# Силабус освітнього компонента

Програма навчальної дисципліни

# Етичний хакінг

**Шифр та назва спеціальності**
К4 – Управління інформаційною безпекою

**Інститут**
ННІ комп`ютерних наук та інформаційних технологій

**Спеціалізація**

**Кафедра**
Кібербезпеки (328)

**Освітня програма**
Управління інформаційною безпекою

**Тип дисципліни**
Вибіркова

**Рівень освіти**
Перший (бакалаврський)

**Форма навчання**
Денна

**Семестр**
4

**Мова викладання**
Українська

## Викладачі, розробники

**ЄВСЕЄВ Сергій Петрович**

serhii.yevseiev@khpi.edu.ua
Доктор технічних наук, професор, завідувач кафедри кібербезпеки НТУ «ХПІ».

Лауреат національної премії імені Бориса Патона.
Кількість наукових публікацій: понад 351, з них патентів на корисну модель 44, 11 монографій, з яких 10 колективних монографій, 31 навчальний посібник, з яких 4 з грифом Міністерства освіти і науки України, 149 статтей у закордонних виданнях та фахових виданнях України, з них 61 у наукометричній базі Scopus, гарант освітньо-професійної програми "Кібербезпека" першого (бакалаврського) рівня вищої освіти.

Детальніше про викладача на сайті кафедри

## Загальна інформація

### Анотація

Навчальна дисципліна "Етичний хакінг" є вибірковою навчальною дисципліною. Вивчення дисципліни забезпечує особистісний і професійний розвиток студента та спрямована на формування ефективного дослідника, здатного до використання сучасних методів дослідження кіберпростору та передачі знань. В курсі розглядається методологія тестування на проникнення та її етапи. Окремо приділена увага створенню звітів на проникнення, як одному із важливих етапів при здійсненні оцінки захищеності інформаційної системи.

## Мета та цілі дисципліни

Підготовка фахівців, в області інформаційної безпеки, а також фахівців з етичного хакінгу, на базі освоєння принципів та методів збору цифрової інформації для дослідження вразливостей операційних систем Linux та Windows, проведення статичного аналізу вразливостей інформаційних систем, використовуючи інструменти та методи етичного хакінгу.

## Формат занять

Лекції, лабораторні заняття, самостійна робота, консультації. Підсумковий контроль – іспит.

## Компетентності

ЗК6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
ЗК 7. Здатність використовувати інформаційні та комунікаційні технології та формувати систему інформаційно-аналітичного забезпечення підтримки прийняття управлінських рішень щодо системи управління інформаційною безпекою.
СК2. Здатність аналізувати та визначати політику та стратегії забезпечення захисту інформації.
СК3. Проектувати системи управління та захисту інформації на підприємстві установі, організації.
СК5. Здатність узагальнення вітчизняного та закордонного досвіду з питань управління інформаційною безпекою.
СК7. Здатність організовувати та проводити аналіз оточення організації установ з метою виявлення та закриття можливих каналів витоку інформації.
СК8. Здатність використовувати механізми забезпечення управління інформаційною безпекою у її визначальних сферах.
СК9. Здатність організації реагування на загрози на об'єктах критичної інфраструктури, установах та підприємствах.
СК10. Здатність забезпечувати неперервність бізнесу згідно з встановленою політикою інформаційної безпеки.
СК11. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації.

## Результати навчання

РН-3. Вміти за допомогою абстрактного мислення, аналізу та синтезу оцінювати результати професійної діяльності та забезпечувати її якість, бути критичним і самокритичним, наполегливим щодо поставлених завдань і взятих зобов'язань.
РН-6. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної безпеки.
РН-7. Вміти розробляти комплекс організаційних заходів щодо формування системи управління інформаційною безпекою.
РН-8. Вміти використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій щодо формування системи управління інформаційної безпеки.
РН-10. Вміти аналізувати виклики та загрози інформаційної безпеки об'єктів критичної інфраструктури та синтезувати інформацію щодо розроблення та реалізації стратегій та політики безпеки.
РН-11. Вміти забезпечувати процеси захисту та функціонування системи управління інформаційною безпекою та захисту інформації на основі практик, навичок та знань, щодо інфраструктури кіберфізичних систем та інформаційних потоків.
РН-12. Вміти використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.
РН-13. Вміти вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління інформаційної безпеки згідно встановленої політики безпеки в інформаційно-комунікаційних системах.
РН-14. Вміти вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів та користувачів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.

