МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Львівський національний університет імені Івана Франка
Факультет прикладної математики та інформатики
Кафедра кібербезпеки

Затверджено
На засіданні кафедри кібербезпеки
факультету прикладної математики та інформатики
Львівського національного університету імені Івана Франка
(протокол № 4/23 від 29 серпня 2023 р.)

Завідувач кафедри .

Венгерський П.С.

ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені ІВАНА ФРАНКА
МЕХАНІКО-
МАТЕМАТИЧНИЙ
ФАКУЛЬТЕТ
* * *

Силабус з навчальної дисципліни

“ Кібербезпека ”,

що викладається в межах ОПП «Статистичний аналіз даних» другого (магістерського) рівня вищої освіти для здобувачів з спеціальності 112 – статистика

Львів 2023 р.

Назва дисципліни	CyberSecurity
Адреса викладання дисципліни	Universytetska St, 1, Lviv, L'vivs'ka oblast, 79000
Факультет та кафедра, за якою закріплена дисципліна	Faculty of Applied Mathematics and Informatics CyberSecurity department
Галузь знань, шифр та назва спеціальності	11 – Mathematics and Statistics 112 – Statistics
Викладачі дисципліни	Roman Karpiuk, Assistant of the CyberSecurity department
Контактна інформація викладачів	roman.karpiuk@lnu.edu.ua
Консультації з питань навчання по дисципліні відбуваються	Consultations on the day of lectures/practical classes (by prior arrangement).
Сторінка курсу	https://ami.lnu.edu.ua/admission/specializations
Інформація про дисципліну	The discipline "Cybersecurity" is a normative discipline from the specialty 112 - statistics for the educational program “Statistical data analysis”, which is taught in the 2 semester in the amount of 5 credits (according to the ECTS European Credit Transfer System).
Коротка анотація дисципліни	The course is aimed at developing students' professional competencies, building a knowledge base on fundamental cybersecurity tools, specifically tools for "defense" and "offense," basic cybersecurity concepts, and fundamental network configuration principles from a cybersecurity perspective.
Мета та цілі дисципліни	The course aims to equip students with practical skills in using popular cybersecurity tools (NMAP, AngryIPScanner, IDS, Vulnerability Management, SIEM), understanding the principles of a "secure network," and the attack cycle on an organization's infrastructure.
Література для вивчення дисципліни	1. Cybersecurity Fundamentals/ ISACA/ www/isaca/org/cyber? Cybersecurity Funamentals Study Guide/ 2003.- 156 p. 2. SIEM “Splunk” documentations - https://docs.splunk.com/Documentation 3. Vulnerability scanner “Tenable” documentations – https://docs.tenable.com/ 4. IDS “Suricata” documentations – https://suricata.readthedocs.io/en/suricata-6.0.5/ 5. MITRE - https://attack.mitre.org/ 6. MITRE Defend - https://d3fend.mitre.org/ 7. Attack killchain overview - https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cyber-101-july2017.pdf
Обсяг курсу	Total duration: 150 hours. Classroom sessions: 48 hours, including 32 hours of lectures and 16 hours of practice work. Self-study: 102 hours.

