Силабус вибіркової дисципліни

№	Назва поля	Детальний контент, коментарі
1.	Назва факультету	Факультет інфокомунікацій
2.	Рівень вищої освіти	Bachelor's, educational and scientific
3.	Код і назва спеціальності	125 Кібербезпека
4.	Тип і назва освітньої програми	ОПП «Управління інформаційною безпекою»
5.	Код і назва дисципліни (інформація з ЦІСТ)	ОАВтЄХ - Основи аналізу вразливостей й етичного хагінгу
6.	Кількість ЄКТС кредитів	5
7.	Структура дисципліни (розподіл за видами та годинами навчання)	34 г. – 17 лк, 8 г. – 4 пз, 20 г. – 5 лб, 10 г. – 5 конс, 2 г. – РГЗ, вид контролю: залік
8.	Графік (терміни) вивчення дисципліни	3-й рік, 5-й семестр
9.	Передумови для навчання за дисципліною	Дисципліна базується на знаннях, отриманих в результаті вивчення дисциплін природничо-наукової підготовки (вища математика, фізика, алгоритмічні мови та програмування, комп'ютерні методи дослідження інформаційних процесів та систем, спеціальні розділи математики, основи теорії кіл, сигнали та процеси в інформаційно-комунікаційних системах, теорія інформації та кодування) з поглибленим вивченням дисциплін фахової підготовки (електроніка та мікросхемотехніка, алгоритмічні основи криптології, криптографічні системи та протоколи, WEB-програмування, комп'ютерні мережі, інформаційно-комунікаційні системи, бази даних та знань, архітектура комп'ютерних систем, мережеві операційні системи, методи та засоби криптоаналізу, обчислювальна техніка, захист інформації в інформаційно-комунікаційних системах, технології та спеціальні розділи програмування).
10.	Анотація (зміст) дисципліни	За результатом вивчення дисципліни студенти повинні знати засоби діагностування вразливостей web-додатків і IP-мереж, прийоми та засоби тестування на проникнення інформаційно-комунікаційних систем, методи налаштування, оптимізації і конфігурації операційної системи, СУБД, і мережевого устаткування, загальні терміни етичного хакінгу: вразливість, експлойт, корисне навантаження, тощо; вміти проводити аналіз інформації та синтезувати на основі цього якісно нову інформацію, зокрема проводити тестування на проникнення інформаційне - комунікаційних систем, виконувати налаштування, оптимізацію та конфігурацію операційної системи, СУБД, і мережевого устаткування для безпечного функціонування інформаційне - комунікаційних систем, реалізувати програми (сніфер, сканер портів, антивірусного

		програмного забезпечення). Мета опанування дисципліни в контексті підготовки фахівців певної освітньої програми. Забезпечити знання загальних основних принципів організації захисту інформації в інформаційно-комунікаційних системах та базову підготовку студентів спеціальності 125 «Кібербезпека» спеціалізації «Управління інформаційною безпекою» для раціонального вирішення питань, пов'язаних з захистом інформації в інформаційно-комунікаційних системах. Викладання навчальної дисципліни «Системи аналізу вразливостей та етичний хакінг» є формування у студентів уміння вирішувати задачі тестування на проникнення інформаційних мереж і систем, застосовувати нормативно-правові, організаційні та технічні процедури етичного хакінгу. Завдання полягає у формуванні теоретичних знань та практичних умінь у сфері тестування на проникнення та етичного хакінгу, інформаційної та кібернетичної безпеки.
11.	Компетентності, знання, вміння, розуміння, якими оволодіє здобувач вищої освіти в процесі навчання	Перелік компетентностей, яких набуде студент після опанування даної дисципліни. Фахова компетентність: КФ-5 — здатність до забезпечення захисту інформації, що обробляється в інформаційно-комунікаційних системах, здійснення адміністрування таких систем та проведення їх експлуатації Програмні результати навчання: ПРз-4 — знати методи і способи розробки та тестування програмного забезпечення з виявлення і усунення активності, що загрожує безпеці системи (антивіруси, firewalls, сніфери, сканери портів). ПРз-5 — вміти проводити семантичний аналіз файлів; вміти виявляти злоякісне програмне забезпечення й файли за їх структурою та поведінкою; вміти відновлювати пошкоджену інформацію; вміти моделювати уразливості ПЗ та використовувати шаблони проектування для захисту ПЗ. ПРз-9 — володіти практичними навичками проведення аудиту безпеки ІКС, їх адміністрування та експлуатації; вміти проектувати перспективні криптосистеми та застосовувати сучасні технології криптографічного захисту інформації в системах інформаційної та/або кібербезпеки.
12.	Результати навчання здобувача вищої освіти	Програмні результати навчання: ПР 1 - виявляти наукову сутність задач, знаходити адекватні шляхи їх розв’язання; - розуміти шляхи самостійного освоєння нових методів досліджень, нового наукового й науково-виробничого профілю діяльності; - здійснювати науково-дослідну роботу в процесі розробки нових технологій забезпечення інформаційної та кібернетичної безпеки об’єктів інформаційної діяльності.