РН-16. Вміти реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційно-комунікаційних системах.
РН-17. Вміти розв'язувати задачі управління інфораційною безпекою в інформаційно-комунікаційних системах на основі моделей управління безпекою.
ПРН-18. Розуміти основні теоретичні поняття, застосовувати набуті практичні навички дослідження та підготовки документів, їх правильного використання в управлінській діяльності.
РН-19. Вміти впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформації в інформаційно-мунікаційних системах.
РН-20. Вміти аналізувати та проводити оцінку ефективності та рівня захищеності інформаційних ресурсів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.
РН-21. Вміти застосовувати теорії та методи захисту для забезпечення безпеки елементів об'єктів критичної інфраструктури, кіберфізичних систем та інформаційно-комунікаційних систем.
РН-22. Вміти застосовувати національні та міжнародні регулятори в сфері інформаційної безпеки щодо розслідування комп'ютерних інцидентів.

### Обсяг дисципліни

Загальний обсяг дисципліни 90 год. (3 кредити ECTS): лекції – 16 год., лабораторні роботи – 16 год., самостійна робота – 58 год.

### Передумови вивчення дисципліни (пререквізити)

Інформаційна безпека держави, Математичні основи криптології, Основи криптографічного захисту, Основи програмування.

### Особливості дисципліни, методи та технології навчання

В ході викладання дисципліни викладачем застосовуються пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний методи навчання. В якості методів викладання, які направлені на активізацію та стимулювання навчально-пізнавальної діяльності здобувачів, застосовуються презентації, бесіди, індивідуальні групові проєкти, майстер-класи.

## Програма навчальної дисципліни

### Навчальні заняття

#### Лекції

| Теми лекцій | Кількість годин |
|---|---|
| **Тема 1. Вступ в навчальну дисципліну.**<br>Цілі та завдання навчальної дисципліни «Тестування на проникнення та етичний хакінг». Місце дисципліни у навчальному процесі підготовки спеціаліста з кібербезпеки. Структура, зміст тематичного плану вивчення дисципліни; навчально-методична література. Особливості вивчення дисципліни; форми контролю знань, умінь та навичок учнів. Напрями науково-дослідної роботи студентів. | 2 |
| **Тема 2. Методології оцінки вразливості. Огляд інструментів етичного злому.**<br>Основні умови. Злом та етичний злом. Що роблять справжні хакери. Методологія тестування на проникнення: OSTMM, ISSAF та ін. Управління проектами з тестування на проникнення. Огляд хакерських інструментів. Застосовні закони. Робота з третіми особами. Питання соціальної інженерії. Логування. Складання звітів. Етичне робоче місце хакера: Kali Linux. Цілі: Metasploitable 2 і т.д. Сканери портів. Сканери вразливостей. Експлуатаційні рамки. | 2 |

