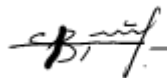


**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**  
**Львівський національний університет імені Івана Франка**  
**Факультет прикладної математики та інформатики**  
**Кафедра кібербезпеки**

**Затверджено**

На засіданні кафедри інформаційних систем  
факультету прикладної математики та інформатики  
Львівського національного університету імені Івана Франка  
(протокол № 3/22 від 3 жовтня 2022 р.)

Завідувач кафедри .



Венгерський П.С.

**Силабус з навчальної дисципліни**  
**“Інструменти SecOps”,**  
**що викладається в межах ОПП Кібербезпека**  
**першого (бакалаврського) рівня вищої освіти для здобувачів з**  
**спеціальності 125 – кібербезпека**

Львів 2022 р.

<b>Назва дисципліни</b>	Інструменти SecOps
<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 125 – кібербезпека
<b>Викладачі дисципліни</b>	Карпюк Роман Валентинович, асистент\аспірант кафедри інформаційних систем
<b>Контактна інформація викладачів</b>	<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 SecOps” є нормативною дисципліною з спеціальності 125 – кібербезпека для освітньої програми Кібербезпека, яка викладається в 6-му та 7-му семестрах в обсязі 6.5-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 практичні інструменти в сфері кібербезпеки, а саме інструменти «захисту» та «нападу». Також розуміння основних принципів побудови та функціонування центрів з протидії кіберзагрозам (CSOC)
<b>Мета та цілі дисципліни</b>	Метою курсу є формування у студентів практичних навиків використання популярних інструментів в сфері кібербезпеки (SIEM, vulnerability scanners, IDS\IPS, Nmap, Metasploit, etc.), розуміння «глибина захисту» та циклу атаки на інфраструктуру організації.
<b>Література для вивчення дисципліни</b>	<ol style="list-style-type: none"> <li>1. Cybersecurity Fundamentals/ ISACA/ <a href="http://www.isaca.org/cyber?Cybersecurity%20Fundamentals%20Study%20Guide">www.isaca.org/cyber?Cybersecurity Funamentals Study Guide/</a> 2003.- 156 p.</li> <li>2. Документація SIEM “Splunk” - <a href="https://docs.splunk.com/Documentation">https://docs.splunk.com/Documentation</a></li> <li>3. Документація сканера вразливостей Tenable – <a href="https://docs.tenable.com/">https://docs.tenable.com/</a></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></li> <li>5. MITRE - <a href="https://attack.mitre.org/">https://attack.mitre.org/</a></li> <li>6. MITRE Defend - <a href="https://d3fend.mitre.org/">https://d3fend.mitre.org/</a></li> <li>7. Загальний огляд ланцюга атаки - <a href="https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/searisk-cyber-101-july2017.pdf">https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/searisk-cyber-101-july2017.pdf</a></li> </ol>
<b>Обсяг курсу</b>	Загальний обсяг: 195 годин. Аудиторних занять: 128 год., з них 64 год. лекцій та 64 год. лабораторних робіт. Самостійної роботи: 67 год.

