МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ СЕМЕНА КУЗНЕЦЯ

"ЗАТВЕРДЖУЮ"
Проректор з навчально-методичної роботи
_____
Каріна НЕМАЩКАЛО

ВСТУП ДО ФАХУ
робоча програма навчальної дисципліни

Галузь знань	***12 Інформаційні технології***
Спеціальність	***125 Кібербезпека***
Освітній рівень	***перший (бакалаврський)***
Освітня програма	***Кібербезпека***

Статус дисципліни	***обов'язкова***
Мова викладання, навчання та оцінювання	***українська***

Завідувач кафедри
кібербезпеки та
інформаційних технологій _____ *Ольга СТАРКОВА*

Харків
2022

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
SIMON KUZNETS KHARKIV NATIONAL UNIVERSITY OF ECONOMIC

"APPROVED"
Vice-rector for educational and methodical work

Karina NEMASHKALO

INTRODUCTION TO SPECIALTY

working program of the educational discipline

Branch of knowledge	***12 Information technologies***
Specialty	***125 Cybersecurity***
Educational level	***first (bachelor's))***
Educational program	***Cybersecurity***

Discipline status	***basic***
Language of instruction, teaching and assessment	***English***

Head of Department
cybersecurity and
information technology *Olha Starkova*

Kharkiv
2022

APPROVED
at a meeting of the Department of Cybersecurity and Information Technology
Protocol № 1 dated August 27, 2022

Developers:
Shapovalova Olena, Ph.D., Assoc. Prof. of the Department of KIT

Update and re-approval letter
working program of the discipline

Academic year	Date of the meeting of the department-developer of WPD	Protocol number	Signature of the head of the department

Abstract of the academic discipline

The task of the educational discipline "Introduction to specialty " is the formation of skills and competencies in the field of detection and identification of cyber threats, development and application of information protection methods in case of cyber attacks.

The educational discipline "Introduction to specialty " belongs to the mandatory educational components of the cycle of professional training of bachelors in the specialty "Cybersecurity", which familiarizes students with the basics of the profession and briefly characterizes threats and methods and means of their detection and elimination.

The subject of study of the discipline is basic definitions and concepts of cyber security, vulnerabilities of information systems, sources of threats, methods of their elimination, security policies.

The objects of study are threats and cyber-attacks, malicious software, methods of blocking unauthorized access attempts and countering attacks.

The purpose of the study discipline "Introduction to specialty " is to provide students with higher education with theoretical knowledge and practical skills in static and dynamic analysis of malicious software, identification of the type of attacks based on a number of signs, mastering the main approaches and principles of information preservation and acquiring skills in their application for the protection of information systems .

The results of the study of the discipline are systematic knowledge and practical skills in the field of detection and identification of threats and the choice of methods of prevention and countermeasures in case of threat realization.

Characteristics of the discipline

Course	**1**
Semester	**1**
Number of ECTS credits	**6**
Final control form	**credit**

Structural and logical scheme of studying the discipline

Prerequisites	Postrequisites
Computer science according to the school program	**Object-oriented programming**
Mathematics according to the school program	**Development and analysis of algorithms**

Competences and learning outcomes in the discipline

Competences	Learning outcomes
CG 1. Ability to apply knowledge in practical situations. CG 2. Awareness and understanding of the subject area and the profession. CG 3. Ability to communicate professionally in national and foreign languages, both orally and in writing.	LO1 – to apply knowledge of state and foreign languages in order to ensure the effectiveness of professional communication;
CG 1. Ability to apply knowledge in practical situations. CG 2. Awareness and understanding of the subject area and the profession. CG 4. Ability to identify, pose and solve problems in a professional direction. CG 5. Ability to search, process and analyze information.	LO 2 – to organize one's own professional activity, to choose optimal methods and ways of solving complex specialized tasks and practical problems in professional activity, to evaluate their effectiveness;

