Міністерство освіти і науки України
Національний університет «Чернігівська політехніка»
Навчально-науковий інститут
електронних та інформаційних технологій
Кафедра кібербезпеки та математичного моделювання

РОБОЧА ПРОГРАМА
Тестування на проникнення та етичний хакінг

ЗАТВЕРДЖУЮ
Завідувачка кафедри
_____ *Ткач Ю.М.*
(підпис) (прізвище та ініціали)
«26» серпня 2025 р.

Розробник: Семендяй Сергій Матвійович, старший викладач кафедри кібербезпеки та математичного моделювання _____

Робочу програму навчальної дисципліни обговорено на засіданні кафедри кібербезпеки та математичного моделювання

Протокол від «__26___»___08_____202_5_р. №_6___

Узгоджено з гарантом освітньої програми: _____ *Ткач Ю.М.*

---

1. Загальна інформація про дисципліну

Тип дисципліни	Вибіркова
Мова викладання	Українська
Рік навчання та семестр	Перший рік, другий семестр. F5 Кібербезпека та захист інформації ОПП Кібербезпека
Викладач (-і)	Семендяй Сергій Матвійович, старший викладач кафедри кібербезпеки та математичного моделювання
Профайл викладача (-ів)	https://mmi.stu.cn.ua/personal-kafedry/ https://scholar.google.com/citations?hl=ru&user=0T31xGYAAAAJ https://orcid.org/0000-0002-7751-5956 https://www.scopus.com/authid/detail.uri?authorId=58751294500
Контакти викладача	+380952859046, serhii_semendiai@icloud.com
Сторінка курсу в системі дистанційного навчання	https://eln.stu.cn.ua/course/view.php?id=4451

2. Анотація курсу.

Дисципліна “Тестування на проникнення та етичний хакінг” охоплює теоретичні основи, методології та практичні аспекти оцінки безпеки інформаційних систем шляхом імітації атак зловмисників. Курс спрямований на формування у студентів навичок проведення етичного хакінгу, виявлення вразливостей у програмному забезпеченні, мережах та системах управління, а також розробки рекомендацій щодо їх усунення.

Програма курсу включає аналіз основних методологій тестування на проникнення (PTES, OWASP, NIST), використання сучасних інструментів (Metasploit, Burp Suite, Nmap, Wireshark тощо), а також вивчення правових та етичних аспектів діяльності спеціалістів у сфері кібербезпеки.

В результаті вивчення дисципліни магістри зі спеціальності F5 – Кібербезпека та захист інформації набудуть практичного досвіду проведення тестів на проникнення, аналізу ризиків, документування знайдених вразливостей та формування звітності для підвищення безпеки інформаційних систем.

3. Мета та цілі курсу.

Метою викладання навчальної дисципліни “Тестування на проникнення та етичний хакінг” є формування у студентів теоретичних знань та практичних навичок з тестування на проникнення та етичного хакінгу для виявлення, аналізу та усунення вразливостей інформаційних систем, а також забезпечення належного рівня кібербезпеки в організаціях.

Об’єкт вивчення – інформаційні системи, мережі, програмне забезпечення та їхні компоненти, що підлягають тестуванню на проникнення та оцінці безпеки.

Предмет дисципліни – методи, інструменти та техніки тестування на проникнення, методології етичного хакінгу, способи виявлення вразливостей та аналіз ризиків інформаційної безпеки.

Основними завданнями вивчення дисципліни “ Тестування на проникнення та етичний хакінг” є:

– ознайомлення з теоретичними основами тестування на проникнення та етичного хакінгу;

– вивчення стандартних методологій тестування на проникнення (PTES, OWASP, NIST, OSSTMM);

– формування навичок використання спеціалізованих інструментів (Metasploit, Nmap, Burp Suite, Wireshark тощо);

– розвиток вмінь планування та проведення тестів на проникнення, аналізу їхніх результатів;

– опанування методів документування знайдених вразливостей та розробки рекомендацій щодо їх усунення;

– вивчення правових та етичних аспектів діяльності фахівців у сфері кібербезпеки;

– формування аналітичного мислення щодо оцінки ризиків та потенційних загроз в інформаційних системах.