| | |
|---|---|
| **Тема 3. Структуровані підходи до збирання інформації. Збір технічної інформації. Аналіз уразливостей.**<br>Методи розвідки із відкритим вихідним кодом. Огляд методів структурованого аналізу. Типи інформації, що збирається: ділова інформація (фінансова, клієнти, постачальники, партнери). Інформація про IT-інфраструктуру. Виявлення джерел інформації. Виявлення IP-адресів. Трасування. Використання Мальтего. Перенесення зони DNS. DNS Брутфорс. Типи вразливостей. Ручний пошук уразливостей. Автоматичний пошук уразливостей. Інструменти аналізу уразливостей. | 2 |
| **Тема 4. Базова експлуатація Фреймворк Метасплот. Парольні атаки.**<br>Що таке експлойт. Використовувати бази даних Google для тестерів на проникнення: www.exploit-db.com. Локальна та віддалена експлуатація. Огляд платформи Metasploit. Типи корисного навантаження. Атаки «людина посередині». Атаки на паролі: онлайн та офлайн. Хеші паролів. Мистецтво ручного підбору пароля. Пройти хеш атаку. | 2 |
| **Тема 5. Експлуатація веб-застосунків. Експлуатація з використанням атак клієнтів.**<br>Типова структура Web-програми. Поширені веб-уразливості. Проекти OWASP. Огляд посібника з тестування OWASP. лом Google. Злом бази даних Google (GHDB). Інструменти тестування веб-безпеки. еб-сканери. Локальні проксі. Фазери. Спеціалізовані браузери та плагіни для браузерів. Експлойти на стороні клієнта. Огляд проекту інфраструктури експлуатації браузера. | 2 |
| **Тема 6. Підтримка доступу.**<br>Підтримка техніки доступу. Використання інтерпретатора. | 2 |
| **Тема 7. Тестування на проникнення бездротових мереж. Стрес-тести мережі.**<br>Стрес-тест мережі (DoS веб-сайту) з SlowHTTPTest в Kali Linux: slowloris, slow body і slow read атаки в одному інструменті. Стрес-тест мережі: DoS веб-сайту в Kali Linux з GoldenEye. Стрес-тест мережі з Low Orbit Ion Cannon (LOIC). Стрес-тест мережі: DoS з використанням hping3 і Спуфінга IP в Kali Linux. | 2 |
| **Тема 8. Злом та захист акаунтів у соціальних мережах. Складання звіту і представлення результатів тестування на вторгнення.**<br>Цілі та виконавці злому акаунтів. Збір інформації. Методи злому. Зламування електронної пошти. Соціальний інжиніринг. Перебір пароля. Фішинг або фейкова сторінка. Клавіатурний шпигун. Підміна DNS. Важливість оформлення звіту щодо результатів тестування на вторгнення. Узагальнений шаблон звіту про вторгнення. Види звітів та методика їх складання. Спеціаліст з етичного хакінгу як свідок. Порівняння ролей експертів і технічних спеціалістів. | 2 |
| **Загальна кількість годин** | **16** |

## Лабораторні заняття

| Теми лабораторних занять | Кількість годин | Вагові коефіцієнти *a* |
|---|---|---|
| **Тема 1. Базова конфігурація Kali Linux та Metasploitable 2.**<br>Встановлення та налаштування Kali Linux (виртуальна машина — VirtualBox/VMware): налаштування мережевого інтерфейсу (NAT/Bridged), оновлення системи, встановлення необхідних пакетів. Розгортання Metasploitable 2 у віртуальному середовищі, налаштування мережі для взаємодії з Kali. Налаштування безпечного робочого середовища: зберігання результатів, | 2 | 1 |

| | | |
|---|---|---|
| ізольовані лабораторні мережі (host-only). Перевірка зв'язку: ping, nmap базове сканування, визначення IP-адрес. Практичне завдання: підготувати шаблон звіту про лабораторію (перелік налаштованих машин, IP, скріншоти конфігурацій). | | |
| **Тема 2. Використання Google для OSINT у проектах тестування на проникнення. Технічна розвідка IT-інфраструктури. Використання Maltego для розвідки.**<br>Основи Google Dorking: формування запитів для пошуку відкритої інформації (файли, конфігурації, адмін-інтерфейси). Збір бізнес-інформації: пошук контактів, доменів, піддоменів, публічних документів. Технічна розвідка: визначення підмереж, відкритих портів, сервісів через публічні джерела. Вступ до Maltego: побудова графів, підключення трансформацій (transforms), збір зв'язків між об'єктами (домен→IP→WHOIS→утримувачі). Практичне завдання: провести OSINT-розвідку заданого домену (без порушень) і подати карту зв'язків у вигляді скріну/експорту Maltego. | 2 | 1 |
| **Тема 3. Аналіз вразливостей. Сканування портів. Ручна оцінка вразливості. Використання сканерів уразливостей. Огляд конфігурації. Спеціальні інструменти сканування.**<br>Портсканування: nmap (опції -sS, -sV, -O, --script), інтерпретація результатів. Ручний аналіз відкритих сервісів: banner grabbing, перевірка версій, вивчення конфігурацій сервісів. Автоматичні сканери вразливостей: Nessus/OpenVAS/Qualys (основні налаштування, політики сканування). Робота зі звітами сканерів: фільтрація шуму, класифікація ризиків, False Positive / False Negative. Додаткові інструменти: masscan (швидке сканування), Nikto (веб-сканер), dirb/feroxbuster (директорії). Практичне завдання: виконати комплексне сканування цілі, скласти короткий список пріоритетних вразливостей і описати кроки верифікації (ручна перевірка). | 2 | 1 |
| **Тема 4. Експлуатація. Атака з використанням ARP-спуфінгу. Командний рядок Metasploit. Armitage. Атаки на паролі баз даних та різних сервісів.**<br>ARP-spoofing / ARP-poisoning: принцип дії, інструменти (ettercap, arpspoof), налаштування IP forwarding, перехоплення трафіку (tcpdump, Wireshark). Metasploit CLI: пошук експлойтів, вибір модулів exploit/payload/auxiliary, налаштування опцій, запуск сеансів. Armitage: графічна робота з Metasploit, сценарії автоматизації атак. Атаки на паролі: brute-force/wordlist атаки (hydra, medusa), атаки на бази даних (MySQL, MSSQL) та служби (SSH, FTP). Захист та етичні вимоги: як документувати докази, як уникати шкоди під час лабораторії. Практичне завдання: провести ARP-spoofing у ізольованій лабораторній мережі, перехопити простий незашифрований трафік; виконати експлуатацію Metasploit проти вразливої служби Metasploitable2 (у межах стенду). | 2 | 1 |
| **Тема 5. Експлуатація веб-застосунків. Сканування веб-застосунків. Брутфорс паролів веб-програми. Виконання команд ОС через веб-сервер.**<br>Виявлення веб-стеків: Wappalyzer, builtwith, заголовки сервера. Сканування веб-застосунків: Burp Suite (Crawler, Scanner), OWASP | 2 | 1 |

