KHMELNYTSKYI NATIONAL UNIVERSITY

APPROVED
Dean of IT Faculty
_____ Tetiana HOVORUSHCHENKO
August 31, 2024

COURSE PROGRAM

Digital forensics
Name of the course

Field of study	12 – Information technology
Major	125 – Cyber Security and Information Protection
Higher education level	Second (Master's)
Educational program	Cyber Security and Information Protection
The scope of the discipline	8 ECTS credits
Discipline code	SC.04
Language of education	English
Discipline status	Selective
Faculty	Information Technologies
Department	Cyber Security

Study mode	Year	Semester	Total number		Number of hours						Student' s individual work	Student' s independent work including individual work	Type of semester control	
					Classwork hours					Student' s independent work including individual work				
			ECTS credits	Hours	Total	Lectures	Laboratory works	Practical classes	Seminar classes				Pass/ fail test	Examination
Full-Time	-	-	8	240	85	34	51	-	-	155		-	+	

Program's author _____ cand. of technical sciences, associate prof. Viktor CHESHUN
Signature — Degree, academic title, Name, SURNAME of the author(s)

Approved at the staff meeting of the department of Cyber Security
Record № 1 of August 30, 2024

Head of the Department of Cyber Security _____ Yuriy KLOTS
Signature — Name, SURNAME

The course program is approved by the Academic Board of the Faculty of Information Technologies

Head of the Academic Board _____ Tetiana HOVORUSHCHENKO
Signature — Name, SURNAME

Khmelnytskyi 2024

DIGITAL FORENSICS

Type of discipline	Selective
Educational level	Second (master's)
Language of teaching	Ukrainian
Number of ECTS credits	8
Forms of obtaining education	Daytime

Learning outcomes. A student who has successfully completed the study of the discipline must: know the theoretical foundations and modern information technologies of analysis and collection of digital forensic information; be able to apply the methods of digital forensics; examine data and identify data sources; be able to receive and describe digital evidence; apply methods of authentication of digital evidence; be able to compare and contrast digital evidence and traditional evidence to establish differences between them; use and critically analyze digital forensics process models; apply national and international regulatory acts in the field of information security to investigate internal and external incidents; apply standards and best practices related to digital evidence in digital forensics; to have the basic concepts, methods and tools of digital forensics; possess the skills of collecting and analyzing digital forensic information, methods of authentication of digital evidence; have the ability to independently master new methods and technologies of cybercrime investigation and cybercrime prevention.

Content of the academic discipline. Fundamentals of digital forensics. Digital forensics of operating systems. Computer crimes and incidents. Investigating digital crimes. Operative and investigative measures and investigative actions. Collection and classification of evidence. Examination of evidence. International Organization for Computer Evidence. The use of regulatory and legal support in digital forensics.

Planned classroom work: the number of classroom hours is not less than 1/3 of the total number of hours planned for studying the discipline.

Teaching methods: verbal, visual and interactive (lectures); practical (laboratory works); explanatory and illustrative and research (independent work).

Forms of evaluation of learning results: protection of laboratory works, testing.

Semester control form: credit.

Educational resources:

1. Digital Forensics Basics: A Practical Guide Using Windows OS/ Edited by Nihad A. Hassan. New York, 2019. 335 p.
2. Виявлення та розслідування кіберзлочинів: навчально-методичний посібник /О.А. Самойленко. Одеса, 2020. 112 с.
3. Кіберзлочини в Україні (кримінально-правова характеристика): навч. посіб. Луцьк: СПД Гадяк Ж. В. друкарня «Волиньполіграф»™, 2019. 304 с.
4. Digital Forensics / Edited by André Årnes. John Wiley & Sons Ltd, 2018. 336 p.
5. Cybercrime: University Module Series, Teaching Guide/ United Nations Office on Drugs and Crime. Vienna, United Nations, Doha Declaration, 2019. 453 p.
6. Hemdan, E.ED., Manjaiah, D. An efficient digital forensic model for cybercrimes investigation in cloud computing. Multimed Tools Appl 80, 14255–14282 (2021).
7. Solanke, A.A., Biasiotti, M.A. Digital Forensics AI: Evaluating, Standardizing and Optimizing Digital Evidence Mining Techniques. Künstl Intell 36, 143–161 (2022).
8. MOODLE - modular learning environment. Access to the resource: https://msn.khmnu.edu.ua/ .
9. University electronic library. Access to the resource: http://library.khmnu.edu.ua/ .

Teacher: Ph.D., associate professor Cheshun V.M.

INTRODUCTION

The discipline "Digital Forensics" is an optional component of the professional training of masters in the field of information technologies in the specialty "Cybersecurity", which covers modern approaches to the disclosure and interpretation of electronic data in the process of accumulating digital evidence, as well as to the preservation of any evidence in its original form under the time of conducting a structured investigation through the collection, identification and verification of digital information in order to reconstruct past events.