CG 1. Ability to apply knowledge in practical situations. CG 2. Awareness and understanding of the subject area and the profession. CG 4. Ability to identify, pose and solve problems in a professional direction. CG 5. Ability to search, process and analyze information.	LO 3 – to use the results of independent search, analysis and synthesis of information from various sources for the effective solution of specialized tasks of professional activity;
CG 1. Ability to apply knowledge in practical situations. CG 2. Awareness and understanding of the subject area and the profession. CG 4. Ability to identify, pose and solve problems in a professional direction. CG 5. Ability to search, process and analyze information.	LO 4 – to analyze, argue, make decisions when solving complex specialized tasks and practical problems in professional activities, which are characterized by complexity and incomplete determination of conditions, to be responsible for the decisions made;
CG 2. Awareness and understanding of the subject area and the profession. CG 4. Ability to identify, pose and solve problems in a professional direction. CG 5. Ability to search, process and analyze information.	LO 5 – to adapt in conditions of frequent changes in the technologies of professional activity, predict the final result;
CG 2. Awareness and understanding of the subject area and the profession.	LO 6 – to critically comprehend main theories, principles, methods and concepts in education and professional activity;
CG 2 . Awareness and understanding of the subject area and the profession. CG 4. Ability to identify, pose and solve problems in a professional direction. CS 1. Ability to apply the legislative and regulatory framework, as well as state and international requirements, practices and standards in order to carry out professional activities in the field of information and/or cyber security.	LO 7 – to act on the basis of the legislative and regulatory framework of Ukraine and the requirements of the relevant standards, in particular international in the field of information and/or cyber security;
CG 2 . Awareness and understanding of the subject area and the profession. CG 4. Ability to identify, pose and solve problems in a professional direction. CS 1. Ability to apply the legislative and regulatory framework, as well as state and international requirements, practices and standards in order to carry out professional activities in the field of information and/or cyber security.	LO 8 – to prepare proposals for normative acts on ensuring information and/or cyber security;
CG 5. Ability to search, process and analyze information. CS 1. Ability to apply the legislative and regulatory framework, as well as state and international requirements, practices and standards in order to carry out professional activities in the field of information and/or cyber security CS 3. Ability to use software and software-hardware complexes of information protection means in information and telecommunication (automated) systems. CS 4. Ability to ensure business continuity in accordance with the established information and/or cyber security policy.	LO 9 – to implement processes based on national and international standards for detection, identification, analysis and response to information and/or cyber security incidents;

CS 5. The ability to ensure the protection of information processed in information and telecommunication (automated) systems for the purpose of implementing the established information and/or cyber security policy. CS 7. Ability to implement and ensure the functioning of complex information protection systems (complexes of regulatory, organizational and technical means and methods, procedures, practical techniques, etc.). CS 8. Ability to carry out incident management procedures, conduct investigations, provide them with an assessment. CS 9. Ability to carry out professional activities based on the implemented information and/or cyber security management system. CS 11. Ability to monitor the processes of functioning of information, information- telecommunication (automated) systems in accordance with the established policy of information and/or cyber security. CS 12. Ability to analyze, identify and evaluate possible threats, vulnerabilities and destabilizing factors to the information space and information resources in accordance with the established policy of information and/or cyber security	
CG 2. Awareness and understanding of the subject area and the profession. CS 2. Ability to use information and communication technologies, modern methods and models of information security and/or cyber security. CS 3. Ability to use software and software-hardware complexes of information protection means in information and telecommunication (automated) systems. CS 4. Ability to ensure business continuity in accordance with the established information and/or cyber security policy. CS 5. The ability to ensure the protection of information processed in information and telecommunication (automated) systems for the purpose of implementing the established information and/or cyber security policy. CS 6. The ability to restore the regular functioning of information, information and telecommunication (automated) systems after the implementation of threats, cyber attacks, failures of various classes and origins. CS 8. Ability to carry out incident management procedures, conduct investigations, provide them with an assessment. CS 11. Ability to monitor the processes of functioning of information, information- telecommunication (automated) systems in accordance with the established policy of information and/or cyber security.	LO 17 – to ensure the processes of protection and functioning of information and telecommunication (automated) systems based on practices, skills and knowledge, regarding structural (structural-logical) schemes, network topology, modern architectures and models of protection of electronic information resources with a display of relationships and information flows, processes for internal and remote components;
CG 1. Ability to apply knowledge in practical situations. CS 4. Ability to ensure business continuity in accordance with the established information and/or cyber security policy. CS 5. The ability to ensure the protection of information processed in information and telecommunication (automated) systems for the purpose of implementing the established information and/or cyber security policy. CS 9. Ability to carry out professional activities based on the implemented information and/or cyber security management system. CS 11. Ability to monitor the processes of functioning of information, information- telecommunication (automated) systems in accordance with the established policy of information and/or cyber security.	LO 24 – to solve the problems of managing access to information resources and processes in information and information and telecommunication (automated) systems based on access management models (mandatory, discretionary, role-based);