4. Результати навчання

Під час вивчення дисципліни здобувач вищої освіти має набути або розширити наступні загальні (КЗ) та фахові (КФ) компетентності, передбачені освітньою програмою спеціальності F5 – Кібербезпека та захист інформації:

КЗ1. Здатність застосовувати знання у практичних ситуаціях.

КЗ3. Здатність до абстрактного мислення, аналізу та синтезу.

КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.

КФ5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

КФ7. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.

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

ПРН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.

ПРН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

ПРН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

ПРН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.

ПРН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

ПРН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.

ПРН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.

У підсумку ЗВО повинні знати :

1) Теоретичні основи тестування на проникнення:
   – основні поняття, принципи та методи тестування на проникнення та етичного хакінгу;
   – класифікацію атак, їхню природу та можливі наслідки.
2) Методології та стандарти безпеки:
   – основні міжнародні методології тестування на проникнення (PTES, NIST, OSSTMM, OWASP);
   – стандарти кібербезпеки та найкращі практики захисту інформаційних систем.
3) Інструменти для тестування на проникнення:
   – використання спеціалізованих програмних засобів, таких як Metasploit, Nmap, Burp Suite, Wireshark, John the Ripper, Hydra тощо;
   – методи автоматизованого та ручного пошуку вразливостей у вебдодатках, мережах і системах.
4) Аналіз вразливостей та експлуатація:
   – види вразливостей (SQL-ін'єкції, XSS, CSRF, RCE, LFI/RFI, MITM-атаки тощо);
   – методи експлуатації вразливостей та вплив на систему.
5) Законодавчі та етичні аспекти:
   – основи етичного хакінгу, правові аспекти тестування на проникнення;
   – відповідальність фахівця з кібербезпеки та дотримання норм законодавства (наприклад, GDPR, ISO 27001, закони про кібербезпеку).
6) Процедури звітування та усунення вразливостей:
   – методи аналізу результатів тестування та оформлення звітів;
   – рекомендації щодо покращення безпеки та усунення виявлених проблем.

вміти :

- планувати й проводити тестування на проникнення;
- використовувати професійні інструменти для аналізу безпеки;
- виявляти й експлуатувати вразливості в інформаційних системах;
- оцінювати рівень ризику та надавати рекомендацій щодо захисту;
- забезпечувати дотримання етичних норм та юридичних вимог під час тестування.

5. Пререквізити

Для успішного засвоєння дисципліни “Тестування на проникнення та етичний хакінг” студент повинен мати базові знання та навички в наступних областях:

1) Теоретичні знання:

– базові принципи інформаційної безпеки, загрози та вразливості;

– розуміння роботи мережевих протоколів (TCP/IP, UDP, HTTP, DNS, ARP), адресації та маршрутизації;

– структура та основні принципи роботи Windows і Linux, розуміння файлових систем, процесів, прав доступу;

– базове володіння Python або Bash для автоматизації процесів тестування;

– базові навички роботи в командному рядку Windows (PowerShell, CMD) та Linux (термінал, основні команди, робота з файлами та мережами);

– основи SQL, принципи роботи реляційних баз даних (MySQL, PostgreSQL, SQLite).

2) Практичні навички:

– робота з Linux та Windows на рівні командного рядка (навігація, перегляд логів, налаштування мережі);

– використання Wireshark або аналогічних інструментів для аналізу мережевого трафіку;

– базове розуміння брандмауерів та систем виявлення вторгнень (IDS/IPS);

– вміння використовувати віртуальні машини (VirtualBox, VMware, Hyper-V) для створення тестових середовищ.

6. Обсяг курсу.