The purpose of discipline. Formation of a system of knowledge and understanding of the basic concepts and methods of digital forensics, skills of collecting digital forensic information using open source tools from Windows and Linux operating systems, specialized software and technical means.

Subject of discipline. Fundamentals of digital forensics, digital forensics of operating systems; computer crimes and incidents, investigations, investigative measures and investigative actions, collection and classification of evidence, examination of evidence, international organization for computer evidence, use of regulatory and legal support in digital forensics.

Tasks of the discipline. To form knowledge about the principles underlying digital forensics, methods and means of searching for digital evidence, technologies for investigating cybercrimes. The study of the discipline should ensure the acquisition of competencies and the achievement of learning outcomes:

competences:

KZ 1. Ability to apply knowledge in practical situations

KZ 2. Knowledge and understanding of the subject area and understanding of the profession

KZ 4. The ability to identify, pose and solve problems in a professional direction.

Professional competences

CF 4. Ability to design, implement, support information networks and resources, security of information technologies (including cloud technologies and applications), as well as security of business/operational processes in order to ensure the functioning of information and communication systems in accordance with the established strategy and policy information security and/or cyber security of the organization.

learning outcomes:

RN 1. 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.

RN 2. To adapt in the conditions of frequent changes in the technologies of professional activity, to predict the final result.

RN 3. To solve the problems of protection of information processed in information and telecommunication systems, using modern methods and means of cryptographic protection of information.

RN 4. To solve the problems of software code analysis for the presence of possible threats.

RN 5. Use modern software and hardware of information and communication technologies.

RN 6. Solve the problems of collection, preservation, analysis and interpretation of digital evidence.

A student who has successfully completed the study of the discipline must: be able to apply the methods of digital forensics; examine data and identify data sources; receive and describe digital evidence; apply methods of authentication of digital evidence; compare and contrast digital evidence and traditional evidence to establish the differences between them; use and critically analyze digital forensics process models; apply national and international regulatory acts in the field of information security to investigate internal and external incidents in the field of cyber security; apply standards and best practices related to digital evidence in digital forensics. to have the basic concepts, methods and tools of digital forensics; skills of collecting and analyzing digital forensic information; methods of authentication of digital evidence; the ability to independently master new methods and technologies of cybercrime investigation and prevention.

COURSE CREDIT STRUCTURE

Name of the topic	Number of hours allocated to:		
	lectures	**laboratory work**	**independent work**
Topic 1. Introduction to Digital Forensics Science (DFS)	4	6	18
Topic 2. Basics of computer literacy of a DFC specialist	6	6	20
Topic 3. Evidence of digital forensics	2	-	5
Topic 4. Crime scene	8	30	68
Topic 5. Digital forensic sub domains	8	-	16
Topic 6. Anti-forensics	4	6	14
Topic 7. Examination and analysis	2	3 (4/2)*	14 (13/15)*
In total:	**34**	**51** (52/50)*	**155** (154/156)*

* By the numerator / by the denominator (calculation is carried out in accordance with the class schedule)

EDUCATIONAL DISCIPLINE PROGRAM

Content of the lecture course

Number lectures	List of lecture topics, their annotations	Number of hours
Topic 1. Introduction to Digital Forensics Science (DFS)		
1	**Introduction to Digital Forensics.** 1. Introduction to digital forensics 2. Definition of digital forensics 3. Science of digital forensics 4. Communities in the field of digital forensics 5. Digital Forensics, Cyber Forensics or Computer Forensics? 1. 6. Definition of digital forensics - parasitic myths and influence of media. Lit.: [1] c.3-17, c.33-39, c.57-61; [22] c.29-70.	2
2	**Basic concepts and definitions of digital forensics.** 1. The context of digital forensics 2. Measures of cyber forensics 3. Digital forensics in different contexts 4. Scientific approach in digital forensics 5. Summary by topic 1 Lit.: [6] c.26-50; [7] c.17-27.	2
Topic 2. Basics of computer literacy of a DFC specialist		
3	**Hard drives are a physical and logical organization** 1. Basics of computer literacy - learning goals 2. The main types of discs 3. Hard Disk Drive (HDD) vs. Solid State Drive (SSD) 4. Hard disk structures (HDD) 5. Calculation of storage capacity 6. Hard disk addressing Lit.: [2] c.153-156.	2
4	**Disk partitioning** 1. Partition or division of the disk into sections and types of formats 2. The main table of sections 3. Partition type codes, partition type hex codes 4. Disk partitioning options 5. Hidden sections 6. Host Protected Area (HPA) 7. Disk Configuration Overlay (DCO) Lit.: [2] c.156-159	2
5	**Boot process** 1. Boot process – basic concepts 2. Boot process – format for older versions (Legacy) 3. The boot process is UEFI 4. Boot process – Windows UEFI 5. The loading process is POST 6. Windows boot process 7. Linux boot process 8. Unix boot process 9. Mac OS boot process Lit.: [2] c.159-190.	2

