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

"ЗАТВЕРДЖУЮ"
Заступник керівника
(проректор з науково-педагогічної роботи)
____
Микола АФАНАСЬЄВ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ СЕМЕНА КУЗНЕЦЯ
№02071211

<u>ЦИФРОВА КРИМІНАЛІСТИКА</u>

робоча програма навчальної дисципліни

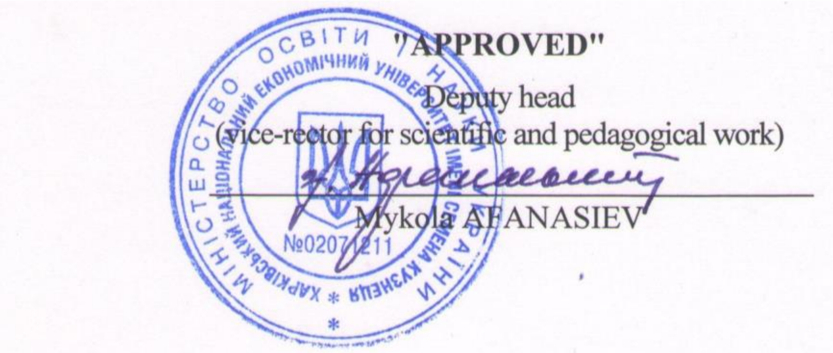
Галузь знань	***12 Інформаційні технології***
Спеціальність	***125 Кібербезпека***
Освітній рівень	***другий (магістерський)***
Освітня програма	***Кібербезпека***

Статус дисципліни	***базова***
Мова викладання, навчання та оцінювання	***англійська***

Завідувач кафедри
кібербезпеки та
інформаційних технологій ______________ *Сергій ЄВСЕЄВ*

Харків
2020

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



"APPROVED"
Deputy head
(vice-rector for scientific and pedagogical work)
Mykola AFANASIEV

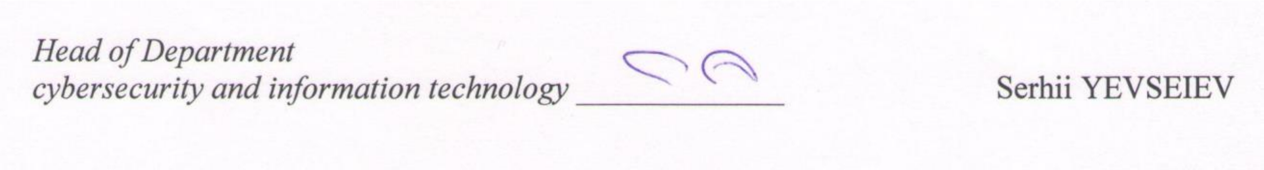
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ СЕМЕНА КУЗНЕЦЯ
№02071211

<u>DIGITAL FORENSIC</u>

Syllabus of the discipline

Field of knowledge	***12 Information technologies***
Speciality	***125 Cybersecurity***
Educational level	***Second (master)***
Educational program	***Cyber Security***

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



Head of Department
cybersecurity and information technology ______________ Serhii YEVSEIEV

Kharkiv

2020

APPROVED
at a meeting of the *Department of Cybersecurity and Information Technology*
Protocol № 2 dated 31.08.2020

Developer:
Milov O.V., Ph.D., Prof. of CIT Department.

Update and re-approval letter
working program of the discipline

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

Abstract of the discipline

The subject of the discipline is the basic concepts and methods of digital forensics, skills of collecting digital forensic information using open source tools from Windows and Linux operating systems.

The purpose of teaching the discipline is to form theoretical knowledge of the basic principles of modern networks, which include local, global and regional networks, through which new approaches to managing the modern information society, as well as the formation of practical skills in building and managing corporate systems and networks.

The results of this discipline are the acquisition of skills to install and configure software to collect digital forensic information, perform malware analysis, use Windows Live Linux Response, independently collect and analyze digital forensic information, develop methods to respond to cybersecurity, use digital tools forensics and recovery for data protection in Windows, Linux.

