3. Educational program

Director of the Master's degree programme – **T.Savchenko**, PhD in Technical Sciences, Associate Professor, Associate Professor of the Department of Software Engineering and Cyber Security.

1. Profile of the educational program «Security of electronic communications systems in the economy» from specialty 125 «Cybersecurity and information protection»

1 – - General information	
Full name of the higher educational establishment and structural unit	State University of Trade and Economics, Faculty of Information Technologies Department of Software Engineering and Cyber Security
Degree of higher education and the name of the qualification in the language of the original	degree of higher education "master" specialty " Cybersecurity and information protection "
The official name of the educational program	«Security of electronic communications systems in the economy»
Conformity to the standard of higher education of the Ministry of Education and Science of Ukraine	The **standard of higher education** of the Ministry of Education and Culture of Ukraine is in charge
Type of diploma and volume of educational program	Master's degree, unitary, 90 ECTS credits
Availability of accreditation	Certificate of accreditation of Educational Professional Program, issued by NAHEQA, No. 6526 from 14.12.2023 to 12.12.2024
Cycle / Level	NRC Ukraine - 7 level, FQ-EHEA - second cycle, EQF-LLL - 7 level
Prerequisites	Individuals who have obtained a bachelor's degree can apply for a master's degree in the specialty 125 «Cybersecurity and information protection» of the field of knowledge 12 «Information technologies». The program of professional entrance exams for persons who have obtained a previous level of higher education in other specialties should provide for verification of the person's acquisition of competencies and learning outcomes defined by the standard of higher education in specialty 125 «Cybersecurity and information protection» for the first (bachelor's) level of higher education.
Language (s) Teaching	Ukrainian
Validity of the educational program	1 year 4 months
Internet address of the permanent placement of the description of the educational program	https://knute.edu.ua

2 – The purpose of the educational program	
To provide students of higher education of the second (master's) level with fundamental training in the specialty 125 «Cybersecurity and information protection», sufficient to solve tasks of a research and/or innovative nature in the field of information and/or cyber security in economy.	
3 – Characteristics of the educational program	
Subject area	**Objects of study:** – modern processes of research, analysis, creation and ensuring the functioning of information systems and technologies, other business operational processes at the objects of information activity and critical infrastructures in the field of information security and/or cyber security; – information systems (information-communication, information-telecommunication, automated) and technologies; – infrastructure of information activity objects and critical infrastructures; – systems and complexes of creation, processing, transmission, storage, destruction, protection and display of data (information flows); – information resources of various classes (including state information resources); – software and technical means (means) of cyber protection; – information security and/or cyber security management systems; – technologies, methods, models and means of information security and/or cyber security. **Learning goals:** Training of specialists capable of solving problems of a research and / or innovative nature in the field of information and / or cyber security. **Theoretical content of the subject area:** Theoretical foundations of science-intensive technologies, physical and mathematical fundamental knowledge, theories of identification and decision-making, system analysis, complex systems, process modeling and optimization, theory of mathematical statistics, cryptographic and technical information protection, risk theory and other interdisciplinary theories and practices in the field of information security and/or cyber security. **Methods, techniques and technologies:** Methods, models, techniques and technologies of creation, processing, transmission, reception, destruction, display, protection (cyber protection) of information resources in cyberspace, as well as methods and models of development and use of applied and specialized software for solving professional tasks in the field of information security and/or cyber security. Technologies, methods and models of research, analysis, management and provision of business/operational processes using a set of regulatory and legal and organizational and technical methods and means of protecting information resources in cyberspace. **Tools and equipment:** Means, devices, network equipment and environment, applied

	and specialized software, automated systems and complexes of design, modeling, operation, control, monitoring, processing, display and protection of data (information flows), as well as methods and models of risk theory and information management resources for research and support of objects of information activity in the field of information security and/or cyber security.
Orientation of educational program	The program is focused on educational, professional and applied training The program is aimed at training a specialist capable of solving professional problems related to electronic communication systems, in particular in the economy.
The main focus of the educational program	Educational and professional. The program is aimed at combining practice and science, regarding the organization, development and operation of complex components of cyberspace in order to ensure the information security of economic entities of the state economy, taking into account possible external cyber influences, probable threats and the level of development of technologies for the protection of electronic communications systems. Keywords: security technologies of wireless and mobile networks, security technologies of Web resources, penetration testing, system vulnerability, information security management system of a business entity, legal provision of information security in economic systems, economic security of the state.
Features of the program	The program involves the training of professionals capable of: modeling and forecasting possible cyber impacts on economic entities of the state economy and individuals; conduct an audit of electronic communications systems of business entities; apply regulatory documents and standards in the development of measures to protect electronic communications systems of economic entities of the state economy.
4 - Eligibility of graduates for employment and further training	
Eligibility for employment	The specialist is able to perform professional work and hold positions defined by the National Classifier of Ukraine "Classifier of Professions ДК 003:2010", in particular: 2359.2 Instructor-methodologist in information security and cyber security. A graduate can hold positions that meet the professional standard for cyber security and information protection and according to the professional titles of jobs characterized by special (professional) competencies, namely: "Instructor-methodologist in information security and cyber security" and "Leading instructor-methodologist in information security" security and cyber security"..
Further education	Continuation of education at the third (educational and scientific) level of higher education. Acquisition of additional qualifications in the adult education system.
5 – Teaching and evaluation	
Teaching and learning	Focused on students teaching, self-studying, laboratory-based learning, problem-based, interactive, project-based, information-computer, self-development, collective and integrative, contextual learning technologies

Assessment	Evaluation of students' educational achievements is carried out on the basis of: "Regulations on the organization of the educational process of students"; "Regulations on the evaluation of learning outcomes of students and graduate students."On a 100-point scale. Written exams, practice, essays, presentations, testing, defense of laboratory works, defense of individual works, defense of the final qualification project.
6 – Program competencies	
Integral competence	The ability of an individual to solve problems of a research and / or innovative nature in the field of information security and / or cybersecurity.
General competences (GC)	GS-1. Ability to apply knowledge in practical situations. GS-2. Ability to conduct research at an appropriate level. GS-3. Ability to abstract thinking, analysis and synthesis. GS-4. The ability to evaluate and ensure the quality of the work performed. GS-5. Ability to communicate with representatives of other professional groups of different levels (with experts from other fields of knowledge / types of economic activity). *GS -6. Ability to act socially responsible and socially conscious.* *GS -7. Ability to adapt and act in a new situation.* *GS -8. Ability to choose a communication strategy, work in a team.* *GS -9. The ability to communicate in the native language both orally and in writing, to communicate in a foreign language (mainly English) at a level that ensures effective professional activity.*
Special competencies (SC)	SC1. The ability to reasonably apply, integrate, develop and improve modern information technologies, physical and mathematical models, as well as technologies for creating and using applied and specialized software to solve professional problems in the field of information security and/or cyber security. SC2 Ability to develop, implement and analyze regulatory documents, regulations, instructions and requirements of technical and organizational direction, as well as integrate, analyze and use the best global practices, standards in professional activities in the field of information security and/or cyber security. SC3. Ability to research, develop, and maintain information security and/or cyber security methods and tools at information activity and critical infrastructure facilities. SC4. The ability to analyze, develop and support the information security and/or cyber security management system of the organization, to form information security strategy and policy taking into account domestic and international standards and requirements. SC5. Ability to research, system analysis and ensure the continuity of business/operational processes in order to identify vulnerabilities of information systems and resources, analyze risks and determine their impact assessment in accordance with the established information security and/or cyber security strategy and policy of the organization. SC6. The ability to analyze, control and provide a management system for access to information resources in accordance with the established strategy and policy of information security and/or cyber security of the organization.

	SC7. Ability to research, develop and implement methods and measures to counter cyber incidents, implement management, control and investigation procedures, as well as provide recommendations for the prevention and analysis of cyber incidents in general. SC8. The ability to research, develop, implement and support methods and means of cryptographic and technical protection of information at objects of information activity and critical infrastructure, in information systems, as well as the ability to evaluate the effectiveness of their use, in accordance with the established strategy and policy of information security and/or cyber security of the organization. SC9. The ability to analyze, develop and support the system of auditing and monitoring the effectiveness of the functioning of information systems and technologies, business/operational processes in the field of information security and/or cyber security of the organization as a whole. SC10. Ability to conduct scientific and pedagogical activities, plan training, monitor and support work with personnel, as well as make effective decisions on issues of information security and/or cyber security. SC*11. The ability to analyze electronic communications networks and counter actions that threaten the availability, integrity or confidentiality of such networks and services, as well as data stored, transmitted or processed, and related services, particularly in the economy.* *SC12. Ability to act as an internal consultant and advisor in your area of expertise.* *SC13. The ability to conduct research and experimental work on the procedure for scanning vulnerabilities and their recognition in security systems.*
7 – Program learning outcomes	
	PLO1. Communicate freely in national and foreign languages, orally and in writing, to present and discuss the results of research and innovation, ensure business/operational processes and issues of professional activity in the field of information security and/or cyber security. PLO2. Integrate fundamental and specialized knowledge to solve complex information security and/or cyber security challenges in broad or multidisciplinary contexts. PLO3. Conduct research and/or innovation activities in the field of information security and/or cyber security, as well as in the field of technical and cryptographic protection of information in cyberspace. PLO4. Apply, integrate, develop, implement and improve modern information technologies, physical and mathematical methods and models in the field of information security and/or cyber security. PLO5. Critically consider the problems of information security and/or cyber security, including at the intersectoral and interdisciplinary level, in particular on the basis of understanding the new results of engineering and physical and mathematical sciences, as well as the development of technologies for creating and using specialized software. PLO6. Analyze and evaluate the security of systems, complexes and means of cyber protection, technologies for creating and using specialized software. PLO7. To justify the use, implement and analyze the best global

