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 № 15/23 від 29 серпня 2023 р.)

Завідувач кафедри П.С.Венгерський

Силабус з навчальної дисципліни

“Інструменти SecOps 2”,

що викладається в межах ОПП Кібербезпека першого (бакалаврського) рівня вищої освіти для здобувачів з спеціальності 125 – кібербезпека та захист інформації

Львів 2023 р.

Назва дисципліни	Інструменти SecOps 2
Адреса викладання дисципліни	Львівський національний університет імені Івана Франка, вул. Університетська 1, м. Львів, Україна, 79000
Факультет та кафедра, за якою закріплена дисципліна	Факультет прикладної математики та інформатики Кафедра кібербезпеки
Галузь знань, шифр та назва спеціальності	12 – інформаційні технології 125 – кібербезпека та захист інформації
Викладачі дисципліни	Костяк Марина Юріївна, к.т.н., доцент кафедри кібербезпеки Карпюк Роман Валентинович, асистент\аспірант кафедри кібербезпеки
Контактна інформація викладачів	Maryna.Kostiak@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 SecOps 2" є нормативною дисципліною з спеціальності 125 – кібербезпека та захист інформації для освітньої програми Кібербезпека, яка викладається в 7-му семестрах в обсязі 4 кредитів (за Європейською Кредитно-Трансферною Системою ECTS).
Коротка анотація дисципліни	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)
Мета та цілі дисципліни	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.
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. Додатково: 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: 120. Аудиторних занять: 64 год., з них 32 год. лекцій та 32 год. лабораторних робіт. Самостійної роботи: 56 год.
Очікувані результати навчання	У результаті вивчення навчальної дисципліни студент має набути таких компетентностей: **знати:** - CVE CVSS score - MITRE ATT&CK - найкращі практики для SecOps активності - базові розуміння клаудів - працювати з наступними інструментами: • SIEM “Splunk” • IDS “Suricata” • EDR “CrowdStrike” • Vulnerability Scanner “Tenable” • Metasploit • NMAP • AngryIPScanner • Metasploit • NVD CVE - опрацювати incident response plan (IRP) на всіх його етепах - формувати чіткий, лаконічний, доказовий звіт щодо реагування на кіберінциденти Курс забезпечує набуття таких компетентностей: ІК, 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 2, ПРН 3, ПРН 4, ПРН 5, ПРН 6, ПРН 9, ПРН 10, ПРН 11, ПРН 12, ПРН 13, ПРН 14, ПРН 15, ПРН 16, ПРН 17, ПРН 18, ПРН 19, ПРН 20, ПРН 22, ПРН 27, ПРН 28, ПРН 29, ПРН 30, ПРН 31, ПРН 33, ПРН 34, ПРН 39, ПРН 41-43
Ключові слова	Кібербезпека, кібератака, загроза, вразливість, конфіденційність, цілісність, безпека даних, IDS, IPS, NGFW, EDR\XDR, SIEM, Scanner, Vulnerability,
Формат курсу	Очний. Проведення лекцій, лабораторних робіт і консультацій.
Теми	Теми подані у Схемі курсу нижче
Пререквізити	Для вивчення курсу студенти потребують базові знання з таких дисциплін: 1. Основи кібербезпеки 2. Операційні системи та комп’ютерні мережі 3. Основи криптографії 4. Організація ІТ на підприємстві 5. Події, опрацювання та аналіз логів

	6. Застосування систем штучного інтелекту в кібербезпеці 7. Інструменти SecOps 1 8. Менеджмент інформаційної безпеки
Підсумковий контроль, форма	Екзамен у кінці 7 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, RangeForce платформа.
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 • екзамен: 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. П**олітика 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 екзамену.	1. Різниця між кібербезпекою і інформаційною безпекою? 2. Що забезпечує кібербезпека? 3. Для чого потрібна DMZ? 4. Збудувати типову архітектуру мережі в типовій організації 5. Як або чим здійснити централізовану автентифікацію тисячів

	користувачів? 6. TCP-handshake 7. Атаки типу MITM 8. Збудувати і обґрунтувати концепцію «безпечного периметру» 9. Що потрібно для моніторингу стану безпеки в організації? 10. Як, не маючи мільонного бюджету, збудувати відносно безпечне робоче середовище? 11. Маючи мільонний бюджет – з чого почати? 12. MITRE ATT&CK 13. Що таке EDR? Яка роль данного інструменту? 14. Що таке IDS? Яка роль данного інструменту? 15. Що таке SIEM? Яка роль данного інструменту? 16. Що таке DLP? Яка роль данного інструменту? 17. Що таке Vulnerability Managment? Яка роль данного процесу? 18. Що таке SSDLC? Яка роль данного процесу? 19. В чому полягає різниця між Vuln. Mgmnt та Vuln.Scanning ? 20. Penetration Testing - навіщо потрібен? 21. Як використати nmap? 22. Mimikatz - це про що? 23. ATP – що це і про що говорить? 24. Forensic – розказати і назвати найбільш популярний інструментарій.
Опитування	Анкету-оцінку з метою оцінювання якості курсу буде надано по завершенню курсу.

Схема курсу

Теми	**Тема, план, короткі тези**	**Форма діяльності/ заняття**	**Література. Інтернет-ресурси**	**Термін виконання**
1	**Introduction to the course**	лекція – 2 год самостійна робота – 4год	[1-5] **Література. Інтернет-ресурси** [1-5]	тиждень
2	**Microsoft security ecosystem**	лекція – 2 год лабораторна – 2 год самостійна робота – 4 год		тиждень
3	EDR	лекція – 4 год лабораторна – 4 год самостійна робота – 8 год		2 тижні
4	**SIEM & SOAR**	лекція – 4 год лабораторна – 4 год самостійна робота – 4 год		2 тижні

5	**Atackers TTPs**	лекція – 2 год лабораторна – 2 год самостійна робота – 4 год		тиждень
6	**Digital Forensic**	лекція – 4 год лабораторна – 4 год самостійна робота – 4 год		2 тижні
7	**Social Engineering**	лекція – 2 год лабораторна – 2 год самостійна робота – 6 год		тиждень
8	**Cloud Security**	лекція – 2 год лабораторна – 2 год самостійна робота – 6 год		тиждень
9	**Email Security**	лекція – 2 год лабораторна – 2 год самостійна робота – 4год		тиждень
10	**Detection of attack patterns (path traversal, scanning, enumeration, credential access, privilege escalation, port knocking, lateral movement, etc.)**	лекція – 6 год лабораторна – 8 год самостійна робота – 10 год		3 тижні
11	**Malware**	лекція – 2 год лабораторна – 2год самостійна робота –2 год		тиждень
	Всього	**120**		