Characteristics of the discipline

Course	**1**
Semester	**2**
Number of ECTS credits	**4**
Form of final control	**Exam**

Structural and logical scheme of studying the discipline

Prerequisites	**Postrequisites**
Mathematical foundations of cryptology Fundamentals of cryptographic protection	

Competences and learning outcomes in the discipline

Competences	**Learning outcomes**
CF 4. Ability to design, implement, maintain information networks and resources, information technology security (including cloud technologies and applications), as well as security of business / operational processes to ensure the functioning of information and communication systems in accordance with the established strategy and policy information security and / or cybersecurity of the organization	PRN2 - plan, analyze and organize their own professional activities, choose the best methods and ways to solve complex specialized problems and practical problems in professional activities, evaluate their effectiveness; PRN7 - identify, describe and use the system of analysis of relationships between information flows and resources (including critical) in the contour of business processes of the organization (enterprise); PRN8 - design, implement and maintain systems for protection of information systems and resources, infrastructure of the institution, develop modern architectures for the use of information technologies and their security (security architectures, information security models, safe operation modes, methods for assessing the quality of open and closed systems, etc.) ; PRN13 - to develop, plan, analyze and implement a system of audit and control of the effectiveness of information and communication systems (access nodes to global networks, software and hardware systems, subsystems, etc.), according to the established policy of information security and / or cybersecurity
CF 7. Ability to analyze the causes and consequences of failures or failures of information systems caused by the	PRN2 - plan, analyze and organize their own professional activities, choose the best methods and ways to solve complex specialized problems and practical problems in professional activities, evaluate their effectiveness;

implementation of various classes of cyber incidents, as well as to develop and implement methods and measures to restore the normal functioning of the infrastructure of the organization as a whole/	PRN8 - design, implement and maintain systems for protection of information systems and resources, infrastructure of the institution, develop modern architectures for the use of information technologies and their security (security architectures, information security models, safe operation modes, methods for assessing the quality of open and closed systems, etc.) ; PRN-10 - to analyze and implement systems for classification of threats to information resources (assets), to rank them according to different classes of parameters (by probability of occurrence, cost, qualitative and quantitative indicators, etc.) PRN-11 - plan, implement, ensure and control the continuity of business / operational processes of the organization (enterprise), according to the established policy of information security and / or cybersecurity and strategy of the organization (enterprise) PRN-12 - to develop, plan, analyze and implement a system of access to information resources, information and communication systems (access nodes to global networks, software and hardware systems, subsystems, software, etc.), according to the established policy of information security and / or cybersecurity PRN-13 - to develop, plan, analyze and implement a system of audit and control of the effectiveness of information and communication systems (access nodes to global networks, software and hardware systems, subsystems, etc.), according to the established policy of information security and / or cybersecurity PRN-16 - to develop, implement, and organize the implementation of processes using methods and means of cryptographic and technical protection of information at the objects of information activities, in accordance with the established policy of information security and / or cybersecurity PRN-17 - to develop, implement and support the processes of detection and identification of cyberattacks, their analysis and implement procedures for responding and managing information and / or cybersecurity incidents

CF 11. Ability to develop, implement and maintain systems for auditing and monitoring the quality of business / operational processes of information and communication systems and technologies, as well as information security management systems and / or cybersecurity of the organization as a whole.	PRN-8 - design, implement and maintain systems for protection of information systems and resources, infrastructure of the institution, develop modern architectures for the use of information technologies and their security (security architectures, information security models, safe operation modes, methods for assessing the quality of open and closed systems). etc) PRN-11 - plan, implement, ensure and control the continuity of business / operational processes of the organization (enterprise), according to the established policy of information security and / or cybersecurity and strategy of the organization (enterprise) PRN-12 - to develop, plan, analyze and implement a system of access to information resources, information and communication systems (access nodes to global networks, software and hardware systems, subsystems, software, etc.), according to the established policy of information security and / or cybersecurity PRN-13 - to develop, plan, analyze and implement a system of audit and control of the effectiveness of information and communication systems (access nodes to global networks, software and hardware systems, subsystems, etc.), according to the established policy of information security and / or cybersecurity PRN-14 - to develop and implement measures to counter cyber incidents, as well as to analyze, implement procedures for incident management and control, organize and conduct investigations, provide recommendations on measures to prevent and combat them PRN-15 - to develop, implement and support processes of management of procedures of identification, authentication, authorization of users and information resources, operational processes of infrastructure of the organization (enterprise), according to the established policy of information security and cybersecurity

