СИЛАБУС
Кафедра кібербезпеки та математичного моделювання

Назва курсу	Тестування на проникнення та етичний хакінг
Мова викладання	Українська
Викладач (-і)	М.Є. Шелест професор кафедри кібербезпеки та математичного моделювання, доктор технічних наук, професор
Профайл викладача (-ів)	0000-0001-7110-4876
Контакти викладача	mishel3141@gmail.com

1. Анотація курсу – в даному курсі розглядаються загрози для інформаційних систем, вивчаються їх вразливості, формуються теоретичні знання та практичні навички щодо проведення тестування на проникнення Тематика курсу – сучасні інформаційні технології.

2. Мета та цілі курсу – формування науково-професійного світогляду магістра спеціальності *Кібербезпека* в області безпеки інформаційних і комунікаційних систем, уміння вирішувати задачі адміністрування мереж та систем, проводити тестування інформаційних систем на проникнення.

Під час вивчення дисципліни здобувач вищої освіти (ЗВО) має набути або розширити наступні загальні (КЗ) та фахові (КФ) компетентності, передбачені освітньою програмою спеціальності 125 - Кібербезпека:

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.

КЗ 2. Знання та розуміння предметної області та розуміння професії.

КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.

КЗ 6. Здатність до відповідальності та навичок до безпечної діяльності відповідно до майбутнього профілю роботи, галузевих норм і правил, а також необхідного рівня індивідуального та колективного рівня безпеки у надзвичайних ситуаціях.

КФ 2. Здатність розробляти, впроваджувати і супроводжувати програмні та програмно-апаратні комплекси засобів інформаційної безпеки та/або кібербезпеки в інформаційно-комунікаційних системах (автоматизованих систем та їх додатків) та у інфраструктурі організації в цілому.

КФ 3. Здатність до проектування, впровадження, супроводження інформаційних мереж і ресурсів, інфраструктури установи, архітектури використання інформаційних технологій (хмарних), а також бізнес/операційних процесів з метою якісного функціонування інформаційно-комунікаційних систем (комутативних або без комутативних), згідно встановленої політики інформаційної безпеки та/або кібербезпеки і

стратегії організації.

КФ 5. Здатність розробляти, планувати, аналізувати та впроваджувати систему доступу до інформаційних ресурсів, а також систему аудиту і контролю ефективності функціонування інформаційно-комунікаційних систем (вузлів доступу до глобальних мереж, програмно-апаратних комплексів, підсистем, тощо), згідно встановленої політики інформаційної безпеки та/або кібербезпеки і стратегії організації.

КФ 6. Здатність розробляти та впроваджувати заходи протидії кіберінцидентам, а також аналізувати, здійснювати процедури управління та контролю інцидентами, організовувати та проводити розслідування, надавати рекомендації щодо заходів їх попередження та протидії.

3. Результати навчання

Під час вивчення дисципліни ЗВО має досягти або вдосконалити наступні програмні результати навчання (ПРН), передбачені освітньою програмою:

ПРН 2. Планувати та організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність.

ПРН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.

ПРН 4. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

ПРН 5. Реалізовувати процеси постійної самоосвіти і професійної сертифікації, критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.

ПРН 7. Проектувати, впроваджувати, та супроводжувати інформаційно-комунікаційні системи, а також забезпечувати захист інформаційних ресурсів мереж (мережева безпека) та всієї інфраструктури установи на базі сучасних моделей, методів і засобів передачі даних в комутативних або без комутативних каналах зв'язку, хмарного простору, протоколів обміну даними, мережного устаткування, тощо.

ПРН 8. Проектувати, впроваджувати, супроводжувати системи та комплекси (програмні, програмно-апаратні) захисту додатків (веб - додатків) з метою забезпечення якісного функціонування інформаційно-комунікаційних систем, згідно встановленої політики інформаційної безпеки та/або кібербезпеки і стратегії організації.

ПРН 11. Розробляти, впроваджувати, супроводжувати системи аудиту та моніторингу (контролю) якості бізнес/операційних процесів функціонування організації та системи управління інформаційною безпекою та/або кібербезпекою за вітчизняними і світовими нормами та стандартами.

ПРН 12. Розробляти, впроваджувати та супроводжувати процеси належного функціонування системи моніторингу інформаційних ресурсів і бізнес процесів в інфраструктурі організації.

ПРН 13. Проводити та планувати навчання персоналу компанії, користувачів з інформаційних технологій організації у відповідності до сучасних норм, вимог, внутрішніх правил безпечного застосування інформаційних технологій, а також у відповідність вітчизняним і світовим стандартам галузі інформаційної та\або кібербезпеки.

Після курсу здобувач вищої освіти отримає наступні навички:

1. проводити сканування мереж;
2. проводити збір даних у мережах;
3. використовувати вразливості інформаційних систем;
4. протидіяти збиранню інформації у мережах;
5. проводити тестування на проникнення;
6. захищати інформаційні системи від кібератак.

4. Обсяг курсу. Зазначте загальну кількість кредитів, кількість занять та годин самостійної роботи

Вид заняття	**Загальна к-сть годин**
лекції	22
практичні заняття	18
самостійна робота, реферат	110

5. Пререквізити – для вивчення даної дисципліни бажаним є прослуховування курсу «Комп'ютерні мережі».

6. Система оцінювання та вимоги

Загальна система оцінювання курсу	З дисципліни ЗВО може набрати до 60% підсумкової оцінки за виконання всіх видів робіт, що виконуються протягом семестру і до 40% підсумкової оцінки – на заліку.
Вимоги до реферату	Відповідність умовам завдання – до 5 балів; посилання на першоджерела – до 5 балів; своєчасність здачі – до 5 балів. Захист реферату: самостійність виконання (відповіді на запитання) – до 5 балів.
Умови допуску до підсумкового контролю	У випадку, якщо ЗВО протягом семестру не виконав в повному обсязі передбачених робочою програмою всіх видів навчальної роботи, має невідпрацьовані лабораторні роботи або не набрав мінімально необхідну кількість балів (20), він не допускається до складання екзамену під час сесії, але має право ліквідувати академічну заборгованість у порядку, передбаченому «Положенням про поточне та

	підсумкове оцінювання знань ЗВО ЧНТУ».

7. Політики курсу - Виконання та особистий захист усіх практичних робіт, зазначених у робочій навчальній програмі з дисципліни, є обов'язковим. Поточний контроль проводиться шляхом спілкування із ЗВО під час лекцій та консультацій та опитувань ЗВО під час захисту практичних робіт.

8. Рекомендована література

1. Peter Kim. The Hacker Playbook 3: Practical Guide To Penetration Testing — 289 p.
2. Weidman G. Penetration Testing: A Hands-On Introduction to Hacking — 528 p.
3. Graham, E., Steinbart, P.J. Wireless Security. 2006.
4. Cisco. Dictionary attack on Cisco LEAP vulnerability, Revision 2.1, 19 July 2004.