	standards, practices in order to solve complex problems of professional activity in the field of information security and/or cyber security. PLO8. Research, develop and support systems and means of information security and/or cyber security at objects of information activity and critical infrastructure. PLO9. Analyze, develop and support the organization's information security and/or cyber security management system based on information security strategy and policy. PLO10. Ensure the continuity of business/operational processes, as well as identify vulnerabilities of information systems and resources, analyze and assess risks for information security and/or cyber security of the organization. PLO11. Analyze, monitor and ensure the effective functioning of the information resources access management system in accordance with the established information security and/or cyber security strategy and policy of the organization. PLO12. Research, develop and implement methods and measures to counter cyber incidents, implement management, control and investigation procedures, as well as provide recommendations for the prevention and analysis of cyber incidents in general. PLO13. Research, develop, implement and use methods and means of cryptographic and technical information protection of business/operational processes, as well as analyze and provide an assessment of the effectiveness of their use in information systems, objects of information activity and critical infrastructure. PLO14. Analyze, develop and support the system of auditing and monitoring the effectiveness of the functioning of information systems and technologies, business/operational processes in the field of information and/or cyber security as a whole. PLO15. Clearly and unambiguously convey own conclusions on information security and/or cyber security issues, as well as the knowledge and explanations that justify them to staff, partners and others. PLO16. Make informed decisions on organizational and technical issues of information security and/or cyber security in complex and unpredictable conditions, including using modern methods and means of optimization, forecasting and decision-making. PLO17. Have the skills of autonomous and independent learning in the field of information security and/or cyber security and related fields of knowledge, analyze one's own educational needs and objectively evaluate the results of training. PLO18. Plan training, as well as accompany and supervise work with personnel in the direction of information security and/or cyber security. PLO19. Choose, analyze and develop suitable typical analytical, calculation and experimental methods of cyber protection, develop, implement and support the project on the protection of information in cyberspace, innovative activities and protection of intellectual property. PLO20. Set and solve complex applied engineering and scientific problems of information security and/or cyber security, taking into account the requirements of domestic and international standards and best practices. PLO21. Use the methods of natural, physical and computer modeling to study processes related to information security and/or cyber security.

	PLO22. Plan and carry out experimental and theoretical research, put forward and test hypotheses, choose suitable methods and tools for this, carry out statistical processing of data, evaluate the veracity of research results, argue conclusions. PLO23. Justify the selection of software, equipment and tools, engineering technologies and processes, as well as their limitations in the field of information security and/or cyber security based on current knowledge in related fields, scientific, technical and reference literature and other available information. PLO*24. Make informed decisions and take appropriate technical and organizational measures to ensure the security of electronic communication networks and services in order to guarantee the integrity of own electronic communication networks, the continuity of the provision of electronic communication services, and the prevention of unauthorized access to electronic communication networks.* *PLO25. Perform the duties of an internal consultant/advisor in the technical field and the field of copyright in relation to electronic media.* *PLO26. Communicate with managers of different levels (interpersonal communication, accessibility, ability to effectively perceive the speaker's language, adjust the style and language of the speech according to the audience).* *PLO27. Conduct security system scanning of information resources for vulnerabilities.* *PLO28. Apply the principles of information security - preservation of confidentiality, integrity and availability.*
8 – Resource support for the implementation of the program	
Personnel provision	Scientific and pedagogical workers with scientific degrees and/or scientific titles, as well as highly qualified specialists and practitioners are involved in the implementation of the program.
Material and technical support	Use of laboratories, computer and specialized classrooms, libraries and SUTE infrastructure in general.
Informational and educational support	The single digital space of the University combines all departments that are aimed at shaping the individual trajectory of a higher education seeker. The existing MOODLE distance learning system and the MS 365 environment ensure independent and individual work of students.
9 – Academic mobility	
9 – Academic mobility	National credit mobility is carried out in accordance with concluded agreements on academic mobility
International credit mobility	International credit mobility is implemented through the conclusion of agreements on international academic mobility (Erasmus+), on double graduation, on long-term international projects that provide for student training, the issuance of a double diploma, etc.
Education for foreign applicants for higher education	It is provided on the condition of mandatory knowledge of the Ukrainian language at a level not lower than B1.

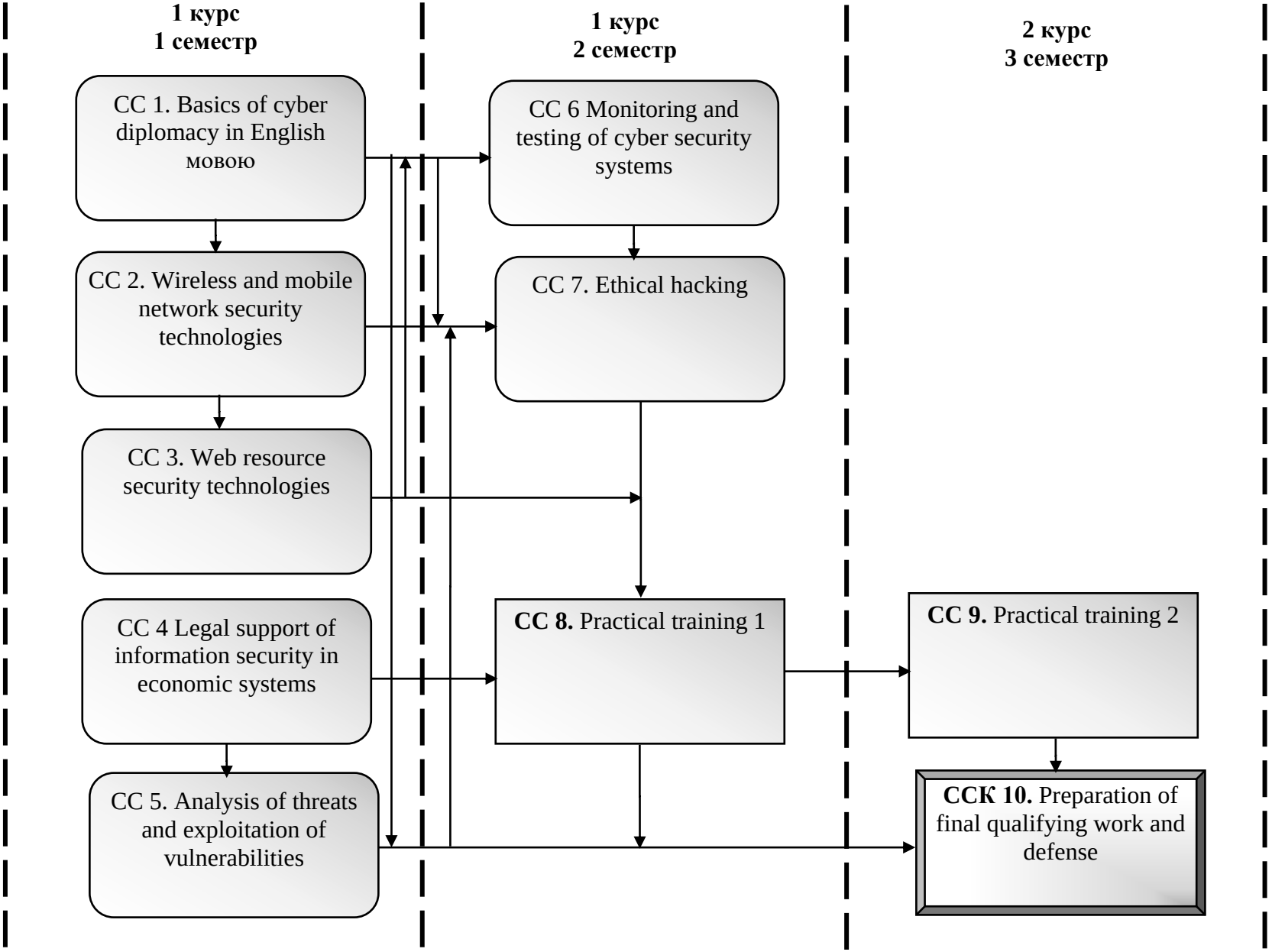
2.1. 2. List of components of the educational program and their logical consistency

2.1. List of components of EP

Code e/d	Components of the educational program (academic disciplines, course projects (works), practices, qualification exam, final qualifying work)	Number of credits
1	2	3
Compulsory Components of EP		
CC 1.	Basics of cyber diplomacy in English	6
CC 2.	Wireless and mobile network security technologies	6
CC 3.	Web resource security technologies	6
CC 4.	Legal support of information security in economic systems	6
CC 5.	Analysis of threats and exploitation of vulnerabilities	6
CC 6.	Monitoring and testing of cyber security systems	6
CC 7.	Ethical hacking	6
CC 8.	Practical training 1	12
CC 9.	Practical training 2	3
CC 10.	Preparation of final qualifying work and defense	9
Total of Compulsory Components:		66
Optional Components of EP		
OC 1	UI/UX Design in English	6
OC 2.	Administration and protection of data storages	6
OC 3.	Mobile applications security	6
OC 4.	Internet of Things technology security	6
OC 5.	Biometric authentication technologies in information systems	6
OC 6.	Business Intelligence Tools	6
OC 7.	Intellectual Property	6
OC 8.	Information technologies in the system of ensuring the economic security of the state	6
OC 9.	IT law	6
OC 10.	Commercial intelligence and internal security in the enterprise	6
OC 11.	Psychology of adaptation	6
OC 12.	Business psychology	6
OC 13.	Stochastic methods in economics	6
OC 14.	Data analysis technologies	6
OC 15.	Philosophy of personality	6
OC 16.	Functional and logical programming	6
Total of Optional Components		**24**
Total of Educational Program		**90**

For all components of the educational program the form of final control is an exam.