CG 1. Ability to apply knowledge in practical situations. CS 4. Ability to ensure business continuity in accordance with the established information and/or cyber security policy. CS 5. The ability to ensure the protection of information processed in information and telecommunication (automated) systems for the purpose of implementing the established information and/or cyber security policy. CS 6. The ability to restore the regular functioning of information, information and telecommunication (automated) systems after the implementation of threats, cyber attacks, failures of various classes and origins.	LO 27 – to solve problems of data flow protection in information, information and telecommunication (automated) systems;
CS 3. Ability to use software and software-hardware complexes of information protection means in information and telecommunication (automated) systems. CS 4. Ability to ensure business continuity in accordance with the established information and/or cyber security policy. CS 5. The ability to ensure the protection of information processed in information and telecommunication (automated) systems for the purpose of implementing the established information and/or cyber security policy. CS 8. Ability to carry out incident management procedures, conduct investigations, provide them with an assessment. CS 9. Ability to carry out professional activities based on the implemented information and/or cyber security management system. CS 12. Ability to analyze, identify and evaluate possible threats, vulnerabilities and destabilizing factors to the information space and information resources in accordance with the established policy of information and/or cyber security	LO 29 - to evaluate the possibility of realizing potential threats to information processed in information and telecommunication systems and the effectiveness of the use of protective equipment complexes in the conditions implementation of threats of various classes;
CG 1. Ability to apply knowledge in practical situations. CS 4. Ability to ensure business continuity in accordance with the established information and/or cyber security policy. CS 5. The ability to ensure the protection of information processed in information and telecommunication (automated) systems for the purpose of implementing the established information and/or cyber security policy. CS 9. Ability to carry out professional activities based on the implemented information and/or cyber security management system. CS 11. Ability to monitor the processes of functioning of information, information- telecommunication (automated) systems in accordance with the established policy of information and/or cyber security.	LO 32 – to solve the tasks of managing the processes of restoring the regular functioning of information and telecommunication systems using backup procedures in accordance with the established security policy;
CS 1. Ability to apply the legislative and regulatory framework, as well as state and international requirements, practices and standards in order to carry out professional activities in the field of information and/or cyber security. CS 4. Ability to ensure business continuity in accordance with the established information and/or cyber security policy. CS 8. Ability to carry out incident management procedures, conduct investigations, provide them with an assessment. CS 9. Ability to carry out professional activities based on the implemented information and/or cyber security management system. CS 12. Ability to analyze, identify and evaluate possible threats, vulnerabilities and destabilizing factors to the information space and information resources in accordance with the established policy of	LO 33 – to solve the tasks of ensuring the continuity of business processes of the organization based on the theory of risks;