| | | |
|---|---|---|
| ZAP. Атаки на аутентифікацію: brute-force, credential stuffing, обходи контролю сесій. Команди ОС через веб-сервер: remote command execution (RCE) вразливості, upload backdoor, reverse shell (опис та безпечна демонстрація у стенді). Практичне завдання: знайти в тестовому веб-додатку незначну вразливість (напр., форма без валідації), відтворити експлуатацію й описати ризики. | | |
| **Тема 6. Експлуатація веб-застосунків. SQL-ін'єкція та офлайн-злом пароля. Експлуатація XSS-вразливості.** SQLi: типи (in-band, blind, time-based), інструменти (sqlmap), ручні методи виявлення та експлуатації. Захоплення даних аутентифікації, вилучення хешів паролів з БД; офлайн-криптоаналіз (hashcat, john) — робота з wordlists. XSS: reflected/stored/DOM, інструменти тестування, payload-и для демонстрації (безпеки стенду). Практичне завдання: відтворити просту SQLi у контрольованому середовищі, отримати хеші й проілюструвати їх офлайн-криптоаналіз (коротка демонстрація на слабкому хеші); знайти і продемонструвати XSS-пейлоад у тестовому додатку. | 2 | 1 |
| **Тема 7. Експлуатація з використанням атак клієнтів. Експлуатація клієнта з BeEF.** Огляд BeEF (Browser Exploitation Framework): архітектура, hook-скрипти, типові модулі. Створення фішингової/використовуваної сторінки у контрольованому середовищі для hook-у клієнта. Модулі BeEF для збору інформації, remote command execution, social engineering hooks. Практичні правила безпечного використання (тільки у стенді, інформування тестових користувачів). Практичне завдання: встановити hook на тестовий браузер у локальній мережі, виконати декілька інформаційних модулів та задокументувати результати. | 2 | 1 |
| **Тема 8. Підтримка доступу. Встановлення та використання руткітів.** Концепція «пост-експлуатації» і підтримка доступу (persistence techniques). Інструменти для створення бекдорів / руткітів у контрольованому середовищі (методи, не шкідливий код — демонстрація у вузькому стенді). Захист від persistence: моніторинг автозапусків, інтеграція AV/EDR, перевірка цілісності системних файлів. Практичне завдання: реалізувати простий механізм збереження сесії (reverse shell persistence) у тестовій VM та показати методи її виявлення й видалення. | 2 | 1 |
| **Загальна кількість годин** | **16** | $\sum_{i=1}^{n} a_i = 8$ |