2.2. Structural Logic Scheme of EP



3. Form of attestation of applicants for higher education

Attestation is carried out in the form of public defense of the final qualifying work.

The qualification work must solve a complex problem of information security and/or cyber security and involve research and/or innovation.

The qualifying work should not contain academic plagiarism, fabrication, or falsification.

The qualification work must be posted on the official website (or in the repository) of the higher education institution or its division. The publication of qualifying works with limited access is carried out in accordance with the requirements of the law.

4.1. Matrix of correspondence of program competencies with the compulsory components of the educational program

Components / Competencies	CC 1	CC 2	CC 3	CC 4	CC 5	CC 6	CC 7	CC 8	CC 9	CC 10
GC-1.	+	+	+	+	+	+	+	+	+	+
GC -2.		+	+	+	+		+			+
GC -3.	+				+	+	+			+
GC -4.			+		+	+		+	+	
GC -5.	+	+		+	+		+			
GC -*6.*	+			+	+		+			
GC -*7.*	+			+	+			+	+	
GC -*8.*	+			+				+	+	
GC -*9.*	+							+	+	+
SC1.		+	+	+	+	+	+	+	+	+
SC 2.	+	+	+	+		+	+	+	+	+
SC 3.		+		+	+	+	+	+	+	+
SC 4.	+	+		+			+	+	+	+
SC 5.	+	+	+		+		+	+	+	+
SC 6.			+					+	+	+
SC 7.			+					+	+	+
SC 8.								+	+	+
SC 9.		+					+	+	+	+
SC 10.	+			+			+	+	+	+
SC 11.		+						+	+	+
SC 12.	+	+	+	+			+	+	+	+
SC 13.		+	+			+	+	+	+	+

5 . Matrix of correspondence of program learning outcomes (PLO) with relevant compulsory components of the educational program

Components / Program learning outcomes	CC 1	CC 2	CC 3	CC 4	CC 5	CC 6	CC 7	CC 8	CC 9	CC 10
PLO 1	+	+		+			+	+	+	+
PLO 2	+	+					+	+	+	+
PLO 3	+						+	+	+	+
PLO 4		+	+				+	+	+	+
PLO 5	+			+	+	+		+	+	+
PLO 6			+	+	+	+		+	+	+
PLO 7	+		+	+				+	+	+
PLO 8		+					+	+	+	+
PLO 9		+					+	+	+	+
PLO 10		+	+		+		+	+	+	+
PLO 11		+	+				+	+	+	+
PLO 12			+	+				+	+	+
PLO 13		+					+	+	+	+
PLO 14				+		+		+	+	+
PLO 15	+	+	+		+	+	+	+	+	+
PLO 16	+		+					+	+	+
PLO 17	+	+		+			+	+	+	+
PLO 18	+						+	+	+	+
PLO 19			+					+	+	+
PLO 20		+					+	+	+	+
PLO 21								+	+	+
PLO 22			+	+				+	+	+
PLO 23			+		+	+		+	+	+
PLO 24		+						+	+	+
PLO 25	+	+	+	+			+	+	+	+
PLO 26	+			+				+	+	+
PLO 27		+	+				+	+	+	+
PLO 28		+	+				+	+	+	+

4. Information about educational components (disciplines)

4.1. Name. Basics of cyber diplomacy in English Type. Compulsory
Year of study. 2024/2025.
Semester. I.
Lecturer, academic title, scientific degree, position. O.Haiduk, Senior Lecturer of the Department of Software Engineering an Cybersecurity
Learning outcomes. Formation of complex knowledge on the basics of cyber diplomacy; awareness of the role and place of cyber diplomacy in the national security system; orientation in the main international legal norms regulating cyberspace; understanding the peculiarities of the implementation of cyber diplomacy by the world's leading states; practical skills of risk and threat analysis in the field of international cyber security; assessment of prospects and possible scenarios for the development of cyber diplomacy; application of acquired knowledge to make informed decisions in the field of cyber diplomacy.
Compulsory previous academic subjects. "Sociotechnical cyber security", "Organization of computer networks", "Security of information systems and networks".
Content. Introduction to cyber diplomacy. Cyber security as a component of national security. International law and norms of state behavior in cyberspace. Institutional structure of cyber diplomacy and its economic and financial content. Regulatory and legal framework for cyber diplomacy of the leading states. Use of information and communication technologies in public diplomacy. Cyber threats and models of cyber conflicts. International cooperation in the field of cyber security. Cybercrime and cyberterrorism. Cyber espionage and cyber intelligence. Economic aspects of cyber diplomacy. Cyber security of critical infrastructure. Cyber dialogue as a tool of cyber diplomacy. Prospects for the development of cyber diplomacy.
Recommended sources and other educational resources / tools.
1. Cyberdiplomacy: Managing Security and Governance Online. Shaun Riordan. – Polity, 2019. – 160 p.
2. Internet Diplomacy. Shaping the Global Politics of Cyberspace. Meryem Marzouki, Andrea Calderaro. – Rowman & Littlefield Publishers, 2023. – 280 p.
3. Cyber-Diplomacy: Managing Foreign Policy in the Twenty-First Century. Edited By Evan H.Potter. – McGill-Queen's University Press, 2022. – 216 p.
Planned educational activities and teaching methods.

The study of the discipline is conducted through lectures (auditory) and laboratory classes (in a computer classroom on a PC), which ensure the consolidation of theoretical knowledge and contribute to the assimilation of practical skills.

Evaluation methods:

– current control (computer testing, survey);

– final control (exam).

Language of learning and teaching. English

4.2. Name. WIRELESS AND MOBILE NETWORK SECURITY TECHNOLOGIES

Type. Compulsory

Year of study. 2024/2025.

Semester. I.

Lecturer, academic title, scientific degree, position. Y. Kostyuk, PhD, Senior Lecturer of the Department of Software Engineering and Cyber Security.

Learning outcomes. Formation of future specialists' skills and competencies for assessment and ensuring the required level of information security in wireless and mobile networks; the ability to solve the problems of wireless and mobile network administration, to apply legal, organizational and technical procedures in the operation of wireless and mobile technologies; provision of knowledge on security and protection of modern wireless and mobile networks; protection of modern hardware and software of wireless and mobile networks.

Compulsory previous educational disciplines: "Organization of computer networks", "Security of information systems and networks".

Content. Basics of the theory of wireless transmission. Threats, attacks and protection of wireless networks. Network protocols and services. Network infrastructure for wireless networks. Standards of mobile communication networks. Threats and vulnerabilities of mobile devices. Architecture of 4G and 5G wireless networks. Security of 4G and 5G wireless networks. Architecture of WiFi technologies. Threats and vulnerabilities of WiFi networks. Security monitoring of wireless networks. Ways to protect wireless networks. Broadband wireless access networks of the IEEE 802.16 family of standards (WiMAX). Security of WSN wireless sensor networks. Security of ZigBee Personal Wireless Networks. Security of Bluetooth Personal Wireless Networks. WiFi security. WIDS wireless intrusion detection system. Protection of networks from unauthorized access using VPN technology.

Recommended sources and other learning resources/tools.

1. Бурячок В.Л., Соколов В.Ю. Методи забезпечення гарантоздатності і функціональної безпеки безпроводової інфраструктури на основі апаратного розділення абонентів: навчальний посібник. Київ: КУБГ, 2019. 164 с.
2. Інформаційна безпека: навчальний посібник / Ю.Я. Бобало, І.В. Горбатий, М.Д. Кіселичник, А.П. Бондарєв та інші; за заг. ред. д-ра техн. наук, проф. Ю.Я. Бобала та д-ра техн. наук, доц. І.В. Горбатого. – Львів: Видавництво Львівської політехніки, 2019. – 580 с.
3. Безпека інформаційних систем: навч. посіб. / В.І. Пашорін, Ю. В. Костюк. – Київ: Держ. торг.-екон. ун-т, 2022. – 376 с.
Planned educational activities and teaching methods. The study of the discipline is conducted through lectures (auditory) and laboratory classes (in a computer classroom on a PC), which ensure the consolidation of theoretical knowledge and contribute to the assimilation of practical skills.
Evaluation methods.
– current control (computer testing, survey);
– final control (exam).
Language of learning and teaching. Ukrainian

4.3. Name. WEB RESOURCE SECURITY TECHNOLOGIES
Type. Compulsory
Year of study. 2024/2025.
Semester. I.
Lecturer, academic title, scientific degree, position. N.Kotenko, Associate Professor, PhD in Education, Associate Professor of the Department of Software Engineering and Cyber Security**.**
Learning outcomes. The formation of theoretical knowledge and practical skills on the protection of web applications, starting from the stages of intelligence and finding vulnerabilities, typical vulnerabilities of the server and client part of the web application, as well as the formation of skills for finding and correcting coding problems of the web application.
Compulsory previous academic subjects. "Information technologies in professional activity", "WEB design and WEB programming".
Content. Basics of Internet Security Configuration: Hypertext Transfer Protocol; HTTPS (hypertext transfer protocol over secure sockets); SSL (Secure Sockets Layer) protocol; symmetric and asymmetric encryption; use of Simple Object Access Protocol (SOAP); SMTP protocol (Simple Mail Transfer Protocol); post office protocol (POP3); Internet Access Protocol (IMAP). An overview of web authentication technologies. Web application firewalls. OWASP Top 10 List Review. Intelligence and vulnerabilities of web applications: opening a web page/structure of the application;

collection of information in web applications; Vulnerability scanning of web applications. Security of the server side of web applications: introduction of server-side vulnerabilities, SQL injection, authentication and authorization of web applications, XXE injection, SSRF-forgery of requests on the server side, business logic vulnerabilities, etc. Security of the client part of web applications: cross-site scripting (XSS), cross-site request forgery (CSRF), cross-sharing of resources (CORS), DOM-based vulnerabilities, etc. Other web application client-side vulnerabilities: unsafe deserialization, web cache poisoning, HTTP host header attacks, OAuth authentication, XML security.