Вид заняття	Загальна кількість годин (очна/заочна форма навчання)
Лекції	16/6
Практичні заняття	16/6
Самостійна робота	88/108
Всього кредитів – *4*	120

Лекційні заняття – дистанційно в MS Teams.

Практичні заняття – очно в лабораторії кафедри та дистанційно в MS Teams.

Самостійна робота – з використанням системи дистанційного навчання університету, рекомендованих інформаційних джерел, презентацій, нормативно-правових актів тощо. Для студентів передбачена можливість проходження навчального курсу "Ethical Hacker" в Академії Cisco НУ "Чернігівська політехніка", розрахованого на 70 годин, із отриманням сертифікатів.

7. Тематика курсу

Змістовий модуль 1. Загрози для інформаційної безпеки

Тема 1. Етичний хакінг і тестування на проникнення

Предмет дисципліни, її цілі та задачі. Структура, завдання і форми контролю, основна література. Основні положення. Введення в статистику витоку інформації. Знайомство з термінологією безпеки. Вектори атак. Загрози для інформаційної безпеки. Хакінг та його концепція.

Знайомство зі стадіями хакінгу. Різновиди хакерських атак. Введення в стандарти інформаційної безпеки. Інформаційна безпека та закони.

Тема 2. Процес збирання інформації

Рекогносцировка, знайомство з її концепцією. Знайомство з методологією збирання інформації. Знайомство з інструментами, що можуть знадобитись для збирання інформації. Протидія збиранню інформації.

Тема 3. Процедура сканування

Алгоритм сканування мережі. Способи сканування. Знайомство з техніками виявлення живих хостів. Знайомство з техніками сканування відкритих портів. Знайомство з прийомами прихованого сканування. Яким чином можливо ухилитись від систем виявлення вторгнень. Сканування вразливостей. Збирання банерів. Прийоми формування мережевих діаграм вразливостей мостів. Введення в проксі. Введення в анонімайзери.

Тема 4. Характеристика хакінгу системи

Введення в схематизацію операційної системи. Де вразлива операційна система. Огляд способів хакінгу. Алгоритм системи хакінгу. Суть злому паролів. Прийоми підвищення рівня привілеїв. Суть приховування файлів. Суть шпигунського ПЗ.

Змістовий модуль 2. Аналіз шкідливого ПЗ
Тема 5. Шкідливе ПЗ. Трояни

Знайомство зі шкідливим ПЗ. Трояни, принципи роботи. Огляд видів троянів. Введення в концепції вірусів та черв'яків. Методи роботи вірусів. Види вірусів. Комп'ютерні черв'яки. Аналіз шкідливого ПЗ. Характеристика антивірусів. Характеристика антитроянського ПЗ. Виявлення шкідливого ПЗ.

Тема 6. Характеристика сніферів

Сніфінг, принципи роботи. Знайомство з видами сніфінгу. Знайомство з апаратними аналізаторами протоколів. Спуфінг. Знайомство з ARP-атаками. Знайомство з MAC-атаками. Знайомство з DHCP-атаками. Введення в порт SPAN. Як проходить отруєння DNS-кешу. Знайомство з методами протидії сніфінгу.

Тема 7. Відмова в обслуговуванні

Знайомство з концепцією Denial-of-Service. DDoS-атака. Знайомство з техніками атак DoS/DDoS. Бот-мережі. Знайомство з інструментарієм, за допомогою якого проводяться DoS-атаки. Як реалізується атака DDoS. Яким чином можливо протидіяти DoS-атакам. Знайомство з інструментарієм захисту від DoS.

Тема 8. Характеристика хакінгу бездротових мереж

Знайомство з концепціями. Суть шифрування. Які загрози можуть виникати для бездротових мереж. Прийоми виявлення бездротових мереж. Процес аналізу трафіка. Прийоми проведення атаки. Злом шифрування бездротових мереж. Знайомство з інструментарієм хакінгу. Знайомство з атаками на Bluetooth. Методи протидії атакам. Методи захисту бездротових мереж.

