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 № 16/23 від 7 вересня 2023 р.)

Завідувач кафедри Петро ВЕНГЕРСЬКИЙ

Силабус з навчальної дисципліни
“Інструменти кібербезпеки”,
що викладається в межах ОПП Інформатика другого (магістерського) рівня вищої освіти для здобувачів зі спеціальності 122 Комп’ютерні науки

Львів 2023 р.

Назва дисципліни	Інструменти кібербезпеки
Адреса викладання дисципліни	Головний корпус ЛНУ ім. І. Франка м. Львів, вул. Університетська 1
Факультет та кафедра, за якою закріплена дисципліна	Факультет прикладної математики та інформатики Кафедра кібербезпеки
Галузь знань, шифр та назва спеціальності	12 – інформаційні технології 122 – комп'ютерні науки
Викладачі дисципліни	Трушевський Валерій Миолайович, кандидат фізико-математичних наук, доцент кафедри кібербезпеки; Карпюк Роман Валентинович, асистент\аспірант кафедри кібербезпеки
Контактна інформація викладачів	valeriy.trushevsky@lnu.edu.ua roman.karpiuk@lnu.edu.ua
Консультації з питань навчання по дисципліні відбуваються	Консультації в день проведення лекцій/практичних занять (за попередньою домовленістю).
Сторінка курсу	https://ami.lnu.edu.ua/admission/specializations
Інформація про дисципліну	Дисципліна "Інструменти кібербезпеки" є дисципліною за вибором з спеціальності 122–комп'ютерні науки для освітньої програми Інформатика, яка викладається в 1-му семестрі в обсязі 5.5-ти кредитів (за Європейською Кредитно-Трансферною Системою ECTS).
Коротка анотація дисципліни	Курс спрямований на формування у студентів професійних компетентностей, розвиток системи знань про основні базові інструменти в сфері кібербезпеки, а саме інструменти «захисту» та «нападу», базові поняття кібербезпеки та базові принципи конфігурування мережі в розрізі кібербезпеки.
Мета та цілі дисципліни	Метою курсу є формування у студентів практичних навиків використання популярних інструментів в сфері кібербезпеки (NMAP, AngryIPScanner, IDS, Vulnerability Management, SIEM), розуміння принципів «безпечної мережі» та циклу атаки на інфраструктуру організації.
Література для вивчення дисципліни	**Основна** 1. ISACA, Cybersecurity Fundamentals Study Guide 3rd Edition, 2021 2. Документація SIEM "Splunk" - https://docs.splunk.com/Documentation. Latest release notes – 2023. 3. Документація сканера вразливостей Tenable – https://docs.tenable.com/. Latest release notes – 2023. 4. Документація IDS "Suricata" – https://suricata.readthedocs.io/en/suricata-6.0.5/. Latest release notes – 2023. 5. MITRE - https://attack.mitre.org/. Latest release notes – 2023. Додаткова література: 1. P.W. Singer, Allan Friedman – "Cybersecurity and Cyberwar: What Everyone Needs to Know". 2. Richard A. Clarke, Robert K. Knake - "The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber

	Threats". 3. Evan Gilman, Doug Barth - "Zero Trust Networks: Building Secure Systems in Untrusted Networks". 4. Stuart McClure, Joel Scambray, George Kurtz - "Hacking Exposed: Network Security Secrets and Solutions". 5. David G. Ries, Daniel J. Solove - "Cybersecurity: A Practical Guide to the Law of Cyber Risk.
Обсяг курсу	Загальний обсяг: 165 годин. Аудиторних занять: 64 год., з них 32 год. лекцій та 32 год. лабораторних робіт. Самостійна робота: 101 год.
Очікувані результати навчання	У результаті вивчення навчальної дисципліни студент має набути таких компетентностей: **знати:** - функціонування мережі - функціонування операційних систем - «периметр» безпеки - ланцюг побудови атаки - базові системи виявлення індикаторів атак **вміти:** - працювати з наступними інструментами: • SIEM “Splunk” • IDS “Suricata” • Vulnerability Scanner “Tenable” • NMAP Курс забезпечує набуття таких компетентностей: ЗК1, ЗК2, ЗК4, ЗК5; та програмних результатів навчання: ПРН 1, ПРН 3, ПРН 4, ПРН 5, ПРН 9, ПРН 14, ПРН 15, ПРН 18, ПРН 19.
Ключові слова	Кібербезпека, кібератака, загроза, вразливість, конфіденційність, цілісність, безпека даних, IDS, IPS, SIEM, Scanner, Vulnerability.
Формат курсу	Очний. Проведення лекцій, лабораторних робіт і консультацій.
Теми	Теми подані у Схемі курсу нижче.
Підсумковий контроль, форма	Залік у кінці 1 семестру.
Навчальні методи та техніки, які будуть використовуватися під час викладання курсу	Презентації, лекції, практичні завдання у вигляді імітації атаки на систему, комплексної аналітики щодо розслідування атаки, формування звіту щодо інциденту та захисту звіту перед умовним CISO. Модульний контроль.
Необхідне обладнання	Комп’ютери, комп’ютерні системи та мережі. Віртуальні машини. Інтернет ресурси. Додаткове програмне забезпечення у вигляді trial-версій для типових інструментів з кібербезпеки.
Критерії оцінювання (окремо для кожного виду навчальної діяльності)	Оцінювання проводиться за 100-бальною шкалою. Бали нараховуються за наступним співвідношенням: • модульний контроль, тестування, усне опитування: 50% семестрової оцінки; максимальна кількість балів 50 • залік: 50% семестрової оцінки; максимальна кількість балів 50 Підсумкова максимальна кількість балів 100.

	Академічна доброчесність: Очікується, що роботи студентів будуть їх оригінальними дослідженнями чи міркуваннями. Відсутність посилань на використані джерела, фабрикування джерел, списування, втручання в роботу інших студентів становлять, але не обмежують, приклади можливої академічної недоброчесності. Виявлення ознак академічної недоброчесності в письмовій роботі студента є підставою для її незарахуванння викладачем, незалежно від масштабів плагіату чи обману. **Відвідання занять** є важливою складовою навчання. Очікується, що всі студенти відвідають усі лекції та практичні зайняття курсу. Студенти повинні інформувати викладача про неможливість відвідати заняття. У будь-якому випадку студенти зобов'язані дотримуватися термінів визначених для виконання всіх видів письмових робіт та індивідуальних завдань, передбачених курсом. **Література.** Уся література, яку студенти не зможуть знайти самостійно, буде надана викладачем виключно в освітніх цілях без права її передачі третім особам. Студенти заохочуються до використання також й іншої літератури та джерел, яких немає серед рекомендованих. **Політика виставлення балів.** Враховуються бали набрані при поточному тестуванні, самостійній роботі та бали підсумкового тестування. При цьому обов'язково враховуються присутність на заняттях та активність студента під час практичного заняття; недопустимість пропусків та запізнень на заняття; користування мобільним телефоном, планшетом чи іншими мобільними пристроями під час заняття в цілях не пов'язаних з навчанням; списування та плагіат; несвоєчасне виконання поставленого завдання і т. ін. Жодні форми порушення академічної доброчесності не толеруються.
Питання до заліку	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? 24. Forensics - explain and name the most popular tools.

Опитування	Анкету-оцінку з метою оцінювання якості курсу буде надано по завершенню курсу.

Схема курсу

Семестр 1

Тиж.	Тема, план, короткі тези	Форма діяльності/ заняття	Література. Інтернет-ресурси	Термін виконання
1	**Introduction to the course**	лекція – 2 год лабораторна – 2 год самостійна робота – 4год	[1-5]	тиждень
2	**CybeeSecurity roles and concepts**	лекція – 2 год лабораторна – 2 год самостійна робота – 6 год		тиждень
3	**Network basis with cybersecurity accents**	лекція – 2 год лабораторна – 2 год самостійна робота – 6 год		тиждень
4	**Operation system basis** with **cybersecurity accents**	лекція – 2 год лабораторна – 2 год самостійна робота – 6 год		тиждень
5	**Cybersecurity threats and solutions.**	лекція – 2 год лабораторна – 2 год самостійна робота – 6 год		тиждень
6	**Popular cyber frameworks: NIST, OWASP**	лекція – 2 год лабораторна – 2 год		тиждень

		самостійна робота – 6 год		
7	**Popular cyber frameworks: MITRE**	лекція – 2 год лабораторна – 2 год самостійна робота – 6 год		тиждень
8	**Cybersecurity threats and solutions.**	лекція – 2 год лабораторна – 2 год самостійна робота – 6 год		тиждень
9	**Cybersecurity threats and solutions.**	лекція – 2 год лабораторна – 2 год самостійна робота – 6 год		тиждень
10	**Cybersecurity Tools: firewalls**	лекція – 2 год лабораторна – 2 год самостійна робота – 6 год		тиждень
11	**Cybersecurity Tools: IDS\IPS**	лекція – 2 год лабораторна – 2 год самостійна робота – 7 год		тиждень
12	**Cybersecurity Tools: EDR**	лекція – 2 год лабораторна – 2 год самостійна робота – 6 год		тиждень
13	**Cybersecurity Tools: DLP, CASB**	лекція – 2 год лабораторна – 2 год самостійна робота – 6 год		тиждень
14	**Cybersecurity Tools: SIEM, SOAR**	лекція – 2 год лабораторна – 4 год		тиждень

		самостійна робота – 10 год		
15,16	**Cybersecurity Tools: attackers toolset**	лекція – 4 год лабораторна – 2 год самостійна робота – 8 год		тиждень