Recommended sources and other learning resources/tools.

1. OWASP Top Ten. URL:https://owasp.org/www-project-top-ten/
2. Professional Pen Testing for Web Applications. Front Cover. Andres Andreu. Wiley India Pvt. Limited, 2016.

Planned educational activities and teaching methods. A combination of traditional and non-traditional teaching methods with the use of innovative technologies: lectures (thematic, problem-based); laboratory classes using modern interactive technologies (traditional, modeling situations); individual work; consultations

Evaluation methods:

– current control (computer testing, survey);
– final control (exam).

Language of learning and teaching. Ukrainian

4.4. Name. LEGAL SUPPORT OF INFORMATION SECURITY IN ECONOMIC SYSTEMS

Type. Compulsory

Year of study. 2024/2025.

Semester. I.

Lecturer, academic title, scientific degree, position. O.Sytnichenko, PhD in Law, Associate Professor of the Department of Legal Support of Business Security.

Learning outcomes. Formation of students in-depth theoretical knowledge in the field of information security, mastering techniques and methods of protection of information resources of enterprises, institutions and organizations, which will help them to create conditions for protecting information from unauthorized access, identify and prosecute the guilty persons for illegal dissemination of information.

Compulsory previous academic subjects. "Jurisprudence", "Information Law".

Content. Theoretical and legal principles of information security. Competence of the state in the field of information security of Ukraine.

Observance of informational rights and human freedoms as the basis of information security. Information in the life of the state, man and society. Observance of informational rights and human freedoms as the basis of information security. Organizational and legal bases of protection and restriction of information flow in order to ensure information security. Organizational support for enterprise information protection. Information resources of the enterprise, bank. Organization of information and analytical work at the enterprise, bank. Legal principles of information infrastructure security. Cyber security. Types of legal responsibility for offenses in the information sphere.

Recommended sources and other learning resources/tools.

1. Бобало Ю.Я., Горбатий І.В, Кіселичник М.Д., Бондарєв А.П, Войтусік С.С. Інформаційна безпека: навч. посібник за заг. ред. Ю.Я. Бобало, І.В Горбатий, М.Д. Кіселичник, А.П Бондарєв, С.С. Войтусік. – Видавництво «Львівська політехніка» – 2019. – 580 с.
2. Гуз А.М., Мамченко С.М., Ткачук Т.Ю. та ін. Кадрова політика у сфері інформаційної безпеки: навч. посіб. – Київ.: Нац. акад. СБУ, 2017. – 210 с.

Planned educational activities and teaching methods. A combination of traditional and non-traditional teaching methods with the use of innovative technologies: lectures (overview), seminars/practical classes (training/presentation/discussion/work in small groups/other).

Evaluation methods.

– current control (surveys, written works, situational tasks);
– final control (exam).

Language of learning and teaching. Ukrainian

4.5. Name. ANALYSIS OF THREATS AND EXPLOITATION OF VULNERABILITIES

Type. Compulsory

Year of study. 2024/2025.

Semester. I.

Lecturer, academic title, scientific degree, position. Y. Khokhlachova, Professor, PhD in Technical Sciences, Professor of the Department of Security of Information Technologies of the National Aviation University.

Learning outcomes. Critically consider the problems of information security and/or cyber security, including at the interdisciplinary and interdisciplinary level, in particular based on the understanding of engineering and physical and mathematical sciences, as well as the

development of technologies for the creation and use of specialized software. Analyze and evaluate the security of systems, complexes and means of cyber protection, the technology of creating and using specialized software. Justify the choice of software, equipment and tools, engineering technologies and processes, as well as their limitations in the field of information security.

Compulsory previous academic subjects. "Basics of cyber security", "Security of operating systems", "Organization of computer networks", "Security of information systems and networks".

Content. National vulnerability. Protocols for documenting, tracking and sharing incident information. Data bank of information security threats. CVSS calculator v2.0. Database of vulnerabilities from open sources (Open Sourced Vulnerability Database). Modern attack databases and their use in intrusion detection systems. Database of web hacking incidents. Databases of attacks formed during cyber security competitions. IBM X-Force Vulnerability Database. US-CERT Vulnerability Record Database. Vulnerability databases in VND. SecurityFocus Vulnerability Database. Databases of KDD-99 attack patterns чи templates. CAPEC attack patterns чи templates.

Recommended sources and other learning resources/tools.

1. Луцький М.Г., Хорошко В.О., Хохлачова Ю.Є., Козловський В.В., Баланюк Ю.В., Прав Ю.Г. Новітні технології захисту інформації: підручник. К.: НАУ, 2023 312 с.
2. М.М. Браіловський, Н.С. Вишневська, В.Д. Козюра, Ю.В. Пепа, В.О. Хорошко, Ю.Є. Хохлачова. Комп’ютерні технології: навчальний посібник. К.: ФОП Ямчинський О.В., 2023. 200 с.
3. Браіловський М.М., Зибін С.В., Кобозєва А.А., Хорошко В.О., Хохлачова Ю.Є. Аналіз кіберзахищеності інформаційних систем Київ: ФОП Ямчинський О.В. 2021. 360 с.
4. Безпека інформаційних систем: навч. посіб. / В. І. Пашорін, Ю. В. Костюк. – Київ: Держ. торг.-екон. ун-т, 2022. – 376 с.

Planned educational activities and teaching methods. Combination of traditional and non-traditional teaching methods with the use of innovative technologies: lectures (overview / thematic); seminars / practical classes.

Evaluation methods:

– current control (testing, oral/written survey, solving legal problems, etc.);
- final control (exam).

Language of learning and teaching. Ukrainian

4.6. Name. MONITORING AND TESTING OF CYBER SECURITY SYSTEMS

Type. Compulsory

Year of study. 2024/2025.

Semester. II.

Lecturer, academic title, scientific degree, position. Y. Khokhlachova, Professor, PhD in Technical Sciences, Professor of the Department of Security of Information Technologies of the National Aviation University.

Learning outcomes. Analyze, develop and support the system of auditing and monitoring the effectiveness of the functioning of information systems and technologies, business/operational processes in the field of information and/or cyber security as a whole. Clearly and unambiguously communicate own conclusions on information security and/or cyber security issues, as well as the knowledge and explanations that substantiate them to staff, partners and others.

Compulsory previous academic subjects. "Security of information systems and networks", "Basics of cyber security".

Content. The subject of the discipline, its goals. Key Terms and Definitions. Organization of information protection in the system. The notion of monitoring. Characteristics and types of events during monitoring. Types of monitoring and main issues. Modern monitoring methods and technologies. Forecasting (prediction). General issues. Monitoring approaches and methods. Methods of testing cryptographic software systems. Basic principles of the testing process. Methodology for software quality assurance.

Recommended sources and other learning resources/tools.

5. 1. Хохлачова Ю.Є. Моніторинг та тестування систем кібербезпеки: лабораторний практикум / Ю.Є. Хохлачова, В.М. Кінзерявий, В.В. Погорелов та ін. К.: НАУ, 2022. 56 с.

6. Браіловський М.М., Зибін С.В., Пискун І.В., Хорошко В.О., Хохлачова Ю.Є. Технології захисту інформації. К.: ЦП «Компринт», 2021. 296 с.

7. Луцький М.Г., Хорошко В.О., Хохлачова Ю.Є., Козловський В.В., Баланюк Ю.В., Прав Ю.Г. Новітні технології захисту інформації: підручник. К.: НАУ, 2023. 312 с.

8. Пирцхалава Л.Г., Хорошко В.О., Хохлачова Ю.Є., Шелест М.Є. Інформаційно-аналітичне забезпечення безпеки. – Київ: ФЛП Ямчинський О.В. 2021. 470 с.