information and/or cyber security	
CS 1. Ability to apply the legislative and regulatory framework, as well as state and international requirements, practices and standards in order to carry out professional activities in the field of information and/or cyber security. CS 4. Ability to ensure business continuity in accordance with the established information and/or cyber security policy. CS 5. The ability to ensure the protection of information processed in information and telecommunication (automated) systems for the purpose of implementing the established information and/or cyber security policy. CS 8. Ability to carry out incident management procedures, conduct investigations, provide them with an assessment. CS 9. Ability to carry out professional activities based on the implemented information and/or cyber security management system. CS 12. Ability to analyze, identify and evaluate possible threats, vulnerabilities and destabilizing factors to the information space and information resources in accordance with the established policy of information and/or cyber security	LO 34 – to participate in the development and implementation of information security and/or cyber security strategy in accordance with the goals and objectives of the organization;
CG 1. Ability to apply knowledge in practical situations. CS 1. Ability to apply the legislative and regulatory framework, as well as state and international requirements, practices and standards in order to carry out professional activities in the field of information and/or cyber security CS 3. Ability to use software and software-hardware complexes of information protection means in information and telecommunication (automated) systems. CS 4. Ability to ensure business continuity in accordance with the established information and/or cyber security policy. CS 5. The ability to ensure the protection of information processed in information and telecommunication (automated) systems for the purpose of implementing the established information and/or cyber security policy. CS 7. Ability to implement and ensure the functioning of complex information protection systems (complexes of regulatory, organizational and technical means and methods, procedures, practical techniques, etc.). CS 8. Ability to carry out incident management procedures, conduct investigations, provide them with an assessment. CS 9. Ability to carry out professional activities based on the implemented information and/or cyber security management system. CS 12. Ability to analyze, identify and evaluate possible threats, vulnerabilities and destabilizing factors to the information space and information resources in accordance with the established policy of information and/or cyber security	LO 35 – to solve the tasks of providing and supporting complex information protection systems, as well as countering unauthorized access to information resources and processes in information and information-telecommunication (automated) systems in accordance with the established policy of information and/or cyber security;
CS 4. Ability to ensure business continuity in accordance with the established information and/or cyber security policy. CS 5. The ability to ensure the protection of information processed in information and telecommunication (automated) systems for the purpose of implementing the established information and/or cyber security policy. CS 8. Ability to carry out incident management procedures, conduct investigations, provide them with an assessment. CS 9. Ability to carry out professional activities based on the implemented information and/or cyber security management system.	LO 42 – to implement the processes of detection, identification, analysis and response to information and/or cyber security incidents;

CS 11. Ability to monitor the processes of functioning of information, information- telecommunication (automated) systems in accordance with the established policy of information and/or cyber security. CS 12. Ability to analyze, identify and evaluate possible threats, vulnerabilities and destabilizing factors to the information space and information resources in accordance with the established policy of information and/or cyber security	
CG 2. Awareness and understanding of the subject area and the profession. CS 1. Ability to apply the legislative and regulatory framework, as well as state and international requirements, practices and standards in order to carry out professional activities in the field of information and/or cyber security CS 4. Ability to ensure business continuity in accordance with the established information and/or cyber security policy. CS 5. The ability to ensure the protection of information processed in information and telecommunication (automated) systems for the purpose of implementing the established information and/or cyber security policy. CS 8. Ability to carry out incident management procedures, conduct investigations, provide them with an assessment. CS 9. Ability to carry out professional activities based on the implemented information and/or cyber security management system. CS 11. Ability to monitor the processes of functioning of information, information- telecommunication (automated) systems in accordance with the established policy of information and/or cyber security. CS 12. Ability to analyze, identify and evaluate possible threats, vulnerabilities and destabilizing factors to the information space and information resources in accordance with the established policy of information and/or cyber security	LO 43 – to apply national and international regulatory acts in the field of information security and/or cyber security to investigate incidents;
CS 1. Ability to apply the legislative and regulatory framework, as well as state and international requirements, practices and standards in order to carry out professional activities in the field of information and/or cyber security. CS 4. Ability to ensure business continuity in accordance with the established information and/or cyber security policy. CS 5. The ability to ensure the protection of information processed in information and telecommunication (automated) systems for the purpose of implementing the established information and/or cyber security policy. CS 8. Ability to carry out incident management procedures, conduct investigations, provide them with an assessment. CS 9. Ability to carry out professional activities based on the implemented information and/or cyber security management system. CS 12. Ability to analyze, identify and evaluate possible threats, vulnerabilities and destabilizing factors to the information space and information resources in accordance with the established policy of information and/or cyber security	LO 44 – to solve the problems of ensuring the continuity of the organization's business processes on the basis of risk theory and the established information security management system, in accordance with domestic and international requirements and standards;
CS 4. Ability to ensure business continuity in accordance with the established information and/or cyber security policy. CS 5. The ability to ensure the protection of information processed in information and telecommunication (automated) systems for the purpose of implementing the established information and/or cyber security policy. CS 8. Ability to carry out incident management procedures, conduct	LO 45 – to apply early classes of information security and/or cyber security policies based on risk-oriented control of access to information assets;