Topic 3. Evidence of digital forensics		
6	**Evidence location and types** 1. Types of digital evidence 2. Location of evidence 3. Location of evidence - e-mail 4. Location of evidence - printers 5. Location of evidence – Roku devices, Fire Sticks media players 6. Location of evidence - routers (routers) 7. Evidence location – Raspberry Pi (single board computers) 8. Geolocation 9. Photos and videos 10. EXIF (Exchangeable Image File Format) [Metadata] 11. Location of iPhone 12. IP geolocation 13. Locations by social networks 14. Geolocation tags for social networks 15. Location of cell towers Lit.: [2] c.13-48; [5]	2
Topic 4. Crime scene		
7	**The principle of exchange and collection of evidence at the crime scene** 1. The principle of exchange 2. What is a crime scene? 3. Evidence 4. Principles of forensic science 5. Discovery of digital (electronic) evidence 6. Procedures to be followed at a crime scene 7. Checklist justified from the point of view of criminology 8. Sets for the work of a forensic expert on the road Lit.: [2] c.61-84.	2
8	**Digital (electronic) evidence** 1. Digital (electronic) evidence 2. Removal and preservation of evidence 3. Evidence on the computer 4. Evidence on the phone 5. Evidence in cloud storage 6. Evidence in the network 7. Investigative Environment (IE) 8. IE - Techniques 9. IE – Daubert Reasoning 10. IE – Tools 11. IE - Technologies 12. IE - Automation 13. IE – Planning Lit.: [2] c.39-40; [10] c.33-64	2
9	**Digital forensics tools** 1. A brief overview of digital forensics tools 2. Hardware write blockers 3. Software write blockers 4. Why images/images are used 5. Bit-by-bit copy (bit stream copy) vs. backup copy 6. Forensic image (image): Physical disk 7. Forensic image (image) of a logical volume	2

	8. MD5 hash function for data image (image) integrity 9. Overview of imaging software 10. Image creation software – FTK Imager 11. Mobile systems for the work of a field forensic expert (MFS) 12. Requirements for disk imaging tools 1. 13. Sets for the work of a forensic expert on the move Lit.: [3] c.19-33	
10	**Examination** 1. Forensic thinking 2. Chronology of events within the framework of the investigation 3. MAC times (parts of file system metadata) 4. Organization of the investigation 5. Questions within the framework of the investigation 6. Model of evidence examination in digital forensics 7. Questions within the framework of the investigation - Requests/Requests 8. Windows registry 9. HKEY_CLASSES_ROOT 10. Registry tools 11. The ntuser.dat and index.dat files 12. Proceedings management tools Lit.: [2] c.61-84; [10] c.164-267	2
Topic 5. Digital forensic sub domains		
11	**Host forensics** 1. Forensics of hosts - objects 2. Host forensics 3. Forensics of hosts - virtual machines Lit.: [2] c. 275-314 ; [4] c. 119-131	2
12	**E-mail forensics** 1. Forensics of e-mail and instant messages - introduction 2. Forensics of e-mail and instant messages 3. E-mail investigation Lit.: [2] c. 275-314 ; [4] c. 119-131	2
13	**Network forensics** 1. What is network forensics? 2. Fundamentals of forensic network analysis 3. Network attacks 4. What evidence can be collected? 5. Network forensics tools 6. Things to remember for network forensics success Lit.: [4] c. 133-144	2
14	**Mobile device forensics** 1. Forensics of mobile devices - introduction 2. Forensics of mobile devices and Hedy Lamar 3. Adjusting the frequency 4. CDMA 5. Mobile phones in history 6. What are we interested in? Types of evidence 7. Forensics of mobile devices and embedded systems as a science 8. Synergy Lit.: [2] c. 191-274; [4] c. 145-161	2

Topic 6. Anti-forensics		
15	**Anti-forensics in terms of techniques and operating systems** 1. Common techniques 2. Anti-forensics 3. Area of swapping 4. Anti-criminology Windows 5. Anti-criminology FS Unix 6. Reserved space 7. Alternative data streams (ADS) 8. Summary of data hiding Lit.: [4] c. 83-103	2
16	**Anti-forensics of file structures. Steganography and steganoanalysis** 1. Delete, reformat and recycle bin 2. Saving files in NTFS 3. Deleted files 4. Deleting the file 5. Sending to the basket / deleting the catalog 6. Deleted files in NTFS 7. Fillers 8. INFO2 file 9. Desktop.ini 10. Steganography 11. Steganoanalysis 12. Tools for detecting traces of steganography Lit.: [4] c. 83-103	2
Topic 7. Examination and analysis		
17	**Examination and analysis. Attribution** 1. Models of investigation • ADFM • IDIP • EIDIP • HOBFDIP 2. Criticism of models 3. Digital crime scene analysis 4. Qualitative forensic procedure 5. Analysis of categories 6. Requirements for analytical tools 7. Summary of the lecture 8. Attribution Lit.: [4] c.27-36, [5]	2
	In total:	**34**