Практичні заняття (16 годин):

1. Сканування портів та проведення атаки – 4 години.
2. Отримання доступу до кореневої файлової системи – 2 години.
3. Сканування порту 21 – 2 години.
4. Злам WPA/WPA2 паролів – 4 години.
5. Знайомство з атаками на Bluetooth – 2 години.
6. Знайомство з техніками атак DoS/DDoS – 2 години.

Самостійна робота:

1. Етичний хакінг і тестування на проникнення.
2. Процес збирання інформації.
3. Процедура сканування.
4. Характеристика хакінгу системи.
5. Шкідливе ПЗ. Трояни.
6. Характеристика сніферів.
7. Відмова в обслуговуванні.
8. Характеристика хакінгу бездротових мереж.

8. Система оцінювання та вимоги

З дисципліни студент може набрати до 60% підсумкової оцінки за виконання всіх видів робіт, що виконуються протягом семестру і до 40% підсумкової оцінки – на екзамені.

Умовою допуску до екзамену є виконання всіх видів навчальної роботи передбачених даною робочою програмою – захист усіх практичних робіт, які виконувались у поточному семестрі, оформлення звіту по практичних роботах відповідно до стандартів.

Для захисту практичної роботи студент повинен відповісти на всі контрольні питання з методичних вказівок та на питання, за вибором викладача, з лекційного курсу по темі практичної роботи. За кожну практичну роботу студент отримує певну кількість балів з урахуванням максимальної кількості балів. При цьому враховується якість оформлення звіту та повнота відповідей на питання при захисті практичної роботи.

Для складання письмової компоненти модульного контролю існує перелік питань до модульного контролю. В залежності від повноти відповіді студент отримує певну кількість балів з урахуванням максимальної кількості балів. Студент, який не здає вчасно роботу, одержує оцінку нуль балів. Повторне складання студентом письмової компоненти модульного контролю не допускається.

Складання екзамену є обов'язковим елементом підсумкового контролю знань для студентів, які претендують на оцінку «добре» або «відмінно». Якщо студент виконав всі види робіт протягом семестру та набрав 60% підсумкової оцінки (тобто «задовільно»), то він, за бажанням, може залишити набрану кількість балів як підсумкову оцінку і не складати екзамен.

З тими ЗВО, які до проведення підсумкового семестрового контролю не встигли виконати всі обов'язкові види робіт та мають підсумкову оцінку від 0 до 19 балів (за шкалою оцінювання), проводяться додаткові індивідуальні заняття, за результатами яких визначається, наскільки глибоко засвоєний матеріал, та чи необхідне повторне вивчення дисципліни. У випадку якщо студент не має необхідних знань, він не допускається до складання екзамену під час семестрового контролю, але має право ліквідувати академічну заборгованість у порядку, передбаченому «Положенням про поточне та підсумкове оцінювання знань студентів НУ «Чернігівська політехніка».

Для складання екзамену існують білети. Якщо відповідь повна і зміст відповіді студента повністю відповідає сутності поставленого запитання, він може отримати від 33 до 40 балів. В тому випадку, коли студент виконує всі завдання без грубих помилок, він може отримати від 24 до 32 балів. Якщо при відповіді на питання білету студент допускає грубі помилки і всі завдання виконані менш ніж на половину, то він може отримати від 17 до 24 балів. При невиконанні хоча б одного завдання білету, студент не може отримати більше 16 балів.

Повторне складання екзамену з метою підвищення позитивної оцінки не дозволяється.