investigations, provide them with an assessment. CS 9. Ability to carry out professional activities based on the implemented information and/or cyber security management system. CS 12. Ability to analyze, identify and evaluate possible threats, vulnerabilities and destabilizing factors to the information space and information resources in accordance with the established policy of information and/or cyber security	
CS 4. Ability to ensure business continuity in accordance with the established information and/or cyber security policy. CS 5. The ability to ensure the protection of information processed in information and telecommunication (automated) systems for the purpose of implementing the established information and/or cyber security policy. CS 8. Ability to carry out incident management procedures, conduct investigations, provide them with an assessment. CS 9. Ability to carry out professional activities based on the implemented information and/or cyber security management system. CS 12. Ability to analyze, identify and evaluate possible threats, vulnerabilities and destabilizing factors to the information space and information resources in accordance with the established policy of information and/or cyber security	LO 46 – to analyze and minimize the risks of information processing in information and telecommunication systems;
CG 1. Ability to apply knowledge in practical situations CG 4. Ability to identify, pose and solve problems in a professional direction. CS 2. Ability to use information and communication technologies, modern methods and models of information security and/or cyber security. CS 3. Ability to use software and software-hardware complexes of information protection means in information and telecommunication (automated) systems. CS 4. Ability to ensure business continuity in accordance with the established information and/or cyber security policy. CS 5. The ability to ensure the protection of information processed in information and telecommunication (automated) systems for the purpose of implementing the established information and/or cyber security policy. CS 6. The ability to restore the regular functioning of information, information and telecommunication (automated) systems after the implementation of threats, cyber attacks, failures of various classes and origins. CS 8. Ability to carry out incident management procedures, conduct investigations, provide them with an assessment. CS 11. Ability to monitor the processes of functioning of information, information- telecommunication (automated) systems in accordance with the established policy of information and/or cyber security. CS 12. Ability to analyze, identify and evaluate possible threats, vulnerabilities and destabilizing factors to the information space and information resources in accordance with the established policy of information and/or cyber security	LO 53 – to solve the problems of software code analysis for the presence of possible threats;
CG 1. Ability to apply knowledge in practical situations. CG 2. Awareness and understanding of the subject area and the profession. CG 6. Ability to realize one's rights and responsibilities as a member of	LO 54 – to realize the values of a civil (free democratic) society and the need for its sustainable development, the rule of law, the

society, to realize the values of a civil (free democratic) society and the need for its sustainable development, the rule of law, the rights and freedoms of a person and a citizen in Ukraine. CG 7. Ability to preserve and multiply moral, cultural, scientific values and achievements of society based on understanding the history and patterns of development of the subject area, its place in the general system of knowledge about nature and society and in the development of society, techniques and technologies, use different types and forms motor activity for active recreation and leading a healthy lifestyle.	rights and freedoms of a person and a citizen in Ukraine.

Curriculum

Content module 1. Cybersecurity as a computer science

Topic 1. Cybersecurity as a component of information technology. Terminology, basic concepts.
Topic 2. Data storage. Functional security services.
Topic 3. Data processing. Encryption as a way to protect information from unauthorized access.
Topic 4. Symmetric and asymmetric encryption algorithms.
Topic 5. Security policies. Discretionary, mandated and role-based access management
Topic 6. Legislative and regulatory framework of protection
Content module 2. Cyber security toolkit
Topic 7. Types of threats and attacks. Types of malwares
Topic 8. MITRE ATT&CK matrix as a way to study malware
Topic 9. Static analysis of malware.
Topic 10. Dynamic analysis of malware
Topic 11. Search for software vulnerabilities
Topic 12. Hacking utilities

The list of laboratory classes, as well as questions and tasks for independent work is given in the table "Rating-plan of the discipline".

Teaching and learning methods

Teaching and learning methods Teaching the discipline involves the involvement of explanatory and illustrative, reproductive, research methods, as well as methods of problem-based learning. Thus, during lectures, the teacher provides applicants with a significant amount of theoretical material with explanations involving graphic presentation (diagrams, tables, presentations) and examples of threat diagnostics involving specialized software and online resources (Topic 6, 7, 8, 9, 10 , 11, 12).