Planned educational activities and teaching methods. Combination of

traditional and non-traditional teaching methods with the use of innovative technologies: lectures (overview / thematic); seminars / practical classes.
Evaluation methods:
– current control (testing, oral/written survey, solving legal problems, etc.);
- final control (exam).
Language of learning and teaching. Ukrainian

4.7. Name. ETHICAL HACKING
Type. Compulsory
Year of study. 2024/2025.
Semester. II.
Lecturer, academic title, scientific degree, position. V.Zverev, Senior Researcher, PhD in Technical Sciences, Associate Professor of the Department of Software Engineering and Cyber Security.
Learning outcomes. Acquisition of theoretical knowledge and practical skills necessary for an information protection professional in the field of technologies for collecting information about computer systems, conducting audits and pentesting of information systems, planning and carrying out an attack on the protective mechanisms of operating systems and applications; working with tools for detecting vulnerabilities and performing security analysis of information systems.
Compulsory preliminary educational disciplines: "Security technologies of wireless and mobile networks", "Digital forensics", "Legal support of information security in economic systems".
Content. Hacking: concept, types and stages. Components of ethical hacking. Basic terms and concepts of hacking. Hacking certification. Phases of hacking (chain of cyber murder): preparation, penetration, distribution and entrenchment in the system, achievement of attack goals, covering traces. Targeted and ATP attacks. Techniques and tools of DoS/DDoS attacks. Attacks on Web applications. OWASP project. Methodology, tool and methods of collecting information. Collection of information without an explicit connection to the object of the attack (footprinting). Analysis of publicly available resources about the object of the attack. Google Toolkit: Google Hacking Database (GHDB). Collection of registration information. Methodology of collecting OSINT information. Network scanning algorithms and methods. Identification of network nodes. Identification of open ports. Scanning tools. Identification of services and applications. Identification of operating systems. Definition of network topology. Obtaining information from the DNS server database. Stealth scanning techniques and evasion of IDS intrusion detection systems. Spyware. Ways to infect systems. Ways to bypass antivirus protection. Rootkits, their

varieties, principles of operation, detection methods. Attacks on event registration mechanisms: cleaning of registration logs, distortion of audit results. Management of compromised systems (use of Trojans and backdoors). Hidden and open channels of interaction. Ways of hiding traces. Tools and techniques for selecting user credentials and passwords. Password protection audit methods. Analysis of the security of information systems. Search and exploitation of system vulnerabilities. Security scanners: Nessus Security Scanner and LANguard Network Security Scanner. Security audit of information systems. Penetration test performance standard and concept. Pentest types, techniques and phases. Preparation for the pentest: agreement on the performance of work, permission for testing. Data collection. Threat modeling. Vulnerability analysis and exploitation. Checking the resistance of systems to attacks. Certification of the system. Preparation of the report. Ethical hacking tools.

Recommended sources and other learning resources/tools.

1. Weidman G. Penetration Testing: A Hands-On Introduction to Hacking. – NY.: Press.Inc, 2014. – 478 p.
2. Jon Erickson, Hacking: The Art Of Exploitation, 2nd Edition. – San Francisco, 2008. – 475 p.
3. Інформаційна безпека: навчальний посібник. / Ю.Я. Бобало, І.В. Горбатий, М.Д. Кіселичник, А. П. Бондарєв та інші; за заг. ред. д-ра техн. наук, проф. Ю.Я. Бобала та д-ра техн. наук, доц. І.В. Горбатого. – Львів : Видавництво «Львівська політехніка», 2019. – 580 с.

Planned educational activities and teaching methods. The study of the discipline is conducted through lectures (auditory) and laboratory classes (in a computer classroom on a PC), which ensure the consolidation of theoretical knowledge and contribute to the assimilation of practical skills.

Evaluation methods.

– current control (computer testing, survey);
– final control (exam).

Language of learning and teaching. Ukrainian

4.8. Name. UI/UX DESIGN IN ENGLISH

Type. Optional

Year of study. 2024/2025, 2025/2026.

Semester. II-III.

Lecturer, academic title, scientific degree, position. N.Kotenko, Associate Professor, PhD in Education, Associate Professor of the Department of Software Engineering and Cyber Security**.**

Learning outcomes. A clear understanding of how the design process works. Basic knowledge in the field of UI/UX design. Practical skills in

using Figma tools to build wireframes, mockups and prototypes of software products according to the given task or formulated problem. Ability to perform interface testing.

Compulsory previous educational disciplines: "English for specific purposes", "Information technologies in professional activity".

Content. What is design and how does it work? How the design process is arranged. Methods and processes. What approaches exist. What approaches and when is better to use. Business needs research. Designer tools. How the software changed. Principles of working with Figma. Basics of the interface. Layout organization. Site elements. Styles, grids, and autolayouts. Visual design: fonts and typography. Collection of data from the customer. Analysis of competitors. Poll. Information architecture. Design system and UI kit. iOS, Android. Features and guidelines. Web analytics. Testing interfaces.

Recommended sources and other learning resources/tools.

1. Hill A. Complete figma tutorial for ui/ux: the comprehensive beginners to expert guide for learning and mastering FIGMA for UI/UX with pictures and illustrations. Independently Published, 2022.
2. Nielsen norman group: UX training, consulting, & research. Nielsen Norman Group. URL: https://www.nngroup.com/
3. Staiano F. Designing and Prototyping Interfaces with Figma: Learn essential UX/UI design principles by creating interactive prototypes for mobile, tablet, and desktop. Packt Publishing, 2022. 382 p.

Planned educational activities and teaching methods. The study of the discipline is conducted through lectures (auditory) and laboratory classes (in a computer classroom on a PC), which ensure the consolidation of theoretical knowledge and contribute to the assimilation of practical skills.

Evaluation methods.

– current control (computer testing, survey);
– final control (exam).

Language of learning and teaching. English

4.9. Name. ADMINISTRATION AND PROTECTION OF DATA STORAGES

Type. Optional

Year of study. 2024/2025, 2025/2026.

Semester. II-III.

Lecturer, academic title, scientific degree, position. S.Rzaeva, Associate Professor, PhD in Technical Sciences, Associate Professor of the Department of Software Engineering and Cyber Security.

Learning outcomes. Formation of theoretical knowledge and practical skills necessary for the analysis of the effectiveness of the selected data storage protection system, justification of the choice of technical and software tools for effective administration and protection of data storage; ensuring the reliability of the operation of data warehouses, taking into account the factors of user error.

Compulsory previous educational disciplines: "Cloud and GRID technologies", "Technologies of designing information systems".

Content. Concept of database, data warehouse, database system. Characteristics and classification of OLTP systems, OLAP systems. General characteristics of data warehouses (Data Warehouse). Types of data storage systems: MOLAP (Multidimensional), ROLAP (Relational), HOLAP (Hybrid). Characteristics of the multidimensional data model. Software data storage tools: tools for integrating heterogeneous databases, data storage management tools, data analysis tools (Data Mining), tools for visualization of processing results. Creation of data windows (Data Mart). Means of protection of data warehouses (Data Warehouse). General characteristics of NoSQLTP systems, OLAP systems. data management systems. Means of protection of NoSQLTP systems, OLAP systems. data management systems. General characteristics of NewSQL TP systems, OLAP systems. data management systems. Means of protection NewSQLTP - systems, OLAP - systems. data management systems. General characteristics of cloud data management systems. Means of protection of cloud data management systems. Protecting data lakes.

Recommended sources and other learning resources/tools.

1. Демиденко М.А. Введення в сучасні бази даних : навч. посіб. / М.А. Демиденко. – Д. : НТУ «Дніпровська політехніка, 2020. – 38 с.
2. Пасічник В.В. Сховища даних: підручник. / В.В. Пасічник, Н.Б. Шаховська – Л. : Магнолія, 2021. – 496 с.
3. Matt How The Modern Data Warehouse in Azure: Building with Speed and Agility on Microsoft’s Cloud Platform. – Apress; 1st ed. edition (June 16, 2020), 304 p.

Planned educational activities and teaching methods. The study of the discipline is conducted through lectures (auditory) and laboratory classes (in a computer classroom on a PC), which ensure the consolidation of theoretical knowledge and contribute to the assimilation of practical skills.

Evaluation methods.

– current control (computer testing, survey);

– final control (exam).

Language of learning and teaching. Ukrainian

4.10. Name. MOBILE APPLICATIONS SECURITY
Type. Optional
Year of study. 2024/2025, 2025/2026.
Semester. II-III.
Lecturer, academic title, scientific degree, position. T.Zhirova, PhD in Education, Associate Professor of the Department of Software Engineering and Cyber Security.
Learning outcomes. Formation of theoretical knowledge and practical skills on the following issues: main threats to mobile software; protection of information in mobile OS; Apple iOS security; Google Android security; mobile application security testing.
Compulsory previous academic subjects. "Information technologies in professional activity", "WEB-design and WEB-programming", "Basics of cyber security".
Content. Introduction. The history of the development of mobile applications and their classification. Information protection in mobile OS. General principles of security and data privacy of mobile devices. Apple iOS security. Apple iOS security enhancements. Google Android Security. Techniques for bypassing user data protection and improving Android security. Mobile application security testing. Mobile application security testing tools. Automation of mobile application security testing.
Recommended sources and other learning resources/tools.
1. Шматко О.В. Аналіз методів і технологій розробки мобільних додатків для платформи Android: навч. посіб. / О.В. Шматко, А.О. Поляков, В.М. Федорченко. – Харків: НТУ «ХПІ», 2018. – 284 с.
2. Бурячок В.Л. Технології забезпечення безпеки мережевої інфраструктури. Підручник. / В.Л. Бурячок, А.О. Аносов, В.В. Семко, В.Ю. Соколов, П.М. Складанний. – К.: КУБГ, 2019. – 218 с.
Planned educational activities and teaching methods. A combination of traditional and non-traditional teaching methods with the use of innovative technologies: lectures (thematic, problem-based); laboratory classes using modern interactive technologies (traditional, modeling situations); individual work; consultations
Evaluation methods:
– current control (computer testing, survey);
– final control (exam).
Language of learning and teaching. Ukrainian