## Контрольні роботи

| Теми контрольних робіт | Вагові коефіцієнти $b$ |
|---|---|
| **Тема 1. Методології тестування на проникнення та правові / етичні аспекти.** Пояснити відмінність між «зломом» і «етичним зломом»; ролі та обов'язки етичного хакера. Описати методології тестування на проникнення: OSTMM, ISSAF (основні етапи та відмінності). Управління проєктом тестування на проникнення: планування, обсяг робіт, взаємодія з третіми сторонами, | 0,5 |

| | |
|---|---|
| узгодження правил залучення (Rules of Engagement). Законодавчі та етичні питання при проведенні пентесту (що дозволено/що заборонено). Практичне завдання: підготувати план (структуру) контракту/угоди про проведення пентесту для вигаданого замовника (вказати обсяг, часові рамки, ROE, критерії успіху). | |
| **Тема 2. Розвідка, сканування та аналіз вразливостей — інструменти та практичні підходи.** Методи збору інформації: OSINT, структурований збір (цільова бізнес-інформація, інфраструктура, DNS, IP). Інструменти та техніки: Maltego, DNS enumeration, трасування, портсканери, сканери вразливостей. Ручний vs автоматичний пошук вразливостей; класифікація типових вразливостей. Логування, збирання доказів і ведення робочої документації під час розвідки. Практичне завдання: виконати (у навчальному середовищі) розвідку заданої цільової підмережі — зібрати список відкритих сервісів, виявлених вразливостей та запропонувати пріоритезацію ризиків (звіт — 1 сторінка). | 0,5 |
| **Тема 3. Експлуатація вразливостей, атаки на веб-застосунки та підготовка звітів.** Основи експлуатації: поняття експлойта, типи payload'ів, локальна і віддалена експлуатація. Метасплоіт (Metasploit): структура, робочий цикл експлуатації, типи навантажень. Вразливості веб-застосунків: OWASP Top 10, інструменти тестування веб-безпеки, проксі, GHDB. Парольні атаки (онлайн/офлайн), хеші паролів, підбір/радужні таблиці, практики захисту. Підтримка доступу, атаки на клієнта (XSS, drive-by), атаки на бездротові мережі і DoS-інструменти (коротко). Формування звіту про пентест: шаблон, пріоритетність знахідок, рекомендації для усунення, юридичні аспекти представлення результатів. Практичне завдання: провести експлуатацію (в навчальному стенді) однієї знайденої вразливості веб-застосунку, зафіксувати доказ (скрін/лог), підготувати короткий звіт з описом вразливості, ризиком і рекомендаціями. | 1 |
| **Загалом** | $\sum_{i=1}^{m} b_i$=2 |

## Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

### Опрацювання теоретичного матеріал

| Теми для самостійного вивчення | Кількість годин |
|---|---|
| **Тема 1. Реверс-інжиніринг і розбір шкідливого ПЗ.** Статичний і динамічний аналіз; інструменти (Ghidra, IDA, x64dbg); практично: розібрати простий malware-sample у ізольованому стенді. | 6 |
| **Тема 2. Цифрова судова експертиза (Forensics).** Збір і збереження доказів, аналіз образів дисків і пам'яті; практично: відновити файл із образу диска, проаналізувати дамп пам'яті. | 6 |
| **Тема 3. Аналіз мережевого трафіку та розробка правил IDS/IPS.** Wireshark, Zeek, Snort/Suricata; практично: написати правило для виявлення простого експлойта. | 6 |
| **Тема 4. Безпека хмарних сервісів (Cloud Security).** Моделі загроз у хмарі, IAM, захист S3/Blob, конфігурації; практично: знайти misconfig у тестовому S3-бакеті (стенд). | 6 |
| **Тема 5. Безпека контейнерів і Kubernetes.** | 6 |

| | |
|---|---|
| Атаки на контейнерні середовища, налаштування RBAC, подолання ізоляції; практично: виявити привілеї в кластері Minikube. | |
| **Тема 6. Мобільна безпека (Android/iOS).** Аналіз APK/IPA, перевірка аутентифікації, вразливості мобільних API; практично: статичний аналіз APK і пошук небезпечних дозволів. | 6 |
| **Тема 7. Threat Intelligence і OSINT-автоматизація.** Збір, нормалізація та кореляція загроз; практично: налаштувати простий потік даних TI (фіди, MISP). | 6 |
| **Тема 8. Secure Coding та перегляд коду на вразливості.** OWASP Secure Coding, пошук уразливостей у коді (SAST); практично: проаналізувати репозиторій на SQLi/XSS-помилки. | 6 |
| **Тема 9. Криптоаналіз практичних схем.** Вразливості застосування криптографії, атаки на реалізації, побічні канали; практично: зламати просту реалізацію повторного використання IV. | 5 |
| **Тема 10. Blue Team: моніторинг, реагування та відновлення.** Побудова лог-пайплайнів, SOAR, практики IR; практично: підготувати playbook для реагування на Ransomware-інцидент. | 5 |
| **Загальна кількість годин** | **58** |