Дисципліну можна вважати такою, що засвоєна, якщо студент:

– розуміє основні поняття тестування на проникнення та етичного хакінгу;
– знає основні типи атак (SQL-ін'єкції, XSS, DoS, MITM тощо), але без детального розуміння їхнього механізму;
– орієнтується в загальних принципах функціонування мереж і основних мережевих протоколів (TCP/IP, HTTP, DNS);

– має уявлення про основні методології тестування на проникнення (PTES, NIST, OWASP) без глибокого розуміння процесу;

– знає правові та етичні аспекти тестування на проникнення, але без впевненого застосування на практиці;

– вміє запускати базові команди у Linux та Windows для аналізу мережевого трафіку (наприклад, ping, tracert, netstat);

– виконує базове сканування мережі за допомогою Nmap, але без детального аналізу результатів;

– використовує прості інструменти для тестування веб-вразливостей, наприклад Burp Suite або Nikto, але без налаштування складних параметрів;

– вміє знайти та інтерпретувати базову інформацію про вразливості за допомогою OWASP Top 10;

– може виконувати прості атаки на контрольованих навчальних стендах (наприклад, отримати хеш пароля за допомогою John the Ripper або провести просте перехоплення трафіку у Wireshark);

– вміє написати короткий звіт про знайдені вразливості з мінімальним аналізом ризиків.

В цьому випадку студент може отримати підсумкову оцінку «задовільно» – 60 балів – E (в т.ч. й під час ліквідації академічної заборгованості з дисципліни).

Засобами оцінювання та методами демонстрування результатів навчання з дисципліни є поточний та семестровий контроль. Поточний контроль складається з опитувань, які проводяться під час лекцій та захисту практичних робіт. Запитання для поточного контролю знаходяться у відповідних методичних рекомендаціях. Семестровий контроль проводиться у вигляді екзамену, запитання до якого на початку семестру розміщується у системі дистанційного навчання. Екзаменаційні білети знаходяться в пакеті документації на дисципліну.

Оцінювання знань ЗВО здійснюється відповідно до «Положення про поточне та підсумкове оцінювання знань здобувачів вищої освіти Національного університету «Чернігівська політехніка»», затвердженого Вченою радою Національного університету «Чернігівська політехніка» 31 серпня 2020 р. протокол № 6 та введено в дію наказом ректора від 31 серпня 2020 р. № 26.

Для визначення рівня засвоєння студентами навчального матеріалу використовуються такі методи оцінювання знань:

– поточний контроль на практичних заняттях (усне та письмове опитування, тестування, оцінка правильності та своєчасності виконання практичних робіт);

– оцінка за різні види самостійної роботи (наукові дослідження, реферати, домашні контрольні роботи, презентації);

– проміжний модульний контроль;

– підсумковий контроль (2-й семестр – екзамен).

Поточний контроль проводиться шляхом спілкування із студентами під час практичних занять та під час оцінювання виконання самостійної роботи. Бали, які набрані студентом під час поточного контролю, додаються до модульних оцінок.

Підсумковий контроль включає модульний та семестровий контроль. Модульний контроль проводиться у вигляді письмової відповіді на теоретичне запитання та вирішення практичної задачі.

Семестровий контроль за результатами вивчення дисципліни проводиться в останній атестаційний тиждень семестру (сесію) шляхом зваженого додавання результатів модульного контролю та постановки підсумкової оцінки до екзаменаційної відомості.

Для діагностики знань використовується модульно-рейтингова система зі 100-бальною шкалою оцінювання.

Розподіл балів, які отримують здобувачі вищої освіти

Модуль за тематичним планом дисципліни та форма контролю		Кількість балів
Змістовий модуль 1.		0…30
1	Оцінка виконання практичних робіт (підготовленість, самостійність, своєчасність).	0…20
2	Самостійна робота.	0…5
3	Модульний контроль.	0…5
Змістовий модуль 2.		0…30
1	Оцінка виконання практичних робіт (підготовленість, самостійність, своєчасність).	0…20
2	Самостійна робота.	0…5
3	Модульний контроль.	0…5
Усього поточний і проміжний модульний контроль		**0…60**
Семестровий контроль (Екзамен)		**0…40**
Разом		**0…100**

