Силабус освітнього компонента

Програма навчальної дисципліни

Етичний хакінг

Шифр та назва спеціальності
F5 – Кібербезпека та захист інформації

Інститут
ННІ комп`ютерних наук та інформаційних технологій

Спеціалізація

Кафедра
Кібербезпеки (328)

Освітня програма
Кібербезпека

Тип дисципліни
Загальна підготовка, Обов'язкова

Рівень освіти
Другий (магістерський)

Форма навчання
Денна, заочна

Семестр
2

Мова викладання
Українська, англійська

Викладачі, розробники

ДУНАЄВ Сергій Владиславович

Serhii.Dunaiev@cs.khpi.edu.ua
Асистент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: 5, з них 3 статті, що реферуються у науково метричних базах Scopus. Лектор з дисциплін: "Веб-програмування" та інших у студентів бакалавріата та магістратури.

Детальніше про викладача на сайті кафедри

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. Провідний лектор з дисциплін: Математичні основи криптології, Комп`ютерні мережі, Основи криптографічного захисту, Методи криптоаналізу, Основи кібербезпеки, Сучасні проблеми

постквантової криптографії, Основи наукових досліджень, Цифрова криміналістика, Етичний хакінг у студентів бакалавріата та магістратури, Методологія наукової та педагогічної діяльності в науках кіберзахисту для аспірантів.

Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Процес тестування на проникнення призначено для 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 тестування на проникнення.

Мета та цілі дисципліни

Підготовка фахівців, в області інформаційної безпеки, безпеки телекомунікаційного забезпечення, і мобільних пристроїв, а також фахівців з тестування на проникнення та 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 тестування на проникнення.

Формат занять

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

Компетентності

КЗ–1. Здатність застосовувати знання у практичних ситуаціях.
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.
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.

Результати навчання

РН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.
РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.
РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.
РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.

РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.
РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.
РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
РН12. 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.
РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.
РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.
РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.
РН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.
РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.
РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.
РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.
РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.
РН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.
РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.

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)

Цифрова криміналістика, Безпека Інтернет речей та сервісів, Безпека систем Клієнт-Сервер.

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 до етичного хакінгу та організація дисципліни. Цілі та завдання курсу, місце дисципліни в підготовці фахівця з кібербезпеки, структура програми, методи контролю знань і напрямки наукової роботи.	2
Тема 2. Методології тестування на проникнення, правові та етичні аспекти. Огляд стандартних методологій (OSTMM, ISSAF, ін.), керування проєктами пентесту, юридичні вимоги, правила роботи з третіми особами, логування й складання звітів; питання соціальної інженерії.	2
Тема 3. Розвідка та збір інформації (OSINT і технічна розвідка). Структуровані підходи до збору інформації, OSINT-методи, збір бізнес- і IT-даних, виявлення IP-адрес, DNS-аналіз, використання інструментів (Maltego, Google dorking).	2
Тема 4. Сканування та аналіз уразливостей. Методи виявлення вразливостей (ручні й автоматизовані), робота зі сканерами портів та вразливостей, класифікація вразливостей, інструменти та інтерпретація результатів.	2
Тема 5. Експлуатація вразливостей і платформа Metasploit. Концