

**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 ОПІ Інформатика другого**  
**(магістерського) рівня вищої освіти для здобувачів зі спеціальності**  
**122 Комп'ютерні науки**

Львів 2023 р.

<b>Назва дисципліни</b>	Інструменти кібербезпеки
<b>Адреса викладання дисципліни</b>	Головний корпус ЛНУ ім. І. Франка м. Львів, вул. Університетська 1
<b>Факультет та кафедра, за якою закріплена дисципліна</b>	Факультет прикладної математики та інформатики Кафедра кібербезпеки
<b>Галузь знань, шифр та назва спеціальності</b>	12 – інформаційні технології 122 – комп'ютерні науки
<b>Викладачі дисципліни</b>	Трушевський Валерій Миолайович, кандидат фізико-математичних наук, доцент кафедри кібербезпеки; Карпюк Роман Валентинович, асистент\аспірант кафедри кібербезпеки
<b>Контактна інформація викладачів</b>	<a href="mailto:valeriy.trushevsky@lnu.edu.ua">valeriy.trushevsky@lnu.edu.ua</a> <a href="mailto:roman.karpiuk@lnu.edu.ua">roman.karpiuk@lnu.edu.ua</a>
<b>Консультації з питань навчання по дисципліні відбуваються</b>	Консультації в день проведення лекцій/практичних занять (за попередньою домовленістю).
<b>Сторінка курсу</b>	<a href="https://ami.lnu.edu.ua/admission/specializations">https://ami.lnu.edu.ua/admission/specializations</a>
<b>Інформація про дисципліну</b>	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).
<b>Коротка анотація дисципліни</b>	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.
<b>Мета та цілі дисципліни</b>	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.
<b>Література для вивчення дисципліни</b>	<p><b>Основна</b></p> <ol style="list-style-type: none"> <li>1. ISACA, Cybersecurity Fundamentals Study Guide 3<sup>rd</sup> Edition, 2021</li> <li>2. Документація SIEM “Splunk” - <a href="https://docs.splunk.com/Documentation">https://docs.splunk.com/Documentation</a>. Latest release notes – 2023.</li> <li>3. Документація сканера вразливостей Tenable – <a href="https://docs.tenable.com/">https://docs.tenable.com/</a>. Latest release notes – 2023.</li> <li>4. Документація IDS “Suricata” – <a href="https://suricata.readthedocs.io/en/suricata-6.0.5/">https://suricata.readthedocs.io/en/suricata-6.0.5/</a>. Latest release notes – 2023.</li> <li>5. MITRE - <a href="https://attack.mitre.org/">https://attack.mitre.org/</a>. Latest release notes – 2023.</li> </ol> <p>Додаткова література:</p> <ol style="list-style-type: none"> <li>1. P.W. Singer, Allan Friedman – “Cybersecurity and Cyberwar: What Everyone Needs to Know”.</li> <li>2. Richard A. Clarke, Robert K. Knake - "The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber</li> </ol>

	<p>Threats".</p> <ol style="list-style-type: none"> <li>3. Evan Gilman, Doug Barth - "Zero Trust Networks: Building Secure Systems in Untrusted Networks".</li> <li>4. Stuart McClure, Joel Scambray, George Kurtz - "Hacking Exposed: Network Security Secrets and Solutions".</li> <li>5. David G. Ries, Daniel J. Solove - "Cybersecurity: A Practical Guide to the Law of Cyber Risk.</li> </ol>
<b>Обсяг курсу</b>	Загальний обсяг: 165 годин. Аудиторних занять: 64 год., з них 32 год. лекцій та 32 год. лабораторних робіт. Самостійна робота: 101 год.
<b>Очікувані результати навчання</b>	<p>У результаті вивчення навчальної дисципліни студент має набути таких компетентностей:</p> <p><b>знати:</b></p> <ul style="list-style-type: none"> <li>- функціонування мережі</li> <li>- функціонування операційних систем</li> <li>- «периметр» безпеки</li> <li>- ланцюг побудови атаки</li> <li>- базові системи виявлення індикаторів атак</li> </ul> <p><b>вміти:</b></p> <ul style="list-style-type: none"> <li>- працювати з наступними інструментами: <ul style="list-style-type: none"> <li>• SIEM “Splunk”</li> <li>• IDS “Suricata”</li> <li>• Vulnerability Scanner “Tenable”</li> <li>• NMAP</li> </ul> </li> </ul> <p>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.</p>
<b>Ключові слова</b>	Кібербезпека, кібератака, загроза, вразливість, конфіденційність, цілісність, безпека даних, IDS, IPS, SIEM, Scanner, Vulnerability.
<b>Формат курсу</b>	Очний. Проведення лекцій, лабораторних робіт і консультацій.
<b>Теми</b>	Теми подані у Схемі курсу нижче.
<b>Підсумковий контроль, форма</b>	Залік у кінці 1 семестру.
<b>Навчальні методи та техніки, які будуть використовуватися під час викладання курсу</b>	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.
<b>Необхідне обладнання</b>	Комп'ютери, комп'ютерні системи та мережі. Віртуальні машини. Інтернет ресурси. Додаткове програмне забезпечення у вигляді trial-версій для типових інструментів з кібербезпеки.
<b>Критерії оцінювання (окремо для кожного виду навчальної діяльності)</b>	<p>Оцінювання проводиться за 100-бальною шкалою. Бали нараховуються за наступним співвідношенням:</p> <ul style="list-style-type: none"> <li>• модульний контроль, тестування, усне опитування: 50% семестрової оцінки; максимальна кількість балів 50</li> <li>• залік: 50% семестрової оцінки; максимальна кількість балів 50</li> </ul> <p>Підсумкова максимальна кількість балів 100.</p>

