Силабус курсу

АНАЛІЗ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Ступінь вищої освіти – магістр
Рік навчання: 1,
Семестр: 1
Кількість кредитів: 5**,**
Мова викладання: українська

Керівник курсу

ПІП	Степан Івасьєв
Контактна інформація	isv@wunu.edu.ua

Опис дисципліни

Мета вивчення дисципліни «Аналіз шкідливого програмного забезпечення» полягає у формуванні у майбутніх спеціалістів умінь та компетенцій для забезпечення ефективного машинного навчання, необхідних для подальшої роботи та навчити застосуванню методів та засобів аналізу шкідливого програмного забезпечення в умовах широкого використання сучасних інформаційних технологій. В результаті вивчення курсу «Аналіз шкідливого програмного забезпечення» студенти повинні: володіти методиками проведення зворотної розробки програмного забезпечення та апаратних пристроїв; засвоїти основні фундаментальні поняття і закони методів реверс інжинірингу для їх використання в сучасних умовах; знати принципи побудови сучасного програмного забезпечення; вміти використовувати основний математичний апарат та закони декомпіляції програмного забезпечення; вміти використовувати програмні засоби, які реалізують основні методи реверс інжинірингу. Завдання проведення лекцій полягає у розгляді найкращих практик динамічного та статичного аналізу шкідливого ПЗ, проведенні декомпіляції та дебагінгу коду. Завдання проведення практичних занять, як одна з основних форм навчального процесу, передбачає набуття практичних навиків з виявлення, ідентифікації, статичного та динаміного аналізу, декомпіляції та дебагінгу шкідливого програмного забезпечення.

Структура курсу

Години лек/пр	Тема	Результати навчання	Завдання
2/0	Основні статичні методики	Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.	Поточне опитування
2/0	Упаковане і обфуційоване шкідливе ПЗ	Розуміння методології проектування запакованого ПЗ. Пакувальники. Архіватори.	Поточне опитування
2/0	Аналіз шкідливих програм в віртуальних машинах	Вміння використовувати технології віртуалізації. Дослідження змін в	Поточне опитування

		реєстрі. Дослідження змін в файловій системі.	
2/0	Використання віртуальної машини для аналізу безпеки	Навики роботи зв сканерами вразливостей. Сервери DCOM. Аналіз відкритих портів та вразливостей ОС.	Поточне опитування
2/0	Основи динамічного аналізу	Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.	Поточне опитування
2/2	Прискорений курс по асемблеру для архітектури x86	Володіння поняттям асемблера. Архітектури операційної системи. Набори інструкцій. Шкідливі програми в середині спеціального ПЗ.	Поточне опитування
2/0	Розпізнавання конструкцій мови С в асемблері	Навики використання дизасемблювання. Аналіз двійкового коду. Розпізнавання конструкцій мови С в асемблері.	Поточне опитування
2/2	Аналіз шкідливих програм для Windows.	Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.	Поточне опитування
4/2	Порівняння налагодження на рівні вихідного і дизасемблювати коду. Аналізатор на рівні асемблера OllyDbg	Навики використання аналізатора на рівні асемблера OllyDbg. Вихідне налагодження. Низхідне налагодження. Дизасемблювання коду	Поточне опитування
2/2	Відлагодження ядра з допомогою WinDbg.	Вміння застосовувати драйвери і код ядра. Відлагоджувальні символи Microsoft. Особливості ядра Windows Vista,7,10. Робота з WinDbg.	Поточне опитування
2/2	Антидизассемблювання. Антивідладка	Знання асемблер для архітектури x86. Технологія IDA Pro. Розпізнавання конструкцій С та їх приховування в асемблері. Аналіз шкідливих програм для Windows. Навики відлагоджування. Технологія OllyDbg. Відлагодження ядра з допомогою WinDbg.	Поточне опитування
2/2	Методи протидії віртуальним машинам.	Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.	Поточне опитування
2/2	Пакувальники і розпакування	Застосовувати антидизасемблювання. Антивідладка. Пакувальники та де пакувальники.	Поточне опитування
4/2	Аналіз коду командної оболонки	Вміння аналізувати код командної стрічки. Аналіз коду С++. Шістдесятчотирьохбітні шкідливі програми.	Поточне опитування