Contents of laboratory work

№	Topic of the laboratory lesson Number of hours	Number of hours
1	Collection and analysis of digital forensic information by means of the operating system Lit.: [2] c. 185-190; [4] c. 65-82	6
2	Retrieving digital forensic information locked by password authentication. Lit.: [1] c. 24-29	6
3	Recovery of hidden and destroyed digital forensic information on drives of various types. Lit.: [2] c. 147-184	6
4	Collection and analysis of digital forensic information by the program for electronic examination FTK. Lit.: [4] c. 38-46	6
5	Collection and analysis of digital forensic information from data carriers by the Autopsy program Lit.: [2] c. 34-49	6
6	Collection and analysis of digital forensic information on the Internet. Lit.: [2] c. 275-314 ; [4] c. 119-131	6
7	Collection and analysis of digital forensic information from mobile devices using Wondershare Dr.Fone for Android Lit.: [2] c. 191-274; [4] c. 145-161	6
8	Anti-criminology with the tools of steganography Lit.: [4] c. 83-103	6
9	Final lesson. Testing.	3 (4/2)*
	In total:	**51** (52/50)*

* By the numerator / by the denominator (calculation is carried out in accordance with the class schedule

Content of independent (including individual) work

Students are assigned to study the lecture material, prepare for the performance and defense of laboratory work. Management of independent work and task performance is carried out by the teacher according to the schedule of consultations outside of class time, including with the use of interactive and distance learning technologies.

Week number	Type of independent work	Number of hours
1	Development of theoretical material, preparation for performance of LW1	9
2	Development of theoretical material, preparation for the defense of LW1	9
3	Development of theoretical material, preparation for performance of LW2	9
4	Development of theoretical material, preparation for the defense of LW2	9
5	Development of theoretical material, preparation for performance of LW3	9
6	Development of theoretical material, preparation for the defense of LW3.	10
7	Development of theoretical material, preparation for performance of LW4	9
8	Development of theoretical material, preparation for the defense of LW 4	9
9	Development of theoretical material, preparation for performance of LW5	9
10	Development of theoretical material, preparation for the defense of LW5	9
11	Development of theoretical material, preparation for performance of LW6	9
12	Development of theoretical material, preparation for the defense of LW6	9
13	Development of theoretical material, preparation for performance of LW7	9
14	Development of theoretical material, preparation for the defense of LW7	9
15	Development of theoretical material, preparation for performance of LW8	9
16	Development of theoretical material, preparation for the defense of LW8	9
17	Development of theoretical material. Preparation for final testing.	10 (9/11)*
	In total:	**155** (154/156)*

Conventional designations: LW - laboratory work

* By the numerator / by the denominator (calculation is carried out in accordance with the schedule of laboratory classes)

TECHNOLOGIES AND TEACHING METHODS

The teaching process in the discipline is based on the use of traditional and modern methods, in particular: lectures using verbal, visual and interactive methods and visualization (lectures); laboratory work using practical, problematic, productive methods, training workshops, independent work involves explanatory and illustrative and research methods.

The teaching methods used in teaching the discipline contribute to the development of soft skills in students: performing part of the laboratory work involves working in small groups with the appointment of a team leader, which contributes to the development of leadership qualities in students, the ability to communicate and organize teamwork on joint tasks, and changeability the composition of working groups between laboratory works promotes the development of adaptability, flexibility, communication skills and the prompt establishment of interpersonal relations in different teams; communication on problematic issues during lectures, public defenses of laboratory works with justification of the decisions made regarding the choice of methods for solving tasks in dialogue with the teacher and the group contribute to the formation and improvement of public speaking skills, empathic listening, defending one's own point of view, introspection and self-criticism; adaptability, the ability to use Internet resources and other sources of information, synthesize and critically interpret information from various sources provided for by the specifics of the discipline, which involves solving problematic tasks using creative approaches; limited time for performing laboratory work and test tasks, clearly defined deadlines for passing checkpoints and working off debts contribute to the development of punctuality, the ability to self-organize and manage time (time management).

Necessary tools, equipment, software: PC with connection to a local network and the Internet, operating systems (Windows, Kali Linux, etc.), programs for collecting digital forensic information (FTK, Autopsy, Wondershare Dr.Fone for Android).

CONTROL METHODS

Current control is carried out during laboratory classes, as well as on the days of control activities established by the work plan of the discipline.

At the same time, the following methods of current control are used:

– oral survey;
– protection of laboratory work;
– testing.

When deriving the final semester grade, the results of the current control are taken into account (credit by rating is formed automatically based on the results of the current control).

