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 № _ від _)

Завідувач кафедри .

Венгерський П.С.

Силабус з навчальної дисципліни
“Полювання на кіберзагрози”,
що викладається в межах ОПП Кібербезпека
першого (бакалаврського) рівня вищої освіти для здобувачів з спеціальності 125 – Кібербезпека

Львів - 2023

Назва дисципліни	Полювання на кіберзагрози
Адреса викладання дисципліни	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 125 – кібербезпека
Викладачі дисципліни	Щербина Микола Юрійович Асистент кафедри кібербезпеки
Контактна інформація викладачів	mykola.shcherbyna@lnu.edu.ua; Головний корпус ЛНУ ім. І. Франка, каб.260. м. Львів, вул. Університетська, 1
Консультації з питань навчання по дисципліні відбуваються	Консультації в день проведення практичних занять (а також за розкладом консультацій кафедри).
Сторінка курсу	https://ami.lnu.edu.ua/admission/specializations
Інформація про дисципліну	Дисципліна “Полювання на кіберзагрози” є вибірковою дисципліною з спеціальності 125 – кібербезпека для освітньої програми “Кібербезпека та захист інформації”, яка проводиться в 7-му семестрі в обсязі 4 кредитів (за Європейською Кредитно-Трансферною Системою ECTS).
Коротка анотація дисципліни	“Полювання на кіберзагрози” є важливим курсом у підготовці спеціаліста з кібербезпеки, оскільки студенти дізнаються про методи пошуку слідів діяльності шкідливого ПЗ в ОС Windows та Linux, його наявності у виконавчих файлах; найпоширеніші експлойти; аналіз такого ПЗ шляхом реверс-інжинірингу.
Мета та цілі дисципліни	Мета і цілі вивчення нормативної дисципліни “Полювання на кіберзагрози” – інструментами моніторингу діяльності ОС Windows та Linux, форматами виконавчих файлів ELF та COFF, архітектурою 32- та 64-розрядних процесорів x86 та ARM, дизасемблерами/декомпіляторами (IDA, Ghidra тощо), способами проникнення шкідливого ПЗ у систему та методами протидії цьому.
Література для вивчення дисципліни	1. Andriesse D. Practical Binary Analysis: Build Your Own Linux Tools for Binary Instrumentation, Analysis, and Disassembly. San Francisco: No Starch Press, 2018. 456 p. 2. Anley C., Heasman J., Lindner F., Richarte G. The Shellcoder's Handbook: Discovering and Exploiting Security Holes, 2nd Edition. Indianapolis: Wiley Publishing, Inc., 2007. 744 p. 3. Russinovich M. E., Margosis A. Troubleshooting with the Windows Sysinternals Tools, 2nd Edition. Redmond: Microsoft Press, 2016. 688 p. 4. IDA Help: The Interactive Disassembler Help Index. Hex

	Rays – State-of-the-art binary code analysis solutions. URL: https://hex-rays.com/products/ida/support/idadoc/index.shtml 5. GitHub - NationalSecurityAgency/ghidra: Ghidra is a software reverse engineering (SRE) framework. GitHub. URL: https://github.com/NationalSecurityAgency/ghidra 6. Intel® 64 and IA-32 Architectures Software Developer's Manual. Combined Volumes: 1, 2A, 2B, 2C, 2D, 3A, 3B, 3C, 3D, and 4. Intel Corporation, 2023. 5066 p. URL: https://software.intel.com/en-us/download/intel-64-and-ia-32-architectures-sdm-combined-volumes-1-2a-2b-2c-2d-3a-3b-3c-3d-and-4 7. Instruction Set Assembly Guide for Armv7 and earlier Arm® architectures. Version 2.0. Reference Guide. Arm Limited, 2019. 590 p. URL: https://documentation-service.arm.com/static/5e7b6a6216d2907d594035c4?token= 8. Arm® A64 Instruction Set Architecture Armv8, for Armv8-A architecture profile. Arm Limited, 2021. 3289 p. URL: https://documentation-service.arm.com/static/61c04c7a2183326f21771ec6?token=
Обсяг курсу	Загальний обсяг: 96 годин. З них 32 год. лекцій і 64 год. лабораторних занять.
Очікувані результати навчання	Після завершення цього курсу студент буде знати: • інструменти пошуку кіберзагроз в ОС Windows та Linux; • способи проникнення шкідливого ПЗ у систему; • основи архітектури і набору команд x86 та x86-64; • основи архітектури і набору команд A32/T32 та A64; • структуру виконавчих файлів COFF та ELF; • основи реверс-інжинірингу за допомогою IDA та Ghidra. Вміти: • знаходити сліди діяльності шкідливого ПЗ у системі; • знаходити та досліджувати кіберзагрози у виконавчих файлах. Курс забезпечує набуття таких компетентностей: КЗ 1, КЗ 2, КЗ 4, КЗ 5, КФ 2, КФ 6, КФ 8, КФ 9, КФ 11, КФ 12, КФ 14 та програмних результатів навчання: ПРН 2, ПРН 3, ПРН 4, ПРН 10, ПРН 15, ПРН 23, ПРН 35, ПРН 42, ПРН 48, ПРН 50, ПРН 52, ПРН 53
Ключові слова	threat hunting, reverse engineering, x86, ARM, Windows, Linux.
Формат курсу	Очний, дистанційний. Проведення лекцій, лабораторних робіт і консультацій.

Теми	Тема 1. Аналіз підозрілої активності. Тема 2. Об'єктні модулі, виконувані файли та спільні бібліотеки. Тема 3. Попередній аналіз підозрілих файлів. Тема 4. Введення у 32-розрядну архітектуру x86. Тема 5. Експлойти та протидія. Тема 6. Введення у 64-розрядну архітектуру x86-64. Тема 7. Дослідження виконавчих файлів Linux (ELF). Тема 8. Дослідження виконавчих файлів Windows (COFF). Тема 9. Використання дизасемблера/декомпілятора IDA. Тема 10. Введення у 32-розрядну архітектуру AArch32. Тема 11. Використання дизасемблера/декомпілятора Ghidra. Тема 12. Введення у 64-розрядну архітектуру AArch64. Тема 13. Декомпіляція програмного забезпечення на Java.
Підсумковий контроль, форма	Залік у кінці 7 семестру
Навчальні методи та техніки, які будуть використовуватися під час викладання курсу	Індивідуальні завдання
Необхідне обладнання	Комп’ютери, комп’ютерні системи та мережі. Інтернет ресурси..
Критерії оцінювання (окремо для кожного виду навчальної діяльності)	Оцінювання проводиться за 100-бальною шкалою. Бали нараховуються за наступним чином: • Індивідуальні завдання: максимальна кількість балів 50 • Захист власних проектів: 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 незарахування 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	Для одержання заліку студент повинен оформити звіт практики, який повинен містити: титульну сторінку; індивідуальні завдання. Для кожного завдання має бути вказано: номер варіанту, формулювання умови, результати роботи програми у вигляді скріншотів, текст коду програмної реалізації.
Опитування	Анкету-оцінку з метою оцінювання якості курсу буде надано по завершенню курсу.