Curriculum of the discipline

Content module 1. Digital forensic foundations

Topic 1. *Introduction to digital forensics*
Topic 2. *Basic concepts and methodology of digital forensic*
Topic 3. *Digital forensic foundations*
Topic 4. *Digital forensic*

Content module 2. Specialized software for digital foransic

Topic 5. *Basic methods of using specialized software*
Topic 6. *Processing of digital forensics in software*
Topic 7. *Typical cases and recommendations for their study*
Topic 8. *Reporting and difficulties in the application of digital forensics*

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

In the course of teaching the discipline the teacher uses explanatory-illustrative (information-receptive) and reproductive teaching methods. Problem-based lectures, presentations, conversations, individual and group mini-projects are used as teaching methods that are aimed at activating and stimulating the educational and cognitive activities of applicants.

The procedure for evaluating learning outcomes

The system of assessment of formed competencies in students takes into account the types of classes, which in accordance with 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 amount of points scored (maximum amount - 60 points; the minimum amount that allows a student to take the exam - 35 points);

2) final / semester control, which is conducted in the form of a semester exam, in accordance with the schedule of the educational process.

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:

- install and configure specialized software;
- to collect and analyze digital forensic information in Windows;
- to collect and analyze digital forensic information in Linux.

Final control of knowledge and competencies of students in the discipline is carried out on the basis of a semester exam, the task of which is to test students' understanding of the program material in general, logic and relationships between individual sections, ability to creatively use accumulated knowledge, ability to formulate their attitude to a particular problem. disciplines, etc.

Lectures: the maximum number of points is 17 (work on lectures - 8, express survey - 9).

Laboratory classes: the maximum number of points is 43 (laboratory work - 8, defense of laboratory work - 15, control work - 20), and the minimum - 24.

Independent work: consists of time that the applicant spends on preparation for laboratory work and preparation for the exam in the discipline, in the technological map points for this type of work are not allocated.

Final control: is carried out taking into account the exam.

The examination ticket covers the program of the discipline and provides for the determination of the level of knowledge and the degree of mastery of competencies by students.

Each exam ticket consists of 3 practical situations (one stereotypical, one diagnostic and one heuristic task), which involve solving typical professional tasks in the workplace and allow to diagnose the level of theoretical training of the student and his level of competence in the discipline. Evaluation of each task of the examination ticket is as follows: the first task is 20 test tasks of the closed form, its performance is estimated by 20 points; the second task - devoted to data analysis, its implementation is estimated at 10 points; the third task - calculation, its performance is estimated at 10 points.

The result of the semester exam is evaluated in points (maximum number - 40 points, minimum number of credits - 25 points) and is affixed in the appropriate column of the examination "Information of performance".

A student should be considered certified if the sum of points obtained from the final / semester test is equal to or exceeds 60. The minimum possible number of points for current and modular control during the semester is 35 and the minimum possible number of points scored in the exam is 25.

The final grade in the discipline is calculated taking into account the scores obtained during the exam and the scores 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.

The final grade is set according to the scale given in the table "Grade scale: national and ECTS".

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

Assessment scale: national and ECTS

The sum of points for all types of educational activities	Score ЄКТС	Score on a national scale	
		for exam, course project (work), practice	For credit
90 – 100	A	excellent	credited
82 – 89	B	fine	
74 – 81	C		
64 – 73	D	satisfactorily	
60 – 63	E		
35 – 59	FX	unsatisfactorily	Not credited

Rating plan of the discipline

Topic	**Forms and types of education**		**Forms of evaluation**	**Max points**
Topic 1	***Classroom work***			
	Lecture	Lecture *" Introduction to digital forensics "*	Lecture	1
	Laboratory work	Laboratory work №1 *"Installation and configuration of specialized software"*	Laboratory work	1
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory work. Execution of laboratory tasks		
Topic 2.	***Classroom work***			
	Lecture	Lecture *"Basic concepts and methodology of digital forensic"*	Lecture	1
	Laboratory work	Laboratory work №1 *"Installation and configuration of specialized software"*	Laboratory work	1
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory work. Execution of laboratory tasks		
Topic 3	***Classroom work***			
	Lecture	Lecture *"Digital forensic foundations"*	Lecture	1
	Laboratory work	Laboratory work №2. *"Collection and analysis of digital forensic information in Windows"*	Laboratory work	1