Шкала оцінювання результатів навчання

Оцінка в балах	**Оцінка ECTS**	**Оцінка за національною шкалою (диференційований залік)**	
		для екзамену (диференційованого заліку), курсового проєкту (роботи), практики, атестації	для заліку
90 – 100	**A** (*відмінно*)	відмінно	зараховано
82-89	**B** (*дуже добре*)	добре	
75-81	**C** (*добре*)		
66-74	**D** (*задовільно*)	задовільно	
60-65	**E** (*достатньо*)		
0-59	**FX** (*незадовільно*)	незадовільно з можливістю повторного складання	незараховано з можливістю повторного складання

9. Обладнання та програмне забезпечення

При вивченні даного курсу використовується типове та специфічне обладнання та програмне забезпечення, а саме:

– системний блок Intel Core i3 8100/ RAM 8 GB/ SSD 120 Gb/ HDD 1 Tb з монітором LG 22MP58VQ – 12 компл.;
– сервер Intel Core i5-650 3.2 HGz/ 4096 Mb * 2/ IP55/ 1000 Gb *2/ 8400 GS/ 500W;
– джерело безперебійного живлення APC Smart-UPS C1000;
– мікрокомп’ютер Raspberry Pi 4 Model 4 Gb – 3 компл.;
– адаптер Wi-Fi ALFA AWUS 036AC – 2 од.;
– маршрутизатор Mikrotik RB3011UiAS-RM;
– бездротовий маршрутизатор Mikrotik hAP ac lite tower (RB952Ui-5ac2nD);

- комутатор Cisco catalyst 2960-S;
- SDR-радіо HackRF One PortaPack H2;
- ПЗ Windows 11 Pro Ukrainian DVD, 12 ліцензій;
- ПЗ Microsoft Office Home and Student 2021 ESD, 12 ліцензій;
- ПЗ ОС Ubuntu Server 24.04.2 LTS, ліцензія GNU;
- ПЗ ОС Kali-Linux 2024.4-Kernel 6.11.0, Xfce 4.18.6, ліцензія GNU;
- ПЗ VirtualBox v. 7.1.6, ліцензія GNU.

10. Політики курсу.

До загальної політики курсу відноситься дотримання принципів відвідування занять у відповідності до затвердженого розкладу, а також вільного відвідування лекційних занять для осіб, які отримали на це дозвіл відповідно до «Порядку надання дозволу на вільне відвідування занять здобувачам вищої освіти НУ «Чернігівська політехніка»». Запорукою успішного вивчення дисципліни є активність та залучення під час проведення практичних та лекційних занять – відповіді на запитання викладача (як один з елементів поточного контролю), задавання питань для уточнення незрозумілих моментів, вирішення практичних завдань. Консультації відбуваються в аудиторіях університету у відповідності до затвердженого розкладу або ж особистих чи групових консультацій на платформі Microsoft Teams та (через вбудований форум) на сторінці курсу в системі дистанційного навчання НУ «Чернігівська політехніка».

Політика дедлайнів

Своєчасність здачі практичної роботи оцінюється в 1 бал за кожну практичну роботу. Відповідно, максимальна оцінка за невчасно здані роботи зменшується на зазначену кількість балів. Виключенням може бути наявність поважних причин несвоєчасної здачі зазначених робіт (хвороба, участь в зазначений час в інших видах навчальної, наукової чи організаційної роботи, офіційна робота за фахом тощо).

Політика користування ноутбуками / смартфонами

Прохання до здобувачів тримати смартфони переведеними у беззвучний режим протягом лекційних та практичних занять, так як дзвінки, переписки та спілкування у соціальних мережах відволікають від проведення занять як викладача, так й інших здобувачів. Ноутбуки, планшети та смартфони не можуть використовуватися в аудиторіях під час занять та під час проведення підсумкового контролю (за виключенням проходження тестового контролю в системі Moodle).

