Силабус навчальної дисципліни

№	Назва поля	Детальний контент, коментарі
1.	Назва факультету	Факультет Комп’ютерної інженерії та управління
2.	Рівень вищої освіти	Магістерський
3.	Код і назва спеціальності	F7 Комп’ютерна інженерія
4.	Тип і назва освітньої програми	ОПП Спеціалізовані комп’ютерні системи (СКС)
5.	Назва дисципліни	Комп'ютерні загрози: методи детектування та аналізу (КУ:МДтА)
6.	Кількість ЄКТС кредитів	4 кредити (120 годин)
7.	Структура дисципліни (розподіл за видами та годинами навчання)	24 г. – 12 лк, 16 г. – 4 лб, 8 г. – 4 конс, 72 г. – самостійна робота, вид контролю – залік.
8.	Графік (терміни) вивчення дисципліни	1-й рік, 2-й семестр
9.	Передумови для нав-чання за дисципліною	Перелік раніше здобутих результатів навчання (спеціальні, фахові, предметні) компетентності: **P11** Здатність оформляти результати технічного аналізу у вигляді звітів, презентацій та технічної документації, зокрема результатів аналізу шкідливого програмного забезпечення та комп’ютерних загроз; **P12** Здатність ідентифікувати, класифікувати та описувати комп’ютерні загрози, їх поведінкові характеристики та вплив на програмно-технічні системи із використанням аналітичних методів; **P13** Здатність застосовувати методи статичного та динамічного аналізу програмного забезпечення для виявлення вразливостей та шкідливої функціональності; **P14** Здатність аналізувати машинний код, використовувати інструменти дизасемблювання та здійснювати базовий реверсивний інжиніринг програм; **P15** Здатність обґрунтовувати вибір методів детектування загроз, інтерпретувати результати аналізу та приймати рішення щодо реагування на інциденти безпеки; **N1** Знати архітектуру комп’ютерних систем (зокрема IA-32/IA-86 та ARM), принципи виконання програм та основи операційних систем; **N2** Знати принципи роботи комп’ютерних мереж, базові протоколи передачі даних та основи мережевої безпеки; **N3** Мати базові знання з програмування (мови рівня C/C++/Python або аналогічні), структури даних та алгоритмів; **N4** Знати основи інформаційної безпеки, типи атак та моделі загроз; **N5** Мати навички роботи з інструментами аналізу (відлагоджувачі, дизасемблери, sandbox-середовища, системи моніторингу); **N6** Розуміти принципи роботи віртуалізації та хмарних середовищ, включаючи базові моделі розгортання та безпеки.
10.	Анотація (зміст) дисципліни	Лекційні теми. **Змістовий модуль 1.**

		Тема 1. Теоретичні відомості про комп'ютерні загрози. Тема 2. Статичні методи аналізу. Тема 3. Динамічні методи аналізу. Тема 4. Дизасемблювання IA-86/ARM. **Змістовий модуль 2.** Тема 1. Сучасні методи детектування загроз. Тема 2. Аналіз загроз в Пісочниці. Тема 3. Аналіз таргетованих атак. Тема 4. Аналіз та детктування хмарних загроз. **Лабораторні заняття.** 1. Детектування шкідливих программ 2. Статичний аналіз загроз 3. Динамічний аналіз загроз 4. Дизасемблювання та реверсивний інжинирінг
11.	Компетентності, знання, вміння, розуміння, якими оволодіє здобувач вищої освіти в процесі навчання	За результатом вивчення дисципліни студенти повинні: **знати:** теоретичні основи комп'ютерних загроз та шкідливого програмного забезпечення; класифікацію та моделі атак; принципи статичного та динамічного аналізу програм; основи дизасемблювання та архітектур IA-86/ARM; сучасні підходи до детектування загроз; принципи роботи sandbox-середовищ; особливості таргетованих атак (APT); базові підходи до аналізу та детектування загроз у хмарних інфраструктурах; **вміти:** застосовувати методи статичного аналізу (аналіз коду, сигнатур, структур файлів); виконувати динамічний аналіз із використанням sandbox та інструментів моніторингу; використовувати дизасемблери та відлагоджувачі для аналізу виконуваних файлів; ідентифікувати ознаки шкідливої поведінки програм; аналізувати мережеву активність програм; застосовувати сучасні методи детектування загроз; інтерпретувати результати аналізу та формувати технічні звіти; **розуміти:** внутрішню логіку виконання програм на рівні машинного коду; взаємозв'язок між поведінкою програми та її впливом на систему; обмеження різних методів аналізу (статичних, динамічних, поведінкових); принципи обходу детекції шкідливим ПЗ; особливості загроз у віртуалізованих та хмарних середовищах; **володіти (перелік сформованих компетентностей):** загальні компетентності: ЗК-3 Здатність до критичного мислення та аналізу складних технічних систем; ЗК-5 Здатність до самостійного навчання та освоєння нових інструментів і технологій; ЗК-6 Здатність приймати обґрунтовані рішення в умовах невизначеності та неповної інформації; ЗК-8 Здатність ефективно комунікувати результати технічного аналізу у професійному середовищі; фахові компетентності: ФК-7 Здатність застосовувати методи аналізу програмного забезпечення для виявлення загроз та вразливостей; ФК-8 Здатність виконувати реверсивний інжиніринг програм та аналіз машинного коду; ФК-9 Здатність використовувати сучасні інструменти та