<p><b>Очікувані результати навчання</b></p>	<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>- читати журнали подій (логи) із різних систем</li> <li>- розуміти MITRE ATT&amp;CK</li> <li>- працювати з наступними інструментами: <ul style="list-style-type: none"> <li>• SIEM “Splunk”</li> <li>• IDS “Suricata”</li> <li>• EDR “CrowdStrike”</li> <li>• Vulnerability Scanner “Tenable”</li> <li>• Metasploit</li> <li>• NMAP</li> </ul> </li> </ul> <p>Курс забезпечує набуття таких компетентностей: КЗ 1, КЗ 2, КЗ 5, КФ 2, КФ 3, КФ 5, КФ 8, КФ 9, КФ 11, КФ 12 ; та програмних результатів навчання: ПРН 1, ПРН 3, ПРН 4, ПРН 5, ПРН 6, ПРН 9, ПРН 10, ПРН 11, ПРН 12, ПРН 14, ПРН 15, ПРН 18, ПРН 19, ПРН 20, ПРН 23, ПРН 27, ПРН 31, ПРН 34, ПРН 42, ПРН 46, ПРН 48, ПРН 52.</p>
<p><b>Ключові слова</b></p>	<p>Кібербезпека, кібератака, загроза, вразливість, конфіденційність, цілісність, безпека даних, IDS, IPS, NGFW, EDR\XDR, SIEM, Scanner, Vulnerability,</p>
<p><b>Формат курсу</b></p>	<p>Очний. Проведення лекцій, лабораторних робіт і консультацій.</p>
<p><b>Теми</b></p>	<ul style="list-style-type: none"> <li>- Актуалізація знання щодо роботи базових сервісів мережі та операційних систем (DNS\DHCP, стек TCP\IP, NAT\PAT, DMZ, TCP\UDP, TCP-handshake, TLS, AD, DC, etc.)</li> <li>- Blue Team VS Red Team</li> <li>- Cyber Security Operation Center</li> <li>- Концепція «глибини» та «периметру» безпеки</li> <li>- MITRE ATT&amp;CK</li> <li>- Ланцюг (kill-chain) атаки</li> <li>- Інструменти: <ul style="list-style-type: none"> <li>• Журнали подій (logs)</li> <li>• Мережеві екрани (firewalls, WAF, NGFW)</li> <li>• Системи виявлення(протидії) мережевих загроз (IDS\IPS)</li> <li>• Сканери вразливостей</li> <li>• Системи управління подіями з інформаційної безпеки (SIEM)</li> <li>• Фреймворки атакуючої сторони</li> </ul> </li> <li>- Криптографія та криптоаналіз в «прикладному» світі</li> </ul>
<p><b>Підсумковий контроль, форма</b></p>	<p>Екзамен у кінці 6 семестру</p>

<p><b>Навчальні методи та техніки, які будуть використовуватися під час викладання курсу</b></p>	<p>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</p>
<p><b>Необхідне обладнання</b></p>	<p>Комп'ютери, комп'ютерні системи та мережі. Віртуальні машини. Інтернет ресурси. Додаткове програмне забезпечення у вигляді trial-версій для типових інструментів з кібербезпеки.</p>
<p><b>Критерії оцінювання (окремо для кожного виду навчальної діяльності)</b></p>	<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>• екзамен: 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>
<p>Питання до екзамену.</p>	<ol style="list-style-type: none"> <li>1. Різниця між кібербезпекою і інформаційною безпекою?</li> <li>2. Що забезпечує кібербезпека?</li> <li>3. Для чого потрібна DMZ?</li> <li>4. Збудувати типову архітектуру мережі в типовій організації</li> <li>5. Як або чим здійснити централізовану автентифікацію тисячів користувачів?</li> <li>6. TCP-handshake</li> <li>7. Атаки типу MITM</li> <li>8. Збудувати і обґрунтувати концепцію «безпечного периметру»</li> <li>9. Що потрібно для моніторингу стану безпеки в організації?</li> <li>10. Як, не маючи мільйонного бюджету, збудувати відносно безпечне робоче середовище?</li> </ol>

	<ul style="list-style-type: none"> <li>11. Маючи мільйонний бюджет – з чого почати?</li> <li>12. MITRE ATT&amp;CK</li> <li>13. Що таке EDR? Яка роль данного інструменту?</li> <li>14. Що таке IDS? Яка роль данного інструменту?</li> <li>15. Що таке SIEM? Яка роль данного інструменту?</li> <li>16. Що таке DLP? Яка роль данного інструменту?</li> <li>17. Що таке Vulnerability Management? Яка роль данного процесу?</li> <li>18. Що таке SSDLC? Яка роль данного процесу?</li> <li>19. В чому полягає різниця між Vuln. Mgmt та Vuln.Scanning ?</li> <li>20. Penetration Testing - навіщо потрібен?</li> <li>21. Як використати nmap?</li> <li>22. Mimikatz - це про що?</li> <li>23. АТР – що це і про що говорить?</li> <li>24. Forensic – розказати і назвати найбільш популярний інструментарій.</li> </ul>
<b>Опитування</b>	Анкету-оцінку з метою оцінювання якості курсу буде надано по завершенню курсу.