ДЕРЖАВНИЙ УНІВЕРСИТЕТ «КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»	**Силабус навчальної дисципліни «Технології етичного хакінгу» «Ethical hacking technologies»** Освітньо-наукова програма: Кібербезпека Спеціальність: F5 Кібербезпека та захист інформації Галузь знань: F Інформаційні технології
Рівень вищої освіти	Третій (освітньо-науковий)
Статус дисципліни	Навчальна дисципліна вибіркового компонента вибору фахового переліку
Курс	1 (перший)
Семестр	2 (другий)
Обсяг дисципліни, кредити ЄКТС/години	5 кредитів / 150 год
Мова викладання	Українська або англійська
Що буде вивчатися (предмет вивчення)	Предметом вивчення дисципліни «Технології етичного хакінгу» є методи та інструменти перевірки інформаційних систем на вразливості з метою їх подальшого усунення та підвищення рівня безпеки.
Чому це цікаво/треба вивчати (мета)	У межах курсу розглядатимуться основи тестування на проникнення, аналізу мережевих протоколів, виявлення й експлуатації типових кібератак, а також застосування спеціалізованого програмного забезпечення для моделювання можливих загроз. Особлива увага приділятиметься дотриманню правових та етичних норм, що регламентують діяльність у сфері етичного хакінгу, формуванню практичних навичок безпечного проведення аудиту систем і впровадженню рекомендацій для захисту інформаційних ресурсів.
Чому можна навчитися (результати навчання)	**РН1.** Мати передові концептуальні та методологічні знання з кібербезпеки та захисту інформації і на межі предметних галузей, а також дослідницькі навички, достатні для проведення наукових і прикладних досліджень на рівні останніх світових досягнень з кібербезпеки та захисту інформації, отримання нових знань та/або здійснення інновацій. **РН2**. Планувати і виконувати експериментальні та/або теоретичні дослідження з кібербезпеки та захисту інформації та дотичних міждисциплінарних напрямів з використанням сучасних інструментів та дотриманням норм професійної і академічної етики. **РН5**. Формулювати і перевіряти гіпотези; використовувати для обґрунтування висновків належні докази, зокрема, результати теоретичного аналізу, експериментальних досліджень і математичного та/або комп'ютерного моделювання, наявні літературні дані. **РН7**. Застосовувати загальні принципи та методи математики, інформатики та інших наук, а також сучасні методи та інструменти, цифрові технології та спеціалізоване програмне забезпечення для провадження наукових досліджень у сфері кібербезпеки та захисту інформації. **РН8**. Розробляти та досліджувати концептуальні, математичні і комп'ютерні моделі процесів і систем, ефективно використовувати їх для отримання нових знань та/або створення інноваційних продуктів у кібербезпеки та захисту інформації та дотичних міждисциплінарних напрямах.

Як можна користуватися набутими знаннями і уміннями (компетентності)	**Загальні компетентності:** **ЗК1**. Здатність до абстрактного мислення, аналізу і синтезу. **ЗК2.** Здатність до пошуку, оброблення та аналізу інформації з різних джерел. **ЗК3.** Здатність працювати в міжнародному контексті. **ЗК4.** Здатність розв'язувати комплексні проблеми предметної області на основі системного наукового світогляду та загального культурного кругозору із дотриманням принципів професійної етики та академічної доброчесності. **Спеціальні (фахові) компетентності:** **СК1.** Здатність виконувати оригінальні дослідження, досягати наукових результатів, які створюють нові знання у сфері кібербезпеки та захисту інформації та дотичних міждисциплінарних напрямах і можуть бути опубліковані у провідних наукових виданнях з кібербезпеки та захисту інформації. **СК2.** Здатність ініціювати, розробляти і реалізовувати комплексні наукові та інноваційні проєкти в сфері кібербезпеки та захисту інформації **СК3.** Здатність розв'язувати значущі проблеми в сфері кібербезпеки та захисту інформації., розширювати та переоцінювати наявні знання і професійні практики. **СК4.** Здатність ефективно застосовувати методи аналізу даних, концептуального, математичного та комп'ютерного моделювання, виконувати натурні та обчислювальні експерименти при проведенні наукових і прикладних досліджень у сфері кібербезпеки та захисту інформації. **СК5.** Здатність генерувати нові ідеї щодо розвитку теорії та практики кібербезпеки та захисту інформації, виявляти, ставити та вирішувати проблеми дослідницького характеру, оцінювати та забезпечувати якість виконуваних досліджень. **СК8**. Здатність до застосування сучасних технологій машинного навчання, штучного інтелекту, обробки великих даних, нейронних мереж, високопродуктивних обчислень для їх оптимізації та синтезу їх нових функціональних можливостей у концепції сталого розвитку.
Навчальна логістика	Дисципліна «Технології етичного хакінгу» охоплює вивчення основ і принципів етичного хакінгу, життєвого циклу тестування на проникнення, методів збору та аналізу інформації про цілі, виявлення й експлуатації вразливостей операційних систем, мереж і веб-додатків, атак на бездротові мережі та IoT-пристрої, застосування технік соціальної інженерії, основ реверс-інжинірингу та створення експлойтів, методів закріплення доступу й приховування активності. Значна увага приділяється формуванню практичних навичок використання сучасних інструментів пентестингу (Burp Suite, Metasploit та ін.), документуванню результатів, підготовці рекомендацій із підвищення кіберстійкості, а також вивченню новітніх тенденцій, включно з автоматизацією тестів і застосуванням штучного інтелекту. **Види занять:** лекції, практичні. **Методи навчання:** проблемний виклад, дослідницькі методи, презентації, бесіди та дискусії, робота в Google Classroom (електронні лекції, семінари, практичні роботи, дистанційні консультації, тестування). **Форми навчання:** очна, дистанційна.
Пререквізити	Базові знання з дисциплін «Методологія наукових досліджень у сфері кібербезпеки та захисту інформації»

Інформаційне забезпечення	**Навчальна та наукова література:** 1. Cybersecurity Attacks — Red Team Strategies (Packt, 2020) 2. Advanced Security Testing with Kali Linux — Daniel W. Dieterle (2022) 3. Guide to Pentesting — Milo Caranti (2020) 4. Web Application PenTesting: A Comprehensive Guide for Professionals (River Publishers) (2021) 5. Real-World Bug Hunting / Bug Bounty case collections (editions 2020–2024)	
Локація та матеріально-технічне забезпечення	Аудиторія теоретичного навчання, Проектор	
Семестровий контроль, екзаменаційна методика	Модульна контрольна робота, залік	
Кафедра	Кафедра кібербезпеки	
Факультет	Факультет комп'ютерних наук та технологій	
Викладач(і)		**Аушев Єгор Володимирович** **Посада:** доцент кафедри кібербезпеки, CEO у CyberUnitTech **Науковий ступінь:** к.ф.-м.н. **Вчене звання:** доцент **Профайл викладача:** https://ua.linkedin.com/in/dr-yegor-aushev-54b18455 **E-mail:** yehor.aushev@npp.nau.edu.ua **Робоче місце:** 11.118
Оригінальність навчальної дисципліни	Авторський курс, викладання українською або англійською мовами.	
Лінк на дисципліну	Після формування групи слухачів створюється кабінет в Google Classroom з необхідними матеріалами для навчання	
Максимальна кількість слухачів	20	