ASSESSMENT OF STUDENT LEARNING OUTCOMES

The evaluation of the student's academic achievements is carried out in accordance with the "Regulations on control and evaluation of the results of studies of students of higher education at KhNU". Each type of work in the discipline is evaluated on an institutional four-point scale. The semester final grade is defined as a weighted average of all types of academic work completed and passed positively, taking into account the weighting factor. The weighting factors change depending on the structure of the discipline and the importance of certain types of its work.

The structuring of the discipline by types of work and the assessment of student learning results in the semester by weighting coefficients

Auditory work	Control measures	Final control measure

Laboratory work №:		Test control 1	Test control 2	Semester control
1 - 8		T 1	T 2-3	Credit
VK:	0,8	0,2	0,2	

Assessment of laboratory work. The grade given for the laboratory session consists of the following elements: an oral survey of students before admission to the laboratory work; knowledge of theoretical material on the topic; the quality of protocol and report execution; the student's fluency in special terminology and the ability to professionally justify the decisions made; timely protection of laboratory work.

The deadline for the defense of the laboratory work report is considered timely if the student defended it on the day of completion or at the next class after completion of the work. The student is obliged to complete the missed laboratory class in the department's laboratories by the deadline set by the teacher, with registration in the department's journal, but no later than two weeks before the end of the theoretical classes in the semester.

The teacher announces the grade for the laboratory session immediately after the defense of the report on the laboratory work and puts it in the electronic journal of the discipline.

Evaluation of test tasks. The thematic test for each student consists of fifteen test tasks, each of which is evaluated by one point. The maximum number of points a student can score is 15.

Correspondence of the scored points for the test task to the grade assigned to the student

The sum of points for the test task	1–5	6–10	11–13	14–15
Evaluation on a 4-point scale	2	3	4	5

15 minutes are allotted for testing (for closed-form tests – one minute for each task). The student records the correct answers in the answer sheet. At the same time, all answer columns must be filled with numbers that correspond to the correct, in the student's opinion, answers. After 15 minutes, students hand in the task with answer sheets to the teacher.

The student can also take the test online in the MOODLE modular learning environment.

The teacher puts the grade for testing in the electronic journal of the discipline.

If a student received a negative grade for a certain type of work, he must resubmit it in the established order, but necessarily before the next inspection deadline.

In the event that the student did not complete the individual discipline plan within the scheduled time without valid reasons, he will be given a grade of "satisfactory" during the course of working off the debt, with a positive answer.

A student who has not completed the individual plan of current work on the discipline in full or in part within the prescribed time frame is not allowed to take the final test.

The credit is considered passed when the student receives a final grade of 3.00 to 5.00 points based on the combined results of the current control. At the same time, according to the national scale, the grade is given on a two-point scale, and according to the ECTS scale, the grade corresponding to the number of points scored by the student is given.

The final semester grade according to the institutional scale and the ECTS scale is set in an automated mode after the teacher enters all the grades into the electronic journal.

The student's assimilation of the theoretical material of the discipline is assessed according to the knowledge assessment criteria listed in the table.

Criteria for evaluating students' knowledge

Evaluation according to the institutional scale	Generalized criterion
1	*2*
Excellent	The student has deeply and completely mastered the content of the educational material, easily navigates in it and skillfully uses the conceptual apparatus; knows how to connect theory with practice, solve practical tasks, confidently express and justify his judgments. An excellent assessment implies a logical presentation of the answer in the national language (in oral or written form), demonstrates high-quality design of work and mastery of special tools. The student does not hesitate when changing the question, knows how to make detailed and generalizing conclusions. When answering, he made two or three insignificant mistakes.
Good	The student has fully mastered the educational material, has a conceptual apparatus and professional terminology, orients himself in the studied material; consciously uses theoretical knowledge to solve practical problems; the presentation of the answer is competent, but the content and form of the answer may contain some inaccuracies, unclear formulations of regularities, etc. The student's answer is based on independent thinking. The student made two or three minor mistakes in the answer.
Satisfactory	The student has demonstrated knowledge of the main program material in the amount necessary for further education and practical work in the profession, copes with the implementation of practical tasks provided for by the program. As a rule, the student's answer is built on the level of reproductive thinking; the student has weak knowledge of the course structure, makes inaccuracies and significant mistakes in the answer, and hesitates when answering a modified question. At the same time, he acquired the skills necessary to perform simple practical tasks that meet the minimum assessment criteria and has knowledge that allows him to eliminate inaccuracies in answers under the guidance of a teacher.
Unsatisfactory	The student has found scattered, unsystematic knowledge, does not know how to distinguish the main and secondary, makes mistakes in defining concepts, distorts their meaning, presents the material chaotically and uncertainly, cannot use knowledge when solving practical tasks. As a rule, the grade "unsatisfactory" is assigned to a student who cannot continue his studies without additional work on studying the discipline.