Політика заохочень та стягнень

За результатами навчальної, наукової або організаційної діяльності здобувачів вищої освіти за курсом їм можуть нараховуватися додаткові бали – до 10 балів, у залежності від вагомості досягнень. Види позанавчальної діяльності, за якими здобувачі вищої освіти заохочуються додатковою кількістю балів: участь у міжнародних проектах, наукові дослідження, тези, участь у науково-практичних конференціях, винаходи, патенти, авторські свідоцтва за напрямами курсу.

Політика академічної доброчесності

Академічна доброчесність повинна бути забезпечена під час проходження даного курсу (принципи описані у Кодексі академічної доброчесності НУ «Чернігівська політехніка»). Списування під час проміжного та підсумкового контролів, виконання практичних завдань на замовлення, підказки вважаються проявами академічної недоброчесності. Від усіх слухачів курсу очікується дотримання академічної доброчесності у зазначених вище моментах. До здобувачів вищої освіти, у яких було виявлено порушення академічної доброчесності, застосовуються різноманітні дисциплінарні заходи (включаючи повторне проходження певних етапів).

Правила перезарахування кредитів

Кредити, отримані в інших закладах вищої освіти, а також результати навчання у неформальній та/або інформальній освіті, можуть бути перезараховані викладачем у відповідності до положення «Порядок визначення академічної різниці та перезарахування навчальних дисциплін у НУ «Чернігівська політехніка»». Визнання результатів навчання у неформальній освіті розповсюджується на окремі змістові модулі (теми) навчальної дисципліни.

11. Рекомендована література та інформаційні джерела

1. Вейдман, Д. Тестування на проникнення: Практичний вступ до хакінгу / Д. Вейдман. – Київ: Діалектика, 2021. – 528 с.
2. Кім, П. Довідник хакера. Практичний посібник з тестування на проникнення / П. Кім. – 3-тє вид. – Нью-Йорк: Secure Planet, 2020. – 357 с.
3. Ості, Д. Тестування на проникнення з Metasploit: Практичний посібник / Д. Ості. – Лондон: Packt Publishing, 2021. – 396 с.
4. Де-Бебоа, Ф. Етичний хакінг: Керівництво з тестування на проникнення / Ф. Де-Бебоа. – 2-ге вид. – Амстердам: Elsevier, 2022. – 412 с.
5. Мейр, С. Практичне тестування безпеки мереж: Виявлення та усунення вразливостей / С. Мейр. – Бостон: O'Reilly Media, 2023. – 480 с.
6. OWASP Testing Guide v4 / Open Web Application Security Project. – 2020. – 250 с.
7. NIST 800-115: Technical Guide to Information Security Testing and Assessment / National Institute of Standards and Technology. – Вашингтон: NIST, 2021. – 164 с.
8. OSSTMM 3.0: Open Source Security Testing Methodology Manual / ISECOM. – Барселона: ISECOM Press, 2020. – 210 с.
9. PTES: Penetration Testing Execution Standard / PTES Organization. – Нью-Йорк: PTES, 2021. – 135 с.
10. OWASP Foundation. OWASP Testing Guide v4 [Електронний ресурс]. – Режим доступу: https://owasp.org/www-project-web-security-testing-guide/. – Дата звернення: 31.03.2024.
11. The Nmap Security Scanner Project. Офіційна документація Nmap [Електронний ресурс]. – Режим доступу: https://nmap.org/book/. – Дата звернення: 31.03.2024.
12. Metasploit Documentation. Використання Metasploit Framework [Електронний ресурс]. – Режим доступу: https://docs.metasploit.com/. – Дата звернення: 31.03.2024.
13. Kali Linux Documentation. Інструменти та методи тестування на проникнення [Електронний ресурс]. – Режим доступу: https://www.kali.org/docs/. – Дата звернення: 31.03.2024.
14. NIST. Technical Guide to Information Security Testing and Assessment [Електронний ресурс]. – Режим доступу: https://csrc.nist.gov/publications/detail/sp/800-115/final. – Дата звернення: 31.03.2024.