## Неформальна освіта

Здобувач має можливість перезарахувати окремі теми або курс шляхом: проходження професійних курсів чи тренінгів, онлайн-освіти, професійних стажувань, у сфері, що відповідає навчальним цілям дисципліни.
Для зарахування необхідно надати: сертифікат (електронний або друкований) про проходження курсу/стажування, опис програми тренінгу із зазначенням змісту тем, обсягу та тривалості.

### Рекомендовані курси, тренінги, стажування

1. Онлайн-курс CISCO «Ethical Hacker»
https://www.netacad.com/catalogs/learn?category=course

## Література, навчальні матеріали та інформаційні ресурси

### Основна література

1. Oriyano Sean-Philip. Penetration Testing Essentials. Sybex, a Wiley brand, 2017, 363 p. 2. Baloch Rafay. Ethical hacking and penetration testing guide. Auerbach Publications, 2017, 523 p.
https://www.tsoungui.fr/ebooks/Ethickal-haking-postexploitation.pdf
2. Євсеєв С.П. Кібербезпека: Лабораторний практикум з основ криптографічного захисту. – Львів “Новий світ-2000”, 2020. – 241 с.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
3. Бобало Ю.Я., Горбатий І.В. (ред.) Інформаційна безпека. Навчальний посібник. — Львів : Видавництво Львівської політехніки, 2019. — 580 с. — ISBN 978-966-941-339-0.
https://pdf.lib.vntu.edu.ua/books/2021/Bobalo_2019_580.pdf
4. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
5. Models of socio-cyber-physical systems security: monograph / S. Yevseiev, O. Milov, Yu. Khokhlachova, S. Ostapov, O. Laptiev and others. – Kharkiv: PC TECHNOLOGY CENTER, 2023. – 168 p.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
6. Modeling of security systems for critical infrastructure facilities: monograph / S. Yevseiev, R. Hryshchuk, O. Milov, K. Molodetska, M. Nazarkevych and others. – Kharkiv: PC TECHNOLOGY CENTER, 2022. – 196 p.

https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju.
7. Етичний хакінг : навчально-практичний посібник / уклад. О. В. Мілов, О. В. Шматко, С. В. Мілевський, О. Г. Король ; за заг. ред. С. П. Євсеєва. – Харків : НТУ «ХПІ», – Львів : «Новий Світ-2000», 2025. – 100 с. – (Серія «Кібербезпека та штучний інтелект»).
https://drive.google.com/file/d/1AHYbnhItLvuyRnjZzVqmXskkXZ6KSjRJ/view?usp=sharing

### Додаткова література

7. Технології захисту інформації./ С. Е. Остапов, С. П. Євсєєв, О.Г. Король. – Чернівці : Чернівецький національний університет, 2013. – 471 с.
http://kist.ntu.edu.ua/textPhD/tzi.pdf
8. Security of Linux operating system: laboratory workshop / S. Yevseiev, S. Pogasiy, A. Goloskokova, O. Shmatko, M. Melnik (Кібербезпека: безпека операційної системи Linux: лабораторний практикум: навчальний посібник для студентів вищих навчальних закладів англійською мовою / Євсеєв С.П., Погасій С.С., Голоскокова А.О., Шматко О.В., Мельник М.О. – Львів: Видавництво «Новий Світ – 2000», 2021. – 256 с.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
9. Євсєєв С.П. Кібербезпека: основи кодування та криптографії/ С.П. Євсеєв, О.В. Мілов, С.Е. Остапов, О.В. Сєвєрінов. – Харків: Вид. “Новий Світ-2000”, 2023. – 657 с.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
10. Технологія Ethernet : лабораторний практикум / М. О. Білова, С. П. Євсеєв, О. С. Жученко, І. С. Іванченко, О. В. Шматко.– Львів: «Новий Світ- 2000», 2020 . – 196 с.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
11. Aaron Philipp, David Cowen, Chris Davis. Hacking exposed computer forensics. Second edition. The McGraw-Hill Companies, 2010.
https://needuxnworkplace.wordpress.com/wp-content/uploads/2014/01/hacking-exposed-computer-forensics-secrets-solutions.pdf
12. Wilhelm, Thomas. Professional penetration testing: Creating and learning in a hacking lab. Newnes, 2013, 525 p.
http://ppdi.stmik-banjarbaru.ac.id/data.bc/13.%20Hacking/2013%20Professional%20Penetration%20Testing%20Creating%20and%20Learning%20in%20a%20Hacking%20Lab.pdf