Correlation of the domestic evaluation scale and the ECTS evaluation scale

Evaluation of ECTS	Institutional interval scoring scale	Institutional assessment, assessment criteria		
A	4,75–5,00	5	Counted in	**Excellent** - deep and complete mastery of the educational material and identification of relevant skills and abilities
B	4,25–4,74	4		**Good** - complete knowledge of the educational material with a few minor errors
C	3,75–4,24	4		**Good** - a generally correct answer with two or three significant errors
D	3,25–3,74	3		**Satisfactory** - incomplete mastery of software material, but sufficient for practical activity by profession
E	3,00–3,24	3		**Satisfactory** - incomplete mastery of the program material that meets the minimum evaluation criteria
FX	2,00–2,99	2	Not counted	**Unsatisfactory** - the unsystematic nature of the acquired knowledge and the impossibility of continuing education without additional knowledge of the discipline
F	0,00–1,99	2		**Unsatisfactory** - serious further work and re-study of the discipline is necessary

QUESTIONS FOR SELF-CONTROL OF LEARNING RESULTS OBTAINED BY STUDENTS

1. Prerequisites for the emergence of digital forensics. Areas of application of digital forensics.
2. The main tasks of digital forensics.
3. Communities of digital forensics.
4. Digital Forensics, Cyber Forensics and Computer Forensics - a comparative analysis.
5. "Three A" of digital forensics.
6. Locar exchange principle.
7. Measures of cyber forensics.
8. Digital forensics in different contexts.
9. Forensics is an applied science of solving crimes related to computer information.
10. The concept of computer crime.
11. Forensic characteristics. Statistics. The identity of the alleged criminal. Operativeness.
12. Typical computer crimes and the action of a forensic scientist: identification of the method of creation, the criminal, the traces, the victim.
13. Traffic fraud: identification of the method of creation, perpetrator, traces, victim.
14. Offline copyright infringement: identification of the method of creation, the perpetrator, the traces, the victim.
15. Violation of copyright on the Internet: identification of the method of creation, the perpetrator, the traces, the victim.
16. Phishing: identification of the method of creation, perpetrator, traces, victim.
17. Cybersquatting: identification of the method of creation, perpetrator, traces, victim.
18. Payments via the Internet: identification of the method of creation, the perpetrator, traces, the victim.
19. Cheating in online games: identification of the method of creation, perpetrator, traces, victim.
20. Use of RBL: identification of the method of creation, perpetrator, traces, victim.
21. Fraud: identification of the method of creation, the criminal, the traces, the victim.
22. Legal evaluation of crimes.
23. Rules for handling evidence (evidence management) in response to incidents.
24. Stage of preparation in response to incidents.
25. Detection and analysis procedures in responding to incidents.
26. Restraint in responding to incidents.
27. Elimination of consequences in response to incidents. Restoration.
28. Activities after a cyber incident.
29. Identification of problematic aspects of digital forensics.
30. Technical problems of digital forensics.
31. Legal aspects and problems of digital forensics.
32. Problems of forensics of mobile technologies. Problems of forensics in network systems.
33. Analysis of the principles of the structure of modern computers as an object of digital forensics.
34. Information carriers are physical and logical structures.
35. Basic methods of hiding digital evidence.
36. Search and recovery of digital evidence.
37. Types of digital evidence.
38. Methods of finding digital evidence.
39. Obtaining and securing digital evidence.
40. Processes and services of operating systems. Tools of operating systems as tools of digital forensics.

41. Interception and investigation of traffic. Encrypted traffic. Study of traffic statistics. Netflow.

42. Kruse and Heiser's model.

43. Model of the US Department of Justice (USDOJ).

44. DFRWS model.

45. Abstract digital forensic model.

46. Integrated Digital Investigation Process (IDIP).

47. Model of the Enhanced Digital Investigation Process (EDIP).

48. Computer Forensic Field Triage Process Model (CFFTPM).

49. General Computer Forensic Investigation Process Model (GCFIPM).

50. Classification, principles of operation and purpose of means of investigation of digital incidents and protection of information.

51. Record blockers.

52. Data recording equipment.

53. Problems of storage, transmission and processing of digital evidence in computer forensics.

54. Principles and methods of preventing information leakage. Means of preventing information leakage: data destruction devices, information safes, etc.

55. Methods of steganography and concealment of digital evidence. Hiding data in text files.

56. Hiding data in still images.

57. Hiding data in the spatial domain and in the frequency set of images.

58. Hiding data in sound and video files.

METHODOLOGICAL SECURITY

The educational process in the discipline "Digital Forensics" is fully and in sufficient quantity provided with the necessary educational and methodical literature, placed in an electronic version in a modular environment.