4.11. Name. INTERNET OF THINGS TECHNOLOGY SECURITY

Type. Optional
Year of study. 2024/2025, 2025/2026.
Semester. II-III.
Lecturer, academic title, scientific degree, position. L.Vlasenko, Associate Professor, PhD in Technical Sciences, Associate Professor of the Department of Software Engineering and Cyber Security.
Learning outcomes. Formation of theoretical knowledge and practical skills on the following issues: generally recognized technologies and standards for ensuring IoT security, security of IoT equipment, security of cloud technologies in IoT, security in the digital world based on IoT.
Compulory previous academic subjects. "Information technologies in professional activity", "Basics of cyber security".
Content. Introduction. Introduction. Digital transformation of business. Commonly recognized technologies and standards for IoT security. The hardware part of the Internet of Things. Security of IoT equipment. Application of automation in IoT. Application of Big Data to support IoT devices. Applying AI and ML, basic programming to support IoT devices. Application of cloud technologies in IoT. Security in the digital world based on IoT. Principles of secure connection of the "Internet of Things" to the network. Examples of secure connection of IoT devices.
Recommended sources and other learning resources/tools.
1. Hanes D. IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things. 1st ed. Cisco Press, 2017. 576 p.
2. Бурячок В.Л. Технології забезпечення безпеки мережевої інфраструктури. Підручник. / В.Л. Бурячок, А.О. Аносов, В.В. Семко, В.Ю. Соколов, П.М. Складанний. – К.: КУБГ, 2019. – 218 с.
Planned educational activities and teaching methods. A combination of traditional and non-traditional teaching methods with the use of innovative technologies: lectures (thematic, problem-based); laboratory classes using modern interactive technologies (traditional, modeling situations); individual work; consultations

Evaluation methods:
– current control ((computer testing, survey);
– final control (exam).
Language of learning and teaching. Ukrainian

4.12.Name. BIOMETRIC AUTHENTICATION TECHNOLOGIES IN INFORMATION SYSTEMS
Type. Optional
Year of study. 2024/2025, 2025/2026.

Semester. II-III.
Lecturer, academic title, scientific degree, position. T.Franchuk, PhD in Economics, Senior Lecturer of the Department of Software Engineering and Cyber Security.
Learning outcomes. Studying the basic provisions of modern biometric technologies, mastering the methods and methodologies of creating biometric authentication systems, which allow to increase the reliability of the functioning of complex information systems.
Compulsory previous educational disciplines: "Methods and means of information protection in computer systems", "Security of information systems and networks".
Content. Biometrics, biometric technologies: basic concepts and definitions. Legal basis of application of biometric technologies in information protection. Biometric protection systems, interaction with other systems. Software tools of biometric technologies. Methods of authentication of biometric systems. Modern types of biometric technologies, positive and negative aspects of the application of each of them. Fields of application of biometric systems. Application of biometric technologies to protect modern data transmission systems. The main directions of the development of biometric technologies.
Recommended sources and other learning resources/tools.
1. Царьов Р.Ю. Біометричні технології: навч. посіб. / Р.Ю. Царьов, Т.М. Лемеха. – Одеса: ОНАЗ ім. О.С. Попова. – 2016. – 140 с.
2. Корченко О. Методологія розроблення нейромережевих засобів інформаційної безпеки Інтернет-орієнтованих інформаційних систем: навч. посіб. / О. Корченко, І. Терейковський, А. Білощицький. – К.: ТОВ «Наш Формат». − 2016. – 249 с.
3. Тарнавський Ю.А. Технології захисту інформації: підручник. – К.: КПІ ім. Ігоря Сікорського. – 2018. – 162 с.
Planned educational activities and teaching methods. The study of the discipline is carried out through lectures (auditorium) and laboratory classes (in a computer class on a PC), which ensure the consolidation of theoretical knowledge and the mastery of biometric authentication technologies.
Evaluation methods:
– current control (computer testing, survey, independent work check);
– final control (exam).
Language of study and teaching: Ukrainian.

4.13. Name. BUSINESS INTELLIGENCE TOOLS
Type. Optional.
Year of study. 2024/2025, 2025/2026.

Semester. II-III.
Lecturer, academic title, scientific degree, position. A.Roskladka, Professor, Doctor of Sciences (Economics), Head of the Department of Digital Economy and System Analysis.
Learning outcomes. Knowledge of the basic algorithmic elements of the R language, data types, data import and export procedures in the RStudio environment, technologies for working with large and distributed data, graphics and data visualization in R, descriptive data statistics. Practical skills to conduct regression, dispersion, factor, cluster business analysis using R language tools.
Compulsory previous academic subjects. "Higher mathematics", "Computer discrete mathematics", "Number theory", "Information technologies in professional activity".
Content. Basic concepts of analytics. Analytical data. Types of analytics. The main components of the R environment. The graphical interface of RStudio. Designing analytical web applications using the Shiny package. Creation of a set of business data. R data types and how to work with them. Methods of working with missing data. Import data from the Internet. Basics of data management in R. Descriptive analytics. Intelligence analytics. Choice of data visualization form. Inductive analytics. Predictive analytics. Analysis of variance. Correlation analysis. Factor analysis. Diagnostics of the data model**.**
Recommended sources and other learning resources/tools.
1. Майборода Р. Є., Сугакова О. В. Аналіз даних за допомогою пакета R: навчальний посібник. – К.: ВПЦ «Київський університет», 2015. – 65 с.
2. Kabacoff R. R in Action. Data analysis and graphics with R. – Manning: Shelter island, 2015. – 608 p.
3. Matloff N. Probability and Statistics for Data Science: Math + R + Data. – London: Chapman & Hall, 2019. – 376 p.
Planned educational activities and teaching methods. A combination of traditional and non-traditional teaching methods with the use of innovative technologies: lectures (thematic, problem-based); laboratory classes (traditional, work in small groups).
Evaluation methods.
– current control (inspection of individual tasks, testing);
– final control (exam).
Language of learning and teaching. Ukrainian

4.14. Name. INTELLECTUAL PROPERTY
Type. Optional.

Year of study. 2024/2025, 2025/2026.
Semester. II-III.
Lecturer, academic title, scientific degree, position. N.Daraganova, Professor, Doctor of Sciences (Law), Professor of the Department of Administrative, Financial and Information Law; A.Gurzhii, Associate Professor, PhD in Law, Associate Professor of the Department of Administrative, Financial and Information Law.
Learning outcomes. Acquaintance with the norms of international and national legislation in the field of intellectual property; mastering the legal mechanisms of registration, implementation and protection of intellectual property rights. Formation of skills to carry out professional activities, as well as practical application of regulatory and legal acts. The ability to realize one's rights and responsibilities as a member of society, to be aware of the values of civil (democratic) society, the rule of law, the rights and freedoms of a person and a citizen in Ukraine. The ability to associate oneself as a member of civil society, to understand and be able to use one's own rights and freedoms, to show respect for the rights and freedoms of others.
Compulsory previous academic subjects. "Science of law".
Content. Concept of intellectual property, objects and subjects of intellectual property. Concepts, principles and sources of copyright; objects and subjects of copyright; personal non-property and property rights to works of literature, art and science; collective management of copyrights; liability for copyright infringement. Legal protection of related rights. Concepts and conditions of legal protection of inventions, utility models, industrial designs. Legal protection of non-traditional intellectual property results. Legal protection of means of individualization of subjects of economic turnover, goods, works and services. Concept and legal protection of commercial (brand) names; trademark and geographical meanings. Protection against unfair competition. Liability for infringement of intellectual property rights.
Recommended sources and other learning resources/tools.
1. Право інтелектуальної власності: підручник / за заг. ред. О.І. Харитонова. – К.: Юрінком Інтер, 2019. – 540 с.
2. Інтелектуальна власність: навч. посібн. / за ред. О.В. Нестерцової-Собакарь. – К.: Дніпро, 2018. – 140 с.
3. Право інтелектуальної власності: підручник. / О.І. Харитонова, Є.О. Харитонов, Т.С. Ківалова, В.С. Дмитришин, О.О. Кулініч, Л.Д. Романадзе та ін. за заг. ред. О.І. Харитонової, 2018. – К.: Юрінком Інтер. – 367 с.

Planned educational activities and teaching methods. A combination of traditional and non-traditional teaching methods with the use of innovative technologies: lectures (overview, thematic, problem-based), practical classes (presentation, discussion, communicative method, case-study method, individual tasks, etc.).

Evaluation methods:

– current control (testing, oral/written survey, solving legal problems, etc.);

– final control (exam).

Language of learning and teaching. Ukrainian

4.15. Name. INFORMATION TECHNOLOGIES IN THE SYSTEM OF ENSURING THE ECONOMIC SECURITY OF THE STATE

Type. Optional.

Year of study. 2024/2025, 2025/2026.

Semester. II-III.

Lecturer, academic title, scientific degree, position. V.Tokar, Professor, Doctor of Sciences (Economics), Professor of the Department of Software Engineering and Cyber Security.

Learning outcomes. As a result of studying the discipline, students should know: the content of the main concepts of the course: "security", "economic security", "economic security of the state", etc.; basic principles and concepts of ensuring the economic security of the state using information technologies; basic methods of assessment and analysis of threats to economic security at the micro, macro and global levels; basic methods and techniques for calculating the threshold values of indicators of economic security of the state; principles of formation and strategies for ensuring economic security with the use of information technologies at the national, regional and global levels; methodological approaches to the analysis and assessment of the level of economic security at the micro, macro and global levels; must be able to: search for and process information about threats to economic security at the micro, macro, and global levels; apply mathematical methods for data analysis and processing in order to assess the level of economic security of the state; conduct an analysis of the economic security of the state by individual components; use existing software solutions to simplify calculations.