			Defense of laboratory work № 1	5
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory work. Execution of laboratory tasks		
Topic 4	***Classroom work***			
	Lecture	Lecture *"Digital forensic"*	Lecture	1
	Laboratory work	Laboratory work №2. *"Collection and analysis of digital forensic information in Windows"*	Laboratory work	1
			Control work 1	10
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory work. Execution of laboratory tasks		
Topic 5	***Classroom work***			
	Lecture	Lecture *"Базові методи використання спеціалізованого програмного забезпечення"*	Lecture	1
			Quiz	4
	Laboratory work	Laboratory work №2. *"Collection and analysis of digital forensic information in Windows"*	Laboratory work	1
Тема 6	***Classroom work***			
	Lecture	Lecture *"Processing of digital forensics in software"*	Lecture	1
	Laboratory work	Laboratory work №2. *"Collection and analysis of digital forensic information in Windows"*	Laboratory work	1
			Defense of laboratory work № 2	5
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory work. Execution of laboratory tasks		
Тема 7	***Classroom work***			
	Lecture	Lecture *"Typical cases and recommendations for their study"*	Lecture	1
	Laboratory work	Laboratory work №3. *" Collection and analysis of digital forensic information in Linux"*	Laboratory work	1
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory work. Execution of laboratory tasks		

Topic 8	***Classroom work***			
	Lecture	Lecture *"Reporting and difficulties in the application of digital forensics"*	Lecture	1
			Quiz	5
	Laboratory work	Laboratory work №3. *"Collection and analysis of digital forensic information in Linux"*	Laboratory work	1
			Defense of laboratory work № 3	5
			Control work 2	10
	Individual work			
	Questions and tasks for self-study	Search, selection and review of literary sources on a given topic. Preparation for laboratory work. Execution of laboratory tasks		
Final Test				40

Recommended References

Basic

1. Маркусь В. О. Криміналістика. Навчальний посібник – К.: Кондор, 2007. – 558 с.

2. 16. Вертузаєв М. С., Голубаєв В. О., Котляревський О. І., Юрченко О. М. Безпека комп'ютерних систем. Комп'ютерна злочинність та її попередження / Під ред. Снігірьова О. П.. –Запоріжжя: ПВКФ «Навел», 1998.

3. Шепітько В.Ю. Криміналістика: Підручник для вищих закладів освіти. – К., Ін Юре, 2001, 2004.

4. Baig Mohsin. 50 Reasons for Mastering Cyber Forensics Amazon Digital Services LLC, 2017. – 14 p.

5. Bell Suzanne. Measurement Uncertainty in Forensic Science: A Practical Guide CRC Press, 2016. – 178 p.

6. JIEC-Council Computer. Forensics: Investigating Data and Image Files Course Technology, 2009. - 224 pages

7. Sachowski J. Implementing Digital Forensic Readiness: From Reactive to Proactive Process Syngress. — 375 p.

8. Shipley Todd G., Bowker Art. Investigating Internet Crimes Elsevier, 2014.

9. Taroni F., Bozza S., Biedermann A., Garbolino P., Aitken C. Data Analysis in Forensic Science: A Bayesian Decision Perspective N.-Y.: Wiley, 2010.- 390p.

Additional

10. ISACA. (2015). Overview of Digital Forensics. http://www.infosecurityeurope.com/__novadocuments/83665?v=635652368156170000.

11. Karie, Nickson M. and H. S. Venter (2015). Taxonomy of Challenges for Digital Forensics. Journal of Forensic Sciences, Vol. 60(4), 885–893.

12. Maras Marie-Helen. (2014). Computer Forensics: Cybercriminals, Laws, and Evidence. Jones and Bartlett.

13. Myers Matthew and Marcus Rogers. (2007). Digital Forensics: Meeting the Challenges of Scientific Evidence. Advances in Digital Forensics: IFIP International Conference on Digital Forensics (pp. 43-50).

14. Roussev Vassil, Candace Quates, and Robert Martel. (2013). Real-time digital forensics and triage. Digital Investigation Vol. 10(2), 158–167.

15. Sammons John. (2017). Digital forensics, 2st edition. Elsevier.

Information resources

16. The site of personal educational systems of KhNEU named after S. Kuznets in the discipline "Digital Forensics" https://pns.hneu.edu.ua/course/view.php?id=5683.