13.	Система оцінювання відповідно до кожного завдання для складання заліку/екзамену	1. Відпрацювати та захистити лабораторні роботи. 2. Виконати контр. роботи на практичних заняттях. 3. Отримати за семестр не менше 60 балів. 4. Скласти екзамен. Оцінка за семестр $O_{\text{сем}}$: (6-10)х4 лб+(6-10)х4 пз+(12-20)х1РГЗ=(60-100) балів. Оцінка за екзамен (залік) $O_{\text{екз}}$ =(60-100) балів. Екзамен комбінований у формі комп. тесту (20 завдань, тривалість 60 хв.). Підсумкова оцінка $O_{\text{д}}^{\text{екз}}$ обчислюється за формулою: $O_{\text{д}}^{\text{екз}} = 0,6 \cdot O_{\text{сем}} + 0,4 \cdot O_{\text{екз}}$.
14.	Якість освітнього процесу	Оновлена робоча програма дисципліни – 2021-2022 уч. р. Лабораторний практикум забезпечено сучасним апаратним та програмним забезпеченням. Необхідний обсяг знань для одержання позитивної оцінки (Якісні критерії оцінювання: Загально теоретичні основи етнічного хакінгу. Методи тестування на проникнення. Основні нормативні документи Верховної Ради та Кабінету Міністрів України, міжнародні закони про конфіденційність та кібербезпеку. Підходи до статичного аналізу коду. Підходи до динамічного аналізу коду. Підготовка звіту з висновками та рекомендаціями по завершенню тестування на проникнення. Підготовка реферату з тематики методологія оцінки ризиків за інформаційною системою оцінки безпеки (ISSAF) (індивідуальне завдання).
15.	Методичне забезпечення	Базова література 1.Messier R. Penetration Testing Basics: A Quick-Start Guide to Breaking into Systems / Ric Messier., 2016. — (Apress).. — 115 ст. 2.Penetration Testing Software.Metasploit [Електронний ресурс] — Режим доступу до ресурсу: https://www.metasploit.com. 3.Lepofsky R. The Manager's Guide to Web Application Security: A Concise Guide to the Weaker Side of the Web / Ron Lepofsky., 2014. — 232 с.. 4.Тецкий А.Г. Методи та засоби тестування на проникнення веб-додатків і мереж. / А.Г.Тецкий, О.А. Ілляшенко, Д. Д. Узун., 2017. — 77 с. Допоміжна література 5.Закон України про «Про основні засоби забезпечення кібербезпеки України». 6.Навчально–методичний посібник “Інформаційні технології в економіці та бізнесі” / Укладач: А.В. Журавка, Харків: ХНУБА, 2016. –116 с. 7.Навчально–методичний посібник “Економіко-

		математичне моделювання за допомогою електронних таблиць" /Укладач: Журавка А.В.– ХНУБА, 2018. – 132 с. 8.Методичні вказівки до практичних занять з дисципліни «Information Security in information and Communication Systems» (Інформаційна безпека в інформаційних та комунікаційних системах) (англ. мовою) для студентів денної форми навчання за спеціальністю 125 «Кібербезпека» [Електронне видання], Упоряд.: А.В. Журавка. – Харків: ХНУРЕ, 2019. – 90 с. 4.«DATABASE ADMINISTRATION AND SECURITY», guidelines for practics works on discipline for foreign students of the specialty «Cybersecurity», [Electronic resource], Composed by A.V.Zhuravka , Electronic Edition - Kharkiv: KNURE, 2020. – 62 p. 5.Навчальний посібник з дисципліни «Адміністрування та безпека баз даних» для студентів денної форми навчання за спеціальністю 125 «Кібербезпека» Упоряд.: А.В. Журавка. – Харків: ХНУРЕ, 2021. – 149 с. 6.Навчальний посібник з дисципліни «Database Administration and Security» для студентів денної форми навчання за спеціальністю 125 «Кібербезпека» Упоряд.: А.В. Журавка. – Харків: ХНУРЕ, 2022. – 139 с.
16.	Розробник силабусу (посада, ПІБ, ел. пошта)	А.В. Журавка, проф. каф. ІКІ, Ph.D. E-mail: Andrii.Zhuravka@nure.ua