PROGRAM OF THE DISCIPLINE
Cybercrime and Digital Evidence
(The name of discipline)

A short description of substantive area	The XIX century was an era of total informatization and cybernetics of all spheres of life in most countries. On the one hand, it allowed to improve and simplify people's lives, on the other hand, it created new challenges. Therefore, the study of issues related to the protection of cyberspace is very relevant today and requires additional attention, including in the training of specialists. The main threats in this area are cyber attacks and cybercrime, etc., which are defined in national and international regulations. In recent years, cybercrime has reached alarming proportions not only in Ukraine but in the world. This is largely due to the lack of proper international cooperation and the rapid processes taking place in the cyber environment. Every year, technology changes, new data systems are created, software is used by criminals, and so on. Of course, this requires adequate measures to respond to and prevent threats, which should be based on scientific and practical recommendations.

2. The structure of the discipline	
Types of caseload	Hours
The amount of credits/ hours	3 / 90
Total hours of classwork, including:	**40**
• Lectures, hours	20
• Practical training, hours	20
• Seminars, hours	-
Total hours of independent study, including:	**50**
• Individual research task, hours	3
• Quiz	2
• Preparation to classwork and control activities, hours	45
Credit	

Lecture session			
Content symbol	Content symbol	Reference to the PH of discipline	Hours
1.	Topic 1. Cybercrime: concepts, types and prevention. 1. The concept of cybercrime and its place in the overall structure of crime. Types of cybercrime. 2. European Convention on Cybercrime Prevention Mechanism: concept and system. 3. Determinants and main directions of cybercrime prevention		4
2.	Topic 2. Criminal law support in the fight against cybercrime.		6

	1. The current state of criminal law in the fight against cybercrime. 2. System and general characteristics of cybercrimes. 3. Implementation of forms of criminal liability for cybercrime.		
3.	Topic 3. Features of the methodology of cybercrime investigation 1. Forensic characteristics of cybercrime. 2. Characteristics of tactics for the investigation of cybercrime. 3. Features of the use of computer technology in the prevention and investigation of cybercrime. 4. Technical features of the inspection of computer equipment found at the scene		6
4.	Topic 4. Electronic evidence in criminal proceedings 1. The concept of electronic evidence in criminal proceedings 2. Types of electronic evidence 3. Methods of collecting electronic evidence 4. Use of electronic evidence during the trial		4

Practical training			
Content symbol	Content symbol	Reference to the PH of discipline	Hours
1.	Theme 1. The concept of restorative justice in criminal proceedings	1, 5	2
2.	Theme 2. Features of negotiations and mediation in criminal proceedings	1, 2, 3, 4, 5	6
3.	Theme 3. Proceedings on the basis of agreements as a special procedure of criminal proceedings in Ukraine	1, 2, 3, 4, 5	2
4.	Theme 4. Criminal proceedings for release from criminal liability	1, 2, 3, 4, 5	2
5.	Theme 5. Features of application of psychological knowledge in the decision of criminal conflict from the point of view of restorative justice	1, 2, 5	2

Independent study			
Content symbol	Description of content (for example themes and kinds of education activity)	Reference to the PH of discipline	Hours
1.	Preparation for training sessions and control activities	1,2,3, 4, 5	15