RECOMMENDED LITERATURE

Main

1. Цифрова криміналістика : консп. лекцій / уклад. І. З. Якименко. - Тернопіль : ТНЕУ, 2019. - 109 с.
2. Digital Forensics / Edited by André Årnes. – John Wiley & Sons Ltd, 2018. – 336 p.
3. Cybercrime: University Module Series, Teaching Guide. / United Nations Office on Drugs and Crime. – Vienna, United Nations, Doha Declaration, 2019. – 453 p.
4. Digital Forensics Basics: A Practical Guide Using Windows OS/ Edited by Nihad A. Hassan. – New York, 2019. – 335 p.
5. Самойленко О. А. Виявлення та розслідування кіберзлочинів: навчально-методичний посібник / О. А. Самойленко. Одеса : , 2020. 112 с.
6. Даник Ю.Г. Основи кібербезпеки та кібероборони: підручник / Ю. Г. Даник, П. П. Воробієнко, В. М. Чернега. – Видання друге, перероб. та доп. – Одеса : ОНАЗ ім. О.С. Попова, 2019. − 320 с.
7. Комп'ютерна стеганографічна обробка й аналіз мультимедійних даних: підручник. / Г. Ф. Конахович, Д. О. Прогонов, О. Ю. Пузиренко. – Київ: «Центр учбової літератури», 2018. – 558 с
8. Кузнецов О. О. Стеганографія : навчальний посібник / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2011. – 232 с.
9. The Basics of Digital Forensics The Primer for Getting Started in Digital Forensics. Second Edition / John Sammons. – Elsevier Inc., 2015. – 180 p.
10. Микитишин А. Г. Комплексна безпека інформаційних мережевих систем: навчальний посібник / А.Г. Микитишин, М.М. Митник, П.Д. Стухляк. .– Тернопіль: ТНТУ, 2016. – 255 с.
11. Practical Information Security: A Competency-Based Education Course / [Izzat Alsmadi, Robert Burdwell, Ahmed Aleroud, Abdallah Wahbeh, Mahmoud Ali Al-Qudah, Ahmad Al-Omari]. – Cham, Switzerland : Springer International Publishing AG, 2018. – 328 p.
12. Про національну безпеку України: Закон України [Електронний ресурс] / Затверджено Указом Президента України від 21 червня 2018 року № 2469^Ш – Режим доступу: https://zakon.rada.gov.ua/laws/show/2469-19. – Назва з екрану.
13. Стратегія кібербезпеки України [Електронний ресурс] / Указ Президента України від 15.01.2016 р. № 96/2016 – Режим доступу:. https://zakon5.rada.gov.Ua/laws/show/96/2016#n11. – Назва з екрану.
14. Стратегія національної безпеки України [Електронний ресурс] / Указ Президента України від 06.05.2015р. № 287/2015 – Режим доступу: https://zakon.rada.gov.ua/laws/show/287/2015. – Назва з екрану.

Additional

15. ДСТУ ISO/IEC 27032:2016 (ISO/IEC 27032:2012, IDT). Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки. – Чинний від 2016-27-12. – Київ : ДП «УкрНДНЦ», 2018. – [50] с.
16. Kim D. Fundamentals of information systems security / David Kim, Michael G. Solomon. – Third edition. – Burlington :Jones & Bartlett Learning, 2018. – 571 p.
17. Поняття та класифікація віртуальних слідів кіберзлочинів // Я. Найдьон. / Криміналістика. – 2019. – №5. – С. 304-307.
18. Проблеми застосування інформаційних технологій правоохоронними структурами України та закладами вищої оевітм зі специ* фінними умовами навчання : збірник наукових етатей за матеріалами доповідей Всеукраїнської науково-практичної конференції 21 грудня 2018 року / упорядник Т. В. Маїеровська / - Львів: ЛьвДУВС, 2018.-281 с.

19. Авдєєва Г. К. Сутність цифрових слідів в криміналістиці / Г. К. Авдєєва // Актуальні питання судової експертизи та криміналістики : зб. матеріалів міжнар. наук.-практ. конфер., присвяч. 95-річчю створення Харків. НДІ суд. експертиз ім. засл. проф. М. С. Бокаріуса (Харків, 10–11 жовт. 2018 р.). – Харків, 2018. – С. 90–93.

20. Evaluation of Digital Forensic Process Models with Respect to Digital Forensics as a Service // Xiaoyu Du, Nhien-An Le-Khac, Mark Scanlon / 16th European Conference on Cyber Warfare and Security (ECCWS 2017) At: Dublin, Ireland, June 2017. – P. 46-57.

21. Шеломенцев В. П. Віртуальність як елемент характеристики кіберзлочинів. Часопис Національного університету "Острозька академія". Серія "Право". – 2011. – №1(3). – С. 1-15

22. Cybersecurity: Geopolitics, Law, and Policy / Amos N. Guiora; Professor of Law at the S.J. Quinney College of Law, University of Utah, USA. – New York : Taylor & Francis Books, 2017. ¬– 177 p.