		середовища для дослідження шкідливого ПЗ; ФК-10 Здатність здійснювати аналіз та детектування комп'ютерних загроз у мережевих та хмарних середовищах; ФК-11 Здатність оцінювати ефективність методів захисту та виявлення загроз, обґрунтовувати вибір підходів до забезпечення безпеки.
12.	Результати навчання здобувача вищої освіти	Програмні результати навчання: ПРН-1 Розуміти природу комп'ютерних загроз, їх класифікацію та механізми реалізації атак; ПРН-2 Вміти здійснювати пошук, відбір та аналіз інформації про сучасні загрози та шкідливе програмне забезпечення з різних джерел; ПРН-3 Вміти застосовувати методи статичного аналізу для дослідження програмного забезпечення та виявлення потенційно шкідливих ознак; ПРН-4 Вміти виконувати динамічний аналіз програм із використанням sandbox-середовищ та інструментів моніторингу; ПРН-5 Вміти використовувати інструменти дизасемблювання та відлагодження для аналізу машинного коду (IA-86/ARM); ПРН-6 Вміти виявляти поведінкові ознаки шкідливого програмного забезпечення та інтерпретувати результати аналізу; ПРН-7 Вміти застосовувати сучасні методи детектування загроз у комп'ютерних системах; ПРН-8 Вміти проводити аналіз загроз у sandbox-середовищах та оцінювати їх ефективність; ПРН-9 Вміти аналізувати таргетовані атаки (APT) та визначати їх характерні особливості; ПРН-10 Вміти здійснювати базовий аналіз та детектування загроз у хмарних середовищах; ПРН-11 Вміти оцінювати обмеження різних методів аналізу (статичних, динамічних, поведінкових) та обирати доцільний підхід; ПРН-12 Вміти оформлювати результати технічного аналізу у вигляді звітів та аргументовано представляти їх.
13.	Система оцінювання відповідно до кожного завдання для складання заліку/екзамену	Відпрацювати та захистити 4 лабораторні роботи. Як захід підсумкового контролю для дисципліни ОНДАП використовується залік. При оцінювання роботи студента протягом семестру підсумкова рейтингова оцінка розраховується як сума оцінок за різні види занять та контрольні заходи. Лабораторні роботи оцінюються від 10 до 25 балів та за сумою складають 100 балів. Максимальний можливий рейтинговий бал протягом семестру – 100 балів.
14.	Якість освітнього процесу	Дотримання принципів академічної доброчесності (http://lib.nure.ua/plagiat) та Положення про організацію освітнього процесу в ХНУРЕ. Оновлення робочої програми дисципліни – 2024 р.
15.	Методичне забезпечення	1. Комплекс навчально-методичного забезпечення навчальної дисципліни "Комп'ютерні загрози: методи детектування та аналізу", спеціальність 123 - Комп'ютерна інженерія, спеціалізація "Спеціалізовані комп'ютерні системи" [Електронний ресурс] / ХНУРЕ ; розроб. О. С. Адамов. – Харків, 2017. – 379 с.

16.	Розробник силабусу (посада, ПІБ, ел. пошта)	В. І. Обрізан, к. т. н., ст. викл. каф. АПОТ, E-mail: <vladimir.obrizan@nure.ua>