## Система оцінювання

Підсумкова оцінка з освітнього компонента визначається відповідальним лектором за темами, видами занять, тощо у відповідності до силабусу і є інтегральною оцінкою результатів усіх вид навчальної діяльності здобувача вищої освіти. Підсумкова оцінка повинна відображати всі оцінки за складовими навчального процесу з урахуванням їх вагових показників $k$:

| Поточний контроль (практичні, семінарські, лабораторні заняття), $k_1$ | Контрольні роботи (за наявності), $k_2$ | Індивідуальне завдання (за наявності), $k_3$ | Підсумковий контроль (для ОК з іспитом), $k_4$ |
|---|---|---|---|
| 0,4 | 0,2 | | 0,4 |

Сума коефіцієнтів повинна складати одиницю: $k_1 + k_2 + k_3 + k_4 = 1$. Підбір вагових коефіцієнтів підсумкової оцінки здійснює розробник курсу.
Розрахунок підсумкової оцінки проводиться за формулою:

$$О = П \cdot k_1 + K \cdot k_2 + І \cdot k_3 + Пк \cdot k_4$$

де: П – середньозважена середня оцінка за поточний контроль
І – оцінка за виконання індивідуального завдання
$K$ – середньозважена оцінка за контрольні роботи
Пк – оцінка за підсумковий контроль

$$П = \frac{П_1 \cdot a_1 + П_2 \cdot a_2 + ... + П_n \cdot a_n}{\sum_{i=1}^{n} a_i}$$

де: $a_i$ - ваговий коефіцієнт за кожне практичне (семінарське) або лабораторне заняття.

$$K = \frac{K_1 \cdot b_1 + K_2 \cdot b_2 + ... + K_m \cdot b_m}{\sum_{i=1}^{m} b_i}$$

де: $b_i$ - ваговий коефіцієнт за кожну контрольну роботу.

Поточні оцінки за кожну складову (П, $K$, І,... ) виставляються за 100-бальною шкалою згідно з положенням «Про критерії та систему оцінювання знань та вмінь і про рейтинг здобувачів вищої освіти» НТУ «ХПІ».

Підсумкова оцінка виставляється відповідно до розрахованої О з округленням до найближчого цілого числа в більшу сторону.

**Шкала оцінювання**

| Сума балів | Національна оцінка | ECTS |
|---|---|---|
| 90–100 | Відмінно | A |
| 82–89 | Добре | B |
| 75–81 | Добре | C |
| 64–74 | Задовільно | D |
| 60–63 | Задовільно | E |
| 35–59 | Незадовільно (потрібне додаткове вивчення) | FX |
| 1–34 | Незадовільно (потрібне повторне вивчення) | F |

## Норми академічної етики і політика курсу

Здобувач вищої освіти повинен дотримуватися «Кодексу етики академічних взаємовідносин та доброчесності НТУ «ХПІ»: виявляти дисциплінованість, вихованість, доброзичливість, чесність, відповідальність. Конфліктні ситуації повинні відкрито обговорюватися в навчальних групах з викладачем, а при неможливості вирішення конфлікту – доводитися до відома співробітників дирекції інституту.
Нормативно-правове забезпечення впровадження принципів академічної доброчесності НТУ «ХПІ» розміщено на сайті: http://blogs.kpi.kharkov.ua/v2/nv/akademichna-dobrochesnist/

## Погодження

| | | | |
|---|---|---|---|
| Силабус погоджено | 30.08.2025 |  | **Завідувач кафедри**<br>Сергій ЄВСЕЄВ |
| | 30.08.2025 |  | **Гарант ОП**<br>Роман КОРОЛЬОВ |