	<p><b>Академічна доброчесність:</b> 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 незарахування викладачем, незалежно від масштабів плагіату чи обману.</p> <p><b>Відвідання занять</b> є важливою складовою навчання. Очікується, що всі студенти відвідають усі лекції та практичні заняття 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.</p> <p><b>Література.</b> 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.</p> <p><b>Політика виставлення балів.</b> 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 запізнь 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.</p>
Питання до заліку	<ol style="list-style-type: none"> <li>1. Difference between cybersecurity and information security?</li> <li>2. What does cybersecurity provide?</li> <li>3. Why is DMZ necessary?</li> <li>4. Design a typical network architecture in a standard organization.</li> <li>5. How to implement centralized authentication for thousands of users?</li> <li>6. TCP-handshake.</li> <li>7. MITM (Man-in-the-Middle) attacks.</li> <li>8. Build and justify the concept of a "secure perimeter."</li> <li>9. What is needed for monitoring the security state in an organization?</li> <li>10. How to establish a relatively secure working environment without a million-dollar budget?</li> <li>11. With a million-dollar budget, where to begin?</li> <li>12. MITRE ATT&amp;CK framework.</li> <li>13. What is EDR (Endpoint Detection and Response)? What is its role?</li> <li>14. What is IDS (Intrusion Detection System)? What is its role?</li> <li>15. What is SIEM (Security Information and Event Management)? What is its role?</li> <li>16. What is DLP (Data Loss Prevention)? What is its role?</li> <li>17. What is Vulnerability Management? What is the role of this process?</li> <li>18. What is SSDLC (Secure Software Development Life Cycle)? What is the role of this process?</li> <li>19. What is the difference between Vulnerability Management and Vulnerability Scanning?</li> <li>20. Penetration Testing - why is it needed?</li> <li>21. How to use nmap?</li> <li>22. Mimikatz - what is it about?</li> <li>23. ATP (Advanced Threat Protection) - what is it, and what does it address?</li> <li>24. Forensics - explain and name the most popular tools.</li> </ol>

<b>Опитування</b>	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	<b>Introduction to the course</b>	лекція – 2 год лабораторна – 2 год самостійна робота – 4 год	[1-5]	тиждень
2	<b>CyberSecurity roles and concepts</b>	лекція – 2 год лабораторна – 2 год самостійна робота – 6 год		тиждень
3	<b>Network basis with cybersecurity accents</b>	лекція – 2 год лабораторна – 2 год самостійна робота – 6 год		тиждень
4	<b>Operation system basis with cybersecurity accents</b>	лекція – 2 год лабораторна – 2 год самостійна робота – 6 год		тиждень
5	<b>Cybersecurity threats and solutions.</b>	лекція – 2 год лабораторна – 2 год самостійна робота – 6 год		тиждень
6	<b>Popular cyber frameworks: NIST, OWASP</b>	лекція – 2 год лабораторна – 2 год		тиждень

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

		самостійна робота – 10 год		
15,16	<b>Cybersecurity Tools: attackers toolset</b>	лекція – 4 год лабораторна – 2 год самостійна робота – 8 год		тиждень