Compulsory previous academic subjects. "Information technologies in professional activity", "Object-oriented programming", "WEB-design and WEB-programming".

Content. The relationship between the concepts of risk and threat. Threat classification The genesis of the notion of security. The notion of economic security. Hierarchy of the notion of economic security. Components of

economic security. Concept economic security of the state. Components of the state's economic security. State macroeconomic security. Foreign economic security of the state. Scientific and technological security of the state. Energy security of the state. Social security of the state. Demographic security of the state. Food security of the state. Industrial safety of the state. The essence of financial security. Components of financial security. Levels of financial security. The concept of global financial security. Global tax evasion. Global Shadow Financial Sector. Offshore schemes. Schemes for financing money laundering and terrorist financing. The concept of the indicator of economic security of the state. Classification of indicators of the state's economic security. Threshold values. An integral indicator of the state's economic security. Expert methods of assessing the level of the state's economic security. Correlation-regression analysis in assessing the economic security of the state. Indicative method of assessing the economic security of the state. The system of ensuring economic security. The essence of the system of ensuring the economic security of the state. The structure of the system of ensuring the economic security of the state. Entities ensuring the economic security of the state. Methods of minimizing and neutralizing threats to the economic security of the state. The notion of economic security of Ukraine. Assessment of the level of provision of the components of Ukraine's economic security.

Recommended sources and other learning resources/tools.

1. Остапов С.Е. Технології захисту інформації: навч. посібник. / С.Е. Остапов, С.П. Євсеєв, О.Г. Король. – Чернівці. – Видавничий дім «Родовід», 2014. – 471 с.
2. Пількевич І.А. Захист інформації в автоматизованих системах управління: навч. посібник. / І.А. Пількевич, Н.М. Лобанчикова, К.В. Молодецька. – Житомир: Вид-во ЖДУ ім. І. Франка, 2015. – 226 с.
3. Хорошко О. В. Захист систем електронних комунікацій: навч. посіб. / В.О. Хорошко, О.В. Криворучко, М.М. Браіловський та ін. – Київ: КНТЕУ, 2019. – 164 с.

Planned educational activities and teaching methods. The study of the discipline is conducted through lectures (auditory) and laboratory classes (in a computer classroom on a PC), which ensure the consolidation of theoretical knowledge and contribute to the assimilation of practical skills.

Evaluation methods:

– current control (testing, scientific report, synopsis check, survey, control work);
– final control (exam).

Language of learning and teaching. Ukrainian, English.

4.16. Name. IT LAW
Type. Optional.
Year of study. 2024/2025, 2025/2026**.**
Semester. II-III.
Lecturer, academic title, scientific degree, position. V.Timashov, Associate Professor, Doctor of Sciences (Law), Professor of the Department of Administrative, Financial and Information Law.
Learning outcomes. Formation of professional knowledge and skills in the application of legal norms regulating relations between participants in the IT sphere.
Compulsory previous academic subjects. "Science of law".
Content. The concept of IT law, its scope and structure. Legal features of opening an IT business in Ukraine. Opening of IT companies in Ukraine. Goals and limitations of international IT business structuring. Legislative regulation of electronic commerce in Ukraine. Legal responsibility for using unreliable information on the Internet. The procedure for registering a copyright on a computer program. Copyrights in the creation of computer code and software. Contractual legal relations in the field of IT Law. Legal regulation of a startup in Ukraine. Confidentiality and ways to protect commercial secrets under the DNA contract. Ensuring the right to privacy when using information technologies. Legal problems of regulating relations in social networks. International legislation in the field of intellectual property protection.
Recommended sources and other learning resources/tools.
1. Основи ІТ-права: навчальний посібник / Т.В. Бачинський, Р.І. Радейко, О.І. Харитонова та ін.; за заг. ред. Т.В. Бачинського. 2-ге вид., допов. і перероб. – К.: Юрінком Інтер, 2019. – 208 с.
2. Бачинський Т. Основи ІТ-права. Навчальний посібник. – Львів: Апріорі, 2018. – 36 с.
3. Кульчій О.О. Інформаційне право: навч.-метод. посіб. / О.О. Кульчій. – Полтава: ВНЗ Укоопспілки «ПУЕТ», 2018. – 193 с.
Planned educational activities and teaching methods. Combination of traditional and non-traditional teaching methods with the use of innovative technologies: lectures (overview); seminar and practical classes (training / presentation / discussion / simulation of situations / work in small groups / other); individual work.
Evaluation methods:
– current control (testing, oral / written survey, checking the prepared essay / etc.);
– final control (exam).
Language of learning and teaching. Ukrainian

4.17. Name. COMMERCIAL INTELLIGENCE AND ENTERPRISE INTERNAL SECURITY

Type. Optional.

Year of study. 2024/2025, 2025/2026.

Semester. II-III.

Lecturer, academic title, scientific degree, position. O.Koryagina, Associate Professor, PhD in Law, Associate Professor of the Department of Legal Support of Business Security.

Learning outcomes. Formation of students' knowledge of the basics of commercial intelligence and detective activities, intelligence and counter-intelligence support of business activities.

Compulsory previous academic subjects. "Science of law".

Content. Commercial intelligence as an element of information provision of entrepreneurial activity. Commercial Intelligence Objects and Sources. Informational research work. Reconnaissance Operations. Intelligence provision of commercial operations. Intelligence support of competitive struggle. Intelligence support of the financial and economic activity of the enterprise, bank. The basics of detective activity. End of the table. Ensuring internal security of the enterprise. Internal threats to the enterprise. Organization of internal security at the enterprise. The work of the security forces of the enterprise with its personnel

Recommended sources and other educational resources/tools.

1. Конкурентна розвідка: навчальний посібник. Копотун І. М., Падалка А. М., Кузьмічова-Кисленко Є. В. та ін. Ірпінь: Університет ДФС України, 2020. 188 с. (Серія «На допомогу студенту УДФСУ», т. 74).
2. Про охоронну діяльність: Закон України від 22.03.2012 // Відомості Верховної Ради України. 2012. № 30. Ст.260 (із змінами і допов.).
3. Про оперативно-розшукову діяльність: Закон України від 18.02.1992 // Відомості Верховної Ради України. 1992. N 22. Ст.303. (із змінами і допов.).

Planned educational activities and teaching methods. A combination of traditional and non-traditional teaching methods with the use of innovative technologies: Lectures (overview / thematic), seminars / practical, case studies, independent work, consultations.

Evaluation methods:

– current (surveys, written works, situational tasks);
– final (exam).

Language of learning and teaching. Ukrainian

4.17. Name. PSYCHOLOGY OF ADAPTATION

Type. Optional.
Year of study. 2023/2024, 2024/2025.
Semester. II-III.
Lecturer, academic title, scientific degree, position.. M.Korolchuk., Professor, Doctor of Sciences (Psychology), Professor of the Department of Psychology.
Learning outcomes. Formation of a system of knowledge regarding the use of adaptive capabilities of the individual to ensure the preservation of working capacity and health and effective and safe activities of specialists.
Compulsory previous academic subjects. "Psychology".
Content. Theoretical and methodological foundations of adaptation psychology. Types, types, dynamics, criteria and limits of adaptive capabilities of specialists. Biological adaptation. Levels of socio-psychological adaptation. Protective mechanisms and adaptive strategies of personality. The contents of professional adaptation. The problem of adaptation of a specialist to extreme operating conditions. Psychological support for optimization of the adaptive capabilities of the individual. Peculiarities of students' adaptation and psychological methods of its optimization to the conditions of professional and educational activities.
Recommended sources and other educational resources / tools.
1. Корольчук М.С. Психофізіологія діяльності: Підручник для студ. вищих навчальних закладів. – К.: Ельга, Ніка-Центр, 2012. – 400 с.
2. Психологія праці в звичайних та екстремальних умовах: навч. посіб. / М.С. Корольчук, В.М. Корольчук, С.М. Миронець, Г. М. Ржевський та ін. – К.: КНТЕУ, 2015. – 652 с.
3. Практична психологія. Навчальний посібник для студентів ВНЗ / Корольчук М.С., Корольчук В.М., Ржевський Г.М., Миронець С.М., Осьодло В.І., Зазимко О.В. – К. : КНТЕУ, 2014. – 728 с.
Planned educational activities and teaching methods.
A combination of traditional and non-traditional teaching methods with the use of innovative technologies: lectures (overview, thematic, problem-based, lecture-conferences, lecture-discussions); practical classes (trainings, presentations, discussions, work in small groups, modeling situations, case studies).
Evaluation methods.
– current control (testing, oral / written survey, etc.);
– final control (exam).
Language of learning and teaching. Ukrainian