Очікувані результати навчання	Upon completing the course, students should have acquired the following competencies: Knowledge: - Understanding of network operations - Understanding of operating systems - Knowledge of security perimeter concepts - Understanding of the attack chain - Basic knowledge of attack indicator detection systems Skills: - Proficiency in working with the following tools: - SIEM "Splunk" - IDS "Suricata" - Vulnerability Scanner "Tenable" - NMAP The course is designed to ensure the development of these competencies: ЗК6, СК7, PH5, PH7, PH11
Ключові слова	CyberSecurity, Cyber attack, Threat, Vulnerability, Privacy, Data Security, IDS, IPS, SIEM, Scanner, Vulnerability.
Формат курсу	In-person. Conducting lectures, laboratory work, and consultations..
Теми	- Updating knowledge about the operation of basic network services and operating systems (DNS\DHCP, TCP\IP stack, NAT\PAT, DMZ, TCP\UDP, TCP-handshake, TLS, AD, DC, etc.) - Blue Team VS Red Team - Concept of "depth" and "perimeter" security - Attack kill-chain - Tools: - Network security devices (firewalls, WAF, NGFW) - Network threat detection and prevention systems (IDS\IPS) - Vulnerability scanners - Security Information and Event Management (SIEM) systems - Attacker-side frameworks - Cryptography and cryptanalysis in the "applied" world
Підсумковий контроль, форма	Exam at the end of the semester
Навчальні методи та техніки, які будуть використовуватися під час викладання курсу	Presentations, lectures, practical tasks in the form of simulating attacks on a system, comprehensive analysis for investigating the attack, creating an incident report, and presenting the report to a hypothetical CISO (Chief Information Security Officer). Modular assessments.
Необхідне обладнання	Computers, computer systems, and networks. Virtual machines. Internet resources. Additional software in the form of trial versions for typical cybersecurity tools.
Критерії оцінювання (ок-	Evaluation is conducted on a 100-point scale, with points allocated as follows: - Modular assessments, tests, oral examinations: 50% of the semester

ремо для кожного виду навчальної діяльності)	grade; maximum score of 50. - Final exam: 50% of the semester grade; maximum score of 50. - The total maximum score is 100. Academic integrity is expected, and all student work should consist of original research or reasoning. Lack of citations for used sources, fabricating sources, plagiarism, and interfering with the work of other students are examples of possible academic dishonesty. The discovery of signs of academic dishonesty in a student's written work can result in non-crediting by the instructor, regardless of the scale of plagiarism or deception. Attendance is an important component of learning. It is expected that all students attend all lectures and practical classes in the course. Students should inform the instructor if they are unable to attend classes. In any case, students are required to meet the deadlines set for all types of written assignments and individual tasks outlined in the course. Literature: All literature that students cannot find on their own will be provided by the instructor exclusively for educational purposes, without the right to transfer it to third parties. Students are encouraged to use other literature and sources not included among the recommended readings. Grading policy: Points earned during ongoing testing, independent work, and final testing are taken into account. This includes attendance and student participation during practical sessions; the inadmissibility of absences and tardiness to classes; the use of mobile phones, tablets, or other mobile devices during classes for non-educational purposes; cheating and plagiarism; failure to complete assigned tasks in a timely manner, and so on. No forms of academic misconduct are tolerated.
Питання до екзамену.	1. Difference between cybersecurity and information security? 2. What does cybersecurity provide? 3. Why is DMZ necessary? 4. Design a typical network architecture in a standard organization. 5. How to implement centralized authentication for thousands of users? 6. TCP-handshake. 7. MITM (Man-in-the-Middle) attacks. 8. Build and justify the concept of a "secure perimeter." 9. What is needed for monitoring the security state in an organization? 10. How to establish a relatively secure working environment without a million-dollar budget? 11. With a million-dollar budget, where to begin? 12. MITRE ATT&CK framework. 13. What is EDR (Endpoint Detection and Response)? What is its role? 14. What is IDS (Intrusion Detection System)? What is its role? 15. What is SIEM (Security Information and Event Management)? What is its role? 16. What is DLP (Data Loss Prevention)? What is its role? 17. What is Vulnerability Management? What is the role of this process? 18. What is SSDLC (Secure Software Development Life Cycle)? What is the role of this process? 19. What is the difference between Vulnerability Management and Vulnerability Scanning? 20. Penetration Testing - why is it needed?

	21. How to use nmap? 22. Mimikatz - what is it about? 23. ATP (Advanced Threat Protection) - what is it, and what does it address? 1. 24. Forensics - explain and name the most popular tools.
Опитування	A course evaluation questionnaire for assessing the course's quality will be provided upon the completion of the course.