23. Гладун А.Я. Таксономія стандартів інформаційної безпеки / А.Я. Гладун, К.О. Хала // Наука, технології, інновації. – 2017. – № 2. – С. 53-64

24. Shojaie B. Implementation of Information Security Management Systems based on the ISO/IEC 27001 / Bahareh Shojaie. - Dissertation with the aim of achieving a doctoral degree at the Faculty of Mathematics, Informatics and Natural Sciences Department of Informatics of Universit¨at Hamburg. February 20, 2018. 147 p.

25. Кондратенко Ю. В. Візуальний аналіз політик безпеки в ERP-системах / Ю. В. Кондратенко, І. Г. Зотова, В. В. Грицюк // Збірник наукових праць Центру воєнно-стратегічних досліджень НУ оборони України ім. Івана Черняховського. – 2018. – № 1. – С. 68-73.

26. Stevens C. Assembling cybersecurity: The politics and materiality of technical malware reports and the case of Stuxnet / Clare Stevens // Contemporary Security Policy. – 2020. – Volume 41, Issue 1: Special issue: Cyber Security Politics. – P. 129-152.

27. Аналіз нормативно-правових та організаційно-технічних аспектів забезпечення інформаційної безпеки / [В. В. Овсянніков, С. В. Дехтяр, С. А. Паламарчук, Ю. О. Черниш, О. В. Шемендюк]. // Сучасні інформаційні технології у сфері безпеки та оборони. – 2015. – № 3(24). – С. 187-193.

28. Борсуковський Ю. В. Визначення сучасних вимог до створення політики управління доступом корпоративних користувачів / Ю. В. Борсуковський // Сучасний захист інформації. – 2016. – № 4. – С. 5-9.

29. Борсуковський Ю. В Визначення сучасних вимог щодо політики використання засобів криптографічного захисту інформації на підприємстві / Ю. В. Борсуковський // Сучасний захист інформації. – 2018. – № 1. – С. 74-81.

30. Ахрамович В. М. Адміністративний рівень інформаційної безпеки / В. М. Ахрамович // Сучасний захист інформації. – 2017. – № 1. – С. 10-14.

31. Dunn M. Cyber security meets security politics: Complex technology, fragmented politics, and networked science / Myriam Dunn Cavelty, Andreas Wenger // Contemporary Security Policy. – 2020. – Volume 41, Issue 1: Special issue: Cyber Security Politics. – P. 5-32.

32. Hend K. Alkahtani. Safeguarding the Information Systems in an Organization through Different Technologies, Policies, and Actions / Hend K. Alkahtani // Computer and Information Science. – Vol. 12, No. 2; 2019. – ISSN 1913-8989, E-ISSN 1913-8997. – Published by Canadian Center of Science and Education. – P. 117-125.

33. Інноваційні методи та цифрові технології в криміналістиці, судовій експертизі та юридичній практиці : матеріали міжнар. «круглого столу» (Харків, 12 груд. 2019 р.) / редкол.: В. Ю. Шепітько (голов. ред.), В. А. Журавель, В. М. Шевчук, Г. К. Авдєєва. – Харків : Право, 2019. – 164 с.

34. Digital forensic readiness framework based on honeypot and honeynet for byod // Audrey Asante, Vincent Amankona. / Journal of Digital Forensics. – Vol. 16 (2021). – P. 1-17.

35. Forensic of an unrooted mobile device // Animesh Kumar Agrawal, Aman Sharma, Sumitra Ranjan Sinha and Pallavi Khatri / International Journal of Electronic Security and Digital Forensic. – 2019. – Vol. 12, No. 1 – P. 118-137.

36. Russia Today, Cyberterrorists Tomorrow: U.S. Failure to Prepare Democracy for Cyberspace // Jonathan F. Lancelot, Norwich UniversityFollow / Journal of Digital Forensics. – Vol. 13 (2018). – P. 23-32.

37. Application of quality in use model to assess the user experience of open source digital forensics tools // Manar Abu Talib, Reem Alnanih and Adel Khelifi / International Journal of Electronic Security and Digital Forensic. – 2019. – Vol. 12, No. 1 – P. 43-76.

38. A Two-Stage Model for Social Network Investigations in Digital Forensics // Anne David, Sarah Morris, Gareth Appleby-Thomas. / Journal of Digital Forensics. – Vol. 15 (2020). – P. 1-36.

39. Hemdan, E.ED., Manjaiah, D. An efficient digital forensic model for cybercrimes investigation in cloud computing. Multimed Tools Appl 80, 14255–14282 (2021).

40. Solanke, A.A., Biasiotti, M.A. Digital Forensics AI: Evaluating, Standardizing and Optimizing Digital Evidence Mining Techniques. Künstl Intell 36, 143–161 (2022).

INFORMATION RESOURCES

1. MOODLE - modular learning environment. Access to the resource: https://msn.khmnu.edu.ua/ .
2. University electronic library. Access to the resource: http://library.khmnu.edu.ua/ .