During the laboratory classes, applicants have the opportunity to acquire practical skills in working with Internet resources both for a deeper acquaintance with the subject field (Topics 1, 2, 3, 4, 5, 6) and for diagnosis and identification of threats (Topics 7, 8, 9, 10, 11, 12). Improvement of practical skills takes place during the performance of tasks using such learning methods as: individual tasks (Topics 2, 3) and independent work (Topics 7, 8, 9, 10, 11).

Each topic is accompanied by a link to video material with additional information. The given teaching methods are aimed at forming the students' ability to solve complex complex problems in the field of mathematical modeling.

The procedure for evaluating learning outcomes

The procedure for evaluating learning outcomes

The system of assessment of formed competencies in students takes into account the types of classes, which according to the curriculum of the discipline include lectures and laboratory classes, as well as independent work. Assessment of the formed competencies of students is carried out

according to the accumulative 100-point system. Control measures include:

1) current control, which is carried out during the semester during lectures and laboratory classes and is estimated by the number of points scored (maximum amount - 100 points; the minimum amount that allows a student to set off - 60 points);

2) final / semester points are calculated as sum of current points for laboratory works and tests.

The procedure for the current assessment of students' knowledge.

Assessment of student knowledge during lectures and laboratory classes is carried out according to the following criteria:

- ability to apply basic methods of analysis of the studied phenomena, processes and design solutions;
- ability to identify cyber threats;
- ability to describe different types of malware and attacks;
- ability to produce the simplest setting up protection means;
- ability to use basic programming concepts;
- ability to describe components of computer system;
- ability to create and implement algorithms;
- ability to apply theories and methods of protection to provide information security in information and telecommunications systems;
- ability to use modern soft- and hardware for information and communication technologies.

The discipline provides the following methods of current formative assessment: questioning and oral comments of the teacher on his results, instructions of teachers in the process of laboratory tasks, the formation of self-assessment skills and discussion of students completed laboratory tasks, control of independent performance of an individual task.

All work must be done independently in order to develop a creative approach to solving problems.

Tests: the maximum number of points is 20.

Laboratory classes: the maximum number of points is 80 (defense of laboratory works - 64, control works - 20), and the minimum - 50.

Individual work: consists of the time that the applicant spends on preparation for laboratory work and on preparation for express surveys of lectures and tests for laboratory work of the discipline, in the technological map points for this type of work are not allocated.

Final control: is based on the points obtained during the semester.

A student should be considered certified if the sum of points obtained from the results of the final / semester performance test is equal to or exceeds 60.

The final grade in the discipline is calculated taking into account the points obtained during the current control of the accumulative system. The total result in points for the semester is: "60 or more points - credited", "59 or less points - not credited" and is entered in the test "Statement of performance" of the discipline.

Forms of assessment and distribution of points are given in the table "Rating-plan of the discipline".

Rating plan of the discipline

Topic	**Forms and types of education**	**Forms of evaluation**	**Max ball**
Topic	***Classroom work***		

1	Lecture	Lecture *" Cybersecurity as a component of information technology. Terminology, basic concepts"*		
	Laboratory lesson	*Laboratory work №1. Basics of working with MS Word*		
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory classes. Execution of laboratory tasks		
Topic 2	***Classroom work***			
	Lecture	Lecture *" Data storage. Functional security services."*		
	Laboratory lesson	*Laboratory work №1. Basics of working with MS Word*	perform and defense of the LW	8
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory classes. Execution of laboratory tasks		
Topic 3	***Classroom work***			
	Lecture	Lecture *" Data processing. Encryption as a way to protect information from unauthorized access."*		
	Laboratory lesson	*Laboratory work № 2. Basic of working with MS Excel*	perform and defense of the LW	8
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory classes. Execution of laboratory tasks		
Topic 4	***Classroom work***			
	Lecture	Lecture *" Symmetric and asymmetric encryption algorithms."*		
	Laboratory lesson	*Laboratory work № 2. Basics of working with MS Excel.*	perform and defense of the LW	8

