ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет математики та інформатики

Кафедра комп’ютерних наук

СИЛАБУС

навчальної дисципліни

ЗВОРОТНА РОЗРОБКА (REVERSE ENGINEERING)

Викладач: асистент Пастушков Олександр Романович

Кафедра: комп’ютерних наук

E-mail: oleks.pastushkov@gmail.com

Консультації: дистанційні – Moodle

Посилання на курс у Moodle:

https://moodle.znu.edu.ua/course/view.php?id=17925

ПАСПОРТ ДИСЦИПЛІНИ

Рівень освіти	Бакалавр
Форма навчання	Денна
Статус дисципліни	Вибіркова
Кредити ECTS	4
Семестр	7
Вид контролю	Залік / практична робота

МЕТА ДИСЦИПЛІНИ

Надати студентам фундаментальні знання та практичні навички з аналізу виконуваних програм без доступу до вихідного коду: дизасемблювання, декомпіляція, динамічний аналіз, техніки обходу захисту та методи аналізу шкідливого ПЗ.

ЗАВДАННЯ ДИСЦИПЛІНИ

- Розкрити основи архітектури процесорів та форматів виконуваних файлів (PE/ELF/Mach-O).
- Навчити використовувати інструменти: Ghidra, IDA Pro, Radare2, x64dbg, OllyDbg.
- Розвинути вміння виконувати статичний і динамічний аналіз програм.
- Ознайомити з техніками обфускації, пакування та антидебаг-захисту.
- Надати навички з безпечної та етичної практики реверсу (правові/етичні аспекти).

КОМПЕТЕНТНОСТІ

Загальні компетентності (ЗК):

- ЗК1 — аналітичне мислення та системний підхід.
- ЗК2 — відповідальність за етичне використання знань.
- ЗК3 — здатність до самостійного опанування професійної літератури.

Фахові компетентності (ФК):

- ФК1 — володіння інструментами статичного/динамічного аналізу.
- ФК2 — здатність виявляти та аналізувати вразливості у виконуваних програмах.
- ФК3 — застосування реверс-технік у задачах кібербезпеки та цифрової криміналістики.

ПРОГРАМНІ РЕЗУЛЬТАТИ НАВЧАННЯ (ПРН)

- ПРН1 — пояснює архітектуру x86/x64 та основи ARM, розуміє регістри, стек, пам’ять.
- ПРН2 — аналізує структуру PE/ELF/Mach-O файлів і розпізнає секції та імпорти.
- ПРН3 — виконує дизасемблювання та декомпіляцію, інтерпретує машинний код.

- ПРН4 — застосовує динамічний аналіз: відлагоджування, трасування, моніторинг.
- ПРН5 — ідентифікує обфускацію, пакери та застосовує методи їх обходу.
- ПРН6 — проводить базовий аналіз шкідливого ПЗ та готує технічний звіт.

ЗМІСТОВІ МОДУЛІ ТА ТЕМИ

1. Модуль 1. Вступ та підготовка середовища: етика, інструменти (Ghidra, IDA, Radare2, x64dbg), створення ізольованого середовища.
2. Модуль 2. Архітектура та формати файлів: інструкції, регістри, стек, формати PE/ELF/Mach-O.
3. Модуль 3. Статичний аналіз: дизасемблювання, декомпіляція, відновлення логіки функцій.
4. Модуль 4. Динамічний аналіз: breakpoints, трасування, дампи пам’яті, моніторинг поведінки.
5. Модуль 5. Обфускація, пакери, антидебаг-техніки та методи обходу.
6. Модуль 6. Аналіз шкідливого ПЗ: ransomware, droppers, indicators of compromise.
7. Модуль 7. Практичний проєкт: reverse crackme або аналіз виконуваного файлу.

СИСТЕМА ОЦІНЮВАННЯ

Лабораторні роботи	40
Контрольні завдання / тести	20
Активність і самостійна робота	10
Підсумковий проєкт / залік	30

ОСНОВНІ ТА ДОДАТКОВІ ДЖЕРЕЛА

- Practical Malware Analysis — Michael Sikorski & Andrew Honig.
- The IDA Pro Book — Chris Eagle.
- Ghidra User Documentation — https://ghidra-sre.org
- Radare2 Book / офіційна документація.

- x64dbg, OllyDbg, Procmon, Wireshark, Binary Ninja — інструментальні посібники.
- Malware Analysis Reports та open CTF writeups.

ЕТИКА ТА БЕЗПЕКА

Реверс здійснюється виключно в навчальних цілях у контрольованому середовищі. Забороняється аналіз комерційного чи захищеного ПЗ без згоди власника. Дотримання етичних і правових норм є обов’язковим.

ГРИФ ПОГОДЖЕННЯ

Обговорено та ухвалено на засіданні кафедри комп’ютерних наук
Протокол № __ від «___» _____ 2025 р.

Завідувач кафедри _____