Літературні джерела

1. Mishra A. Mobile App Reverse Engineering: Get started with discovering, analyzing,

and exploring the internals of Android and iOS apps. Birmingham: Packt Publishing, 2022. - 165 p.
2. Omar M. Defending Cyber Systems through Reverse Engineering of Criminal Malware. Springer, 2022. - 59 p.
3. Додонов А.Г. та ін. Комп'ютерна конкурентна розвідка. Додонов А.Г., Ланде Д.В., Прищепа В.В., Путятін В.Г. - Київ: ТОВ Інжиніринг, 2021. - 355 с.
4. Belous A., Saladukha V. Viruses, Hardware and Software Trojans: Attacks and Countermeasures. Springer, 2020. - 838 p.
5. Alrabaee S., Debbabi M., Shirani P., Wang L., Youssef A., Rahimian A., Nouh L., Mouheb D., Huang H., Hanna A. Binary Code Fingerprinting for Cybersecurity: Application to Malicious Code Fingerprinting. Springer, 2020. - 264 p.
6. Basant Vidya. Hacking Mastery With Kali Linux. Independently published, 2021. - 200 p.
7. Mohanta Abhijit, Saldanha Anoop. Malware Analysis and Detection Engineering: A Comprehensive Approach to Detect and Analyze Modern Malware. Apress Media LLC, 2020. — 948 p.
8. Budgen David. Software Design: Creating Solutions for Ill-Structured Problems. 3rd edition. — Routledge, 2021. — 365 p.
9. Martins Luiz Eduardo, Gorschek Tony. Requirements Engineering for Software and Systems. River Publishers, 2022. — 230 p.
10. Wardle Patrick. The Art of Mac Malware: The Guide to Analyzing Malicious Software. No Starch Press, 2022. — 320 p
11. Kohnfelder Loren. Designing Secure Software. No Starch Press, 2022. — 332 p.

Політика оцінювання

Політика щодо дедлайнів та перескладання: Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку (-20 балів). Перескладання модулів відбувається із дозволу деканату за наявності поважних причин (наприклад, лікарняний).

Політика щодо академічної доброчесності: Списування під час контрольних робіт та екзаменів заборонені (в т.ч. із використанням мобільних девайсів).

Політика щодо відвідування: Відвідування занять є обов'язковим компонентом оцінювання, за яке нараховуються бали. За об'єктивних причин (наприклад, хвороба, міжнародне стажування) навчання може відбуватись в он-лайн формі за погодженням із керівником курсу.

Оцінювання

Заліковий модуль 1	Заліковий модуль 2 (ректорська контрольна робота)	Заліковий модуль 3 (підсумкова оцінка за КПІЗ враховуючи поточне опитування)	Заліковий модуль 4 (письмовий екзамен)
20%	20%	20%	40%
1. Теоретичні питання – max 40 балів. 2. Практичне завдання: 2 практичні завдання по 30 балів – max 60 балів.	1. Теоретичні питання – max 40 балів. 2. Практичне завдання: 2 практичні завдання по 30 балів – max 60 балів.	1. Підготовка КПІЗ – max 40 балів. 2. Захист КПІЗ – max 40 балів. 3. Участь у тренінгах – max 20 балів	1. Теоретичні питання: 3 питання по 20 балів - max 60 балів. 2. Практичне завдання - max 40 балів

Шкала оцінювання:

За шкалою університуту	За національною шкалою	За шкалою ECTS
90–100	відмінно	A (відмінно)
85–89	добре	B (дуже добре)

75-84		C (добре)
65-74	задовільно	D (задовільно)
60-64		E (достатньо)
35-59	незадовільно	FX (незадовільно з можливістю повторного складання)
1-34		F (незадовільно з обов’язковим повторним курсом)