	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory classes. Execution of laboratory tasks		
	Classroom work			
	Lecture	Lecture *" Security policies. Discretionary, mandated and role-based access management"*		
	Laboratory lesson	*Laboratory work №3. Basics of working with MS Excel. Data Validation.*	perform and defense of the laboratory work	8
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory classes. Execution of laboratory tasks		
	Classroom work			
	Lecture	Lecture *" Legislative and regulatory framework of protection "*		
	Laboratory lesson	*Laboratory work №4. Basics of working with MS Excel. Diagram*	Test	10
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory classes. Execution of laboratory tasks		
	Classroom work			
	Lecture	Lecture *" Types of threats and attacks. Types of malwares"*		
	Laboratory lesson	*Laboratory work № 5. Study types of threats and attacks*	perform and defense of the laboratory work	8
	Individual work			

	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory classes. Execution of laboratory tasks		
	Classroom work			
	Lecture	Lecture *" MITRE ATT&CK matrix as a way to study malware "*		
	Laboratory lesson	*Laboratory work №6. MITRE ATT&CK matrix as a way to study malware*	perform and defense of the laboratory work	8
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory classes. Execution of laboratory tasks		
	Classroom work			
	Lecture	Lecture *" Static analysis of malware."*		
	Laboratory lesson	*Laboratory work №7. Static analysis of malware*	perform and defense of the laboratory work	8
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory classes. Execution of laboratory tasks		
	Classroom work			
	Lecture	Lecture *" Dynamic analysis of malware "*		
	Laboratory lesson	*Laboratory work №8. Dynamic analysis of malware*	perform and defense of the laboratory work	8
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory classes. Execution of laboratory tasks		

	Classroom work			
	Lecture	Lecture *" Search for software vulnerabilities "*		
	Laboratory lesson	*Laboratory work № 9. Fundamentals of algorithm.)*	perform and defense of the laboratory work	8
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory classes. Execution of laboratory tasks		
	Classroom work			
	Lecture	Lecture *" Hacking utilities*	test	10
	Laboratory lesson	*Laboratory work № 10. Fundamentals of programming*	perform and defense of the laboratory work	8
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory classes. Execution of laboratory tasks		

Recommended Books

Basic

1. Heard Nick, Adams Niall, Rubin-Delanchy Patrick, Turcotte Melissa Data Science for Cyber-Security - WSPC (EUROPE), 2018 – 304 p.
2. Brooks C. J., Grow, C., Craig, P., & Short, D. Cybersecurity essentials. – John Wiley & Sons, 2018. – 767 p.
3. Yuri Diogenes, Dr. Erdal Ozkaya Cybersecurity – Attack and Defense Strategies Packt Publishing, 2019. -- 634p.
4. Moschovitis, C. Privacy, Regulations, and Cybersecurity. 1st edn. Wiley, 2021.- Available at: https://www.perlego.com/book/2173931/privacy-regulations-and-cybersecurity-the-essential-business-guide-pd
5. Rains, T. Cybersecurity Threats, Malware Trends, and Strategies. 1st edn. Packt Publishing, 2020. -- Available at: https://www.perlego.com/book/1484871/cybersecurity-threats-malware-trends-and-strategies-mitigate-exploits-malware-phishing-and-other-social-engineering-attacks-pdf .
6. Aumasson J.-P. Serious Cryptography. A Practical Introduction to Modern Encryption. No Starch

Press, 2018. – 434p.
7. Seacord R.C. Effective C. An introduction to Professional C Programming. – No Starch Press, 2020. – 305p.

Optional

8. Hall G., Watson E. Computer Hacking, Security Testing, Penetration Testing and Basic Security, 2020. – 356p.
9. Chio C., Freeman D. Machine learning and security: Protecting systems with data and algorithms. – " O'Reilly Media, Inc.", 2018. – 385p.
10. Bowne S. Hands-On Cryptography with Python. – Packt, 2018. – 124 p.

Information resource

1. Web-site of personal learning systems KNEU on discipline "Introduction to Specialty"- https://pns.hneu.edu.ua/course/view.php?id=9045.