4.19. Name. BUSINESS PSYCHOLOGY
Type. Optional.

Year of study. 2024/2025, 2025/2026.
Semester. II-III.
Lecturer, academic title, scientific degree, position. I.Ovdienko, PhD in Psychology, Associate Professor of the Department of Psychology, I.Yevchenko, PhD in Psychology, Associate Professor of the Department of Psychology.
Learning outcomes. To know the main areas of research and tasks of business psychology, to understand its interdisciplinary nature, its structure and connection with other sciences; to have the basic concepts of business psychology, methods and approaches to conducting socio-psychological research in the business sphere.
Compulsory previous academic subjects. "Psychology", "Management Psychology", "Philosophy".
Content. Basic concepts, methodology, methods, tasks and principles of business psychology. Psychological sources, factors, mechanisms and regularities of the development of business as a system, as well as psychological factors of the emergence of crisis phenomena in economic relations. Psychological prerequisites of business activity formation. Process of formation of entrepreneurial motivation; professionally important psychological and psychophysiological qualities of a businessman; socio-psychological factors of successful business management. The main directions and approaches in the assessment of professional and business qualities of a businessman; basics of recruitment and promotion of personnel. The main moral and ethical problems of modern business representatives. The role and significance of communication processes in the activity of an entrepreneur; the psychological importance of business communication in achieving success, the psychology of decision-making in a difficult situation.
Recommended sources and other educational resources / tools.
1. Гура Т., Романовський О., Книш А. Психологія лідерства в бізнесі: Навчальний посібник / Т. Гура, О. Романовський, А. Книш. – Харків : «Друкарня Мадрид», 2017. – 100 с.
2. Гусєва О. Ю., Легомінова С. В., Воскобоєва О. В., Ромащенко О. С., Хлевицька Т. Б. Психологія підприємництва та бізнесу: Навчальний посібник. – К.: Держ. ун-т телекомунікацій, 2019. – 257с.
3. Мілютіна К. Л., Трофімов А. Ю. Психологія сучасного бізнесу: Навчальний посібник. – К.: Видавництво Ліра-К, 2020. – 168 с.
Planned educational activities and teaching methods.
A combination of traditional and non-traditional teaching methods with the use of innovative technologies: lectures (overview, thematic, problem-

based, lecture-conferences, lecture-discussions); practical classes (trainings, presentations, discussions, work in small groups, simulation of situations).
Evaluation methods:
– current control (oral testing / written survey; verification of the prepared essay / review / report / presentation / situational tasks, etc.);
– final control (written exam).
Language of learning and teaching. Ukrainian

4.20. Name. STOCHASTIC METHODS IN ECONOMICS
Type. Optional.
Year of study. 2024/2025, 2025/2026 .
Semester. II-III.
Lecturer, academic title, scientific degree, position. V.Gamalii, Professor, Doctor of Sciences (Physics and Mathematics), Professor of the Department of Digital Economy and System Analysis.
Learning outcomes. Gaining theoretical knowledge and acquiring practical skills of quantitative analysis and stochastic mathematical modeling of economic processes.
Compulsory previous academic subjects. "Higher mathematics", "Number theory", "Economic theory".
Content. Introduction to the theory of random processes. Probabilistic economic models using homogeneous Markov chains. Setting of stochastic optimal planning problems. Probabilistic models of the simplest economic systems. Analytical method of stochastic economic model research. Methods of economic and mathematical analysis of applied stochastic models of the economy.
Recommended sources and other educational resources / tools.
1. Лукяненко І.Г., Семко Р.Б. Динамічні стохастичні моделі загальної рівноваги: теорія побудови та практика використання у фінансових дослідженнях: І.Г. Лукяненко, Р.Б. Семко. Навчальний посібник. – К.: НУ «Києво-Могилянська академія», 2015. – 248 с.
2. Козак Ю.Г. Математичні методи та моделі для магістрів з економіки. Практичне застосування. Навч. посіб. / Ю.Г. Козак, В.М. Мацкул. – К.: Центр учбової літератури, 2017. – 254 с.
3. Шамровський О.Д. Системний аналіз: математичні методи та застосування. Навчальний посібник / О.Д. Шамровський. – Львів: Магнолія 2006. – 2021. – 275 с.
Planned educational activities and teaching methods. A combination of traditional and non-traditional teaching methods with the use of innovative technologies: lectures (thematic, problem-based); practical training.
Evaluation methods:

– current control (testing; oral and written survey);
– final control (exam).
Language of learning and teaching. Ukrainian

4.21. Name. DATA ANALYSIS TECHNOLOGIES
Type. Optional.
Year of study. 2024/2025, 2025/2026.
Semester. II-III.
Lecturer, academic title, scientific degree, position. A.Roskladka, Professor, Doctor of Sciences (Economics), Head of the Department of Digital Economy and System Analysis.
Learning outcomes. Knowledge of the main sections of data science. Knowledge of data processing procedures: consolidation, transformation, cleaning, data enrichment; designing the structure of data warehouses and OLAP systems; models and methods of intelligent data analysis: association, clustering, classification, regression, forecasting, data visualization; modern data analysis software. Practical skills to conduct data analysis for the discovery of knowledge, to build and research systems of intelligent data analysis when solving applied problems using modern analytical platforms Tableau and Microsoft Power BI.
Compulsory previous academic subjects. "Computer discrete mathematics", "Higher mathematics", "Number theory".
Content. Data Science. Data consolidation. Data transformation. Search for associative rules (Rules Mining). Cluster analysis of data. Visual data analysis (Visual Mining). Analysis of text information (Text Mining). Internet data analysis (Web Mining). Data analysis in real time (Real Time Data Mining). Software analytical platforms.
Recommended sources and other learning resources/tools.1. Гладун А.Я. Data mining: пошук знань в даних. Посібник. / А.Я. Гладун, Ю. В. Рогушина. – Київ: АДЕФ-Україна, 2016. – 451 с.
2. Олійник А.О. Інтелектуальний аналіз даних: навч. посібн. / А.О. Олійник, С.О. Субботін, О.О. Олійник. – Запоріжжя: ЗНТУ, 2012. – 278 с.
3. Cuesta H., Kumar S. Practical Data Analysis.Birmingham: Packt Publishing Ltd, 2016. – 316 p.
Planned educational activities and teaching methods. A combination of traditional and non-traditional teaching methods with the use of innovative technologies: lectures (thematic, problem-based); laboratory classes (traditional, work in small groups).
Evaluation methods:
– current control (inspection of individual tasks, testing);

– final control (exam).
Language of learning and teaching. Ukrainian

4.22. Name. PHILOSOPHY OF PERSONALITY
Type. Optional.
Year of study. 2024/2025, 2025/2026.
Semester. II-III.
Lecturer, academic title, scientific degree, position. A.Morozov, Professor, Doctor of Sciences (Philosophy), Professor of the Department of Philosophy, Sociology and Political Science.
Learning outcomes. The formation of the philosophical self-awareness of the personality of a specialist psychologist, the ability of theoretical research and generalization of historical, socio-cultural, ideological and axiological foundations of the formation and development of the personality.
Compulsory previous academic subjects. "Philosophy", "Psychology".
Content. The human problem in ancient philosophy. Understanding the personality in the philosophical quests of the Christian Middle Ages. Interpretations of the human phenomenon in modern and postmodern paradigms of thinking. Existential dimensions of personality. Mystical personal experience, peak experiences and the importance of intuition in spiritual life. Consciousness, the unconscious, the brain: problems of genesis and development. Meaning and values in being a person. Humanism and trans-humanism: issues of gender and cloning.
Recommended sources and other learning resources/tools.
1. Бауман З. Актуальність Голокосту. Посібник. – К., Логос, 2018. – 316 с.
2. Франкл В. Людина в пошуках справжнього сенсу. Посібник. – К., Основи, 2017. – 360 с.
3. Морозов А.Ю. Зло: метафізичні і богословські виміри. Посібник. – К., КНТЕУ, 2018. – 256 с.
Planned educational activities and teaching methods. Activities: visiting the Ukrainian National Museum of Fine Arts. General methods: the combination of the logical and historical, the method of identity-opposites. Conducting lectures, seminars using multimedia technologies.
Evaluation methods:
– current control (computer testing, survey); modular (computer testing, control work);
– final control (exam).
Language of learning and teaching. Ukrainian

4.23. Name. FUNCTIONAL AND LOGIC PROGRAMMING

Type. Optional.
Year of study. 2024/2025, 2025/2026.
Semester. II-III.
Lecturer, academic title, scientific degree, position. T.Savchenko, Associate Professor, PhD in Technical Sciences, Associate Professor of the Department of Software Engineering and Cyber Security.
Learning outcomes. Formation of the ability to algorithmic and logical thinking; motivated to choose programming languages and development technologies to solve the tasks of creating and maintaining software; theoretical knowledge and practical skills necessary for mastering the basics of functional and logical programming and solving complex and informal problems found in real economic, organizational and production systems, as well as problems of artificial intelligence using the Lisp and Prolog languages.
Compulsory previous academic subjects. "Object-oriented programming", "Databases", "Expert systems".
Content. Dominant programming paradigms. The concept of functional programming. General understanding of functional programming and its application. Elementary LISP. Construction of lists. Numerical functions. Management structures. The concept of recursion. Functional. Logical programming concept. Application areas of the Prolog language. Visual Prolog language features. Visual Prolog facts and rules. Concept of arguments and predicates. Assignment of queries in Prolog. Use of high-level programming languages for building expert systems.
Recommended sources and other learning resources/tools.
1. Заяць В.М. Логічне і функціональне програмування. Системний підхід: підруч. / В.М. Заяць, М.М. Заяць. – Рівне: НУВГП, 2018. – 421 с.
2. Месюра В. І. Функціональне та логічне програмування: посіб. / В. І. Месюра, Н. В. Лисак, О. І. Суприган – Вінниця : ВНТУ, 2011. – 105 с.
3. Бадаєв Ю. І. Функціональне програмування : навч. посіб. / Ю.І. Бадаєв та ін. – К. : НТУУ «КПІ», 2012. – 135 с.
Planned educational activities and teaching methods.
Lectures, laboratory classes, independent work.
Evaluation methods:
– current control (survey, testing);
– final control (exam).
Language of learning and teaching. Ukrainian

CONTENT