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 № 3/22 від 3 жовтня 2022 р.)

Завідувач кафедри .

Венгерський П.С.

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

Львів 2022 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	Карпюк Роман Валентинович, асистент\аспірант кафедри кібербезпеки
Контактна інформація викладачів	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/course/instrumenty-kiberbezpeky
Інформація про дисципліну	Дисципліна "Інструменти кібербезпеки" є дисципліною за вибором з спеціальності 122 – комп'ютерні науки для освітньої програми Інформатика, яка викладається в 9-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	1. Cybersecurity Fundamentals/ ISACA/ www/isaca/org/cyber? Cybersecurity Funamentals Study Guide/ 2003.- 156 p. 2. Документація SIEM "Splunk" - https://docs.splunk.com/Documentation 3. Документація сканера вразливостей Tenable – https://docs.tenable.com/ 4. Документація IDS "Suricata" – https://suricata.readthedocs.io/en/suricata-6.0.5/ 5. MITRE - https://attack.mitre.org/ 6. MITRE Defend - https://d3fend.mitre.org/ 7. Загальний огляд ланцюга атаки - https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cyber-101-july2017.pdf
Обсяг курсу	Загальний обсяг: 128 годин. Аудиторних занять: 64 год., з них 32 год. лекцій та 32 год. лабораторних робіт. Самостійної роботи: 64 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: 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.
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	- 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.) - Blue Team VS Red Team - Концепція «глибини» та «периметру» безпеки - Ланцюг (kill-chain) атаки - Інструменти: • Мережеві екрани (firewalls, WAF, NGFW) • Системи виявлення(протидії) мережевих загроз (IDS\IPS) • Сканери вразливостей • Системи управління подіями з інформаційної безпеки (SIEM) • Фреймворки атакуючої сторони - Криптографія та криптоаналіз в «прикладному» світі
Підсумковий контроль, форма	Залік у кінці 1 семестру 1-го року навчання у магістратурі
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 • 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. **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 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 міліонного бюджету, збудувати відносно безпечне робоче середовище? 11. Маючи міліонний бюджет – з чого почати? 12. MITRE ATT&CK 13. Що таке EDR? Яка роль даного інструменту? 14. Що таке IDS? Яка роль даного інструменту? 15. Що таке SIEM? Яка роль даного інструменту? 16. Що таке DLP? Яка роль даного інструменту? 17. Що таке Vulnerability Managment? Яка роль даного процесу?

	18. Що таке SSDLC? Яка роль даного 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.