Силабус навчальної дисципліни

№	Назва поля	Детальний контент, коментарі
1.	Назва факультету	Факультет Комп'ютерної інженерії та інформаційних технологій
2.	Рівень вищої освіти	Бакалаврський
3.	Код і назва спеціальності	F7 Комп’ютерна інженерія
4.	Тип і назва освітньої програми	ОПП Комп’ютерна інженерія
5.	Назва дисципліни	Комп'ютерні віруси і засоби боротьби з ними (КВіЗБ)
6.	Кількість ЄКТС кредитів	3 кредити (104 годин)
7.	Структура дисципліни (розподіл за видами та годинами навчання)	20 г. – 10 лк, 16 г. – 4 лб, 8 г. – 4 конс, 72 г. – самостійна робота, вид контролю – залік.
8.	Графік (терміни) вивчення дисципліни	4-й рік, 7-й семестр
9.	Передумови для нав-чання за дисципліною	Перелік раніше здобутих результатів навчання (спеціальні, фахові, предметні) компетентності: **P11** Здатність оформляти результати аналізу інформаційної безпеки у вигляді технічних звітів, пояснювальних записок та презентацій; **P12** Здатність ідентифікувати, класифікувати та описувати комп’ютерні віруси, вразливості та загрози безпеки інформації; **P13** Здатність застосовувати базові методи аналізу програмного забезпечення для виявлення потенційно небезпечної поведінки; **P14** Здатність використовувати інструменти дослідження програм (браузерні інструменти розробника, базові засоби аналізу виконуваного коду, дизасемблери на початковому рівні); **P15** Здатність оцінювати ризики інформаційної безпеки та обґрунтовувати вибір методів захисту інформаційних систем; **N1** Знати основи функціонування комп’ютерних систем та операційних систем (процеси, пам’ять, файлові системи); **N2** Знати базові принципи роботи комп’ютерних мереж, протоколів передачі даних та клієнт-серверної взаємодії; **N3** Мати базові знання з програмування (скриптові мови, такі як JavaScript або Python) та розуміння структури програм; **N4** Знати основи інформаційної безпеки, типи атак, базові поняття (вразливість, експлойт, шкідливе ПЗ, соціальна інженерія); **N5** Мати навички роботи з веб-технологіями (HTTP, браузери, клієнтські скрипти) для аналізу вразливостей; **N6** Розуміти базові принципи захисту інформаційних систем, включаючи антивірусний захист, контроль доступу та оновлення програмного забезпечення.
10.	Анотація (зміст) дисципліни	Лекційні теми. **Змістовий модуль 1.** Тема 1. Історія виникнення комп’ютерних вірусів. Тема 2. Теоретичні відомості про комп'ютерні віруси Тема 3. Класифікація вірусів. Тема 4. Загрози безпеки інформації. **Змістовий модуль 2.**

		Тема 1. Що таке антивірус. Тема 2. Захист шлюзів. Тема 3. Захист поштових систем. Тема 4. Захист серверів та робочих станцій. Лабораторні заняття. 1. Дослідження вразливостей браузерів та їх реалізації в скрипт технологіях 2. Основи роботы з дизассемблером 3. Технології розпакування виконуваного коду 4. Основні ознаки присутності шкідливих програм і методи по усунення наслідків вірусних заражень
11.	Компетентності, знання, вміння, розуміння, якими оволодіє здобувач вищої освіти в процесі навчання	Мета: Надати розгорнуте уявлення о проблемі вірусної загрози у мережах різного масштабу, методах боротьби з вірусами та принципах будови комплексних систем антивірусного захисту. Завдання. Навчити виявляти комп'ютерні загрози у мережах різного масштабу, методах боротьби з вірусами та принципах будови комплексних систем антивірусного захисту. У результаті вивчення навчальної дисципліни студент повинен знати: основи теорії комп'ютерних вірусів та основних отриманих на сьогодні результатів, одним з яких є неможливість створення універсального антивірусу. Принципи класифікації шкідливих програм, сучасні тенденції розвитку загроз виниклих через використання програмного забезпечення. Існуючі принципи і технології застосованих в боротьбі з шкідливими програмами та іншими мережевими загрозами. Нормативно-правову основу для створення систем антивірусного захисту.
12.	Результати навчання здобувача вищої освіти	Програмні результати навчання: ПРН-2 використовувати загальні принципи побудови системи антивірусного захисту. Описати продукти для захисту систем та мереж, розкрити призначення та основні можливості кожного з них (або знати призначення та основні можливості по захисту інформації від сучасних загроз). Спроектувати оптимальне рішення по захисту корпоративної мережі організації. Виконати впровадження системи антивірусного захисту. Здійснювати обслуговування впровадженої системи на всіх стадіях експлуатації.
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 віруси та засоби боротьби з ними" підготовка бакалавр, спеціальність 123 - Комп'ютерна інженерія [Електронний ресурс] / ХНУРЕ; розроб. О. С. Адамов. – Харків, 2017. – 126 с.

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