 1st Edition — O'Reilly Media, 2021 — 282 p.

4. Sean P. Kane, Karl Matthias. Docker: Up & Running: Shipping Reliable Containers in Production. — 3rd Edition — O'Reilly Media, 2023 — 422 p.
5. Alan Hohn. The Book of Kubernetes: A Complete Guide to Container Orchestration. — No Starch Press, 2022 — 384 p.
6. Chris Richardson. Microservices Patterns: With examples in Java. — 1st Edition — Manning, 2018 — 520 p.
7. Thomas Erl, Zaigham Mahmood, and Ricardo Puttini. Cloud Computing Concepts, Technology & Architecture. Prentice Hall, 2013 . - 528 p.
8. Ray J Rafaels. Cloud Computing: From Beginning to End. CreateSpace Independent Publishing Platform, 2015 – 152p.

Additional

1. AWS Documentation. <https://docs.aws.amazon.com/>
2. Azure documentation. <https://learn.microsoft.com/en-us/azure/>
3. Google Cloud documentation. <https://cloud.google.com/docs/>
4. Yevgeniy Brikman. Terraform: Up and Running: Writing Infrastructure as Code. — 3rd Edition — O'Reilly Media, 2022 — 457 p.

15. Electronic information resources

1. <https://mon.gov.ua/> – official website of the Ministry of Education and Science of Ukraine;
2. <http://nbuv.gov.ua/> - Website of the V. I. Vernadskyi National Library of Ukraine;
3. <http://www.dnpgov.ua/> - Website of the V.O. Sukhomlynskyi State Scientific and Pedagogical Library of Ukraine;
4. <http://onu.edu.ua/> - Website of the library of ONU named after I.I. Mechnikov;
5. <http://odnb.odessa.ua/> - Website of the Odesa National Scientific Library;
6. <http://korolenko.kharkov.com/> - Website of the Kharkiv State Scientific Library named after V.G. Korolenko.
7. <https://cloudonair.withgoogle.com/events/cloud-for-students/resources> - Materials of webinars for students on the GCP platform
8. <https://www.cloudskillsboost.google/> - training, events and testing on the GCP platform from Google Cloud Skills Boost
9. https://aws.amazon.com/training/?intClick=gsrc_navbar – AWS training and certification
10. <https://learn.microsoft.com/uk-ua/training/browse/?products=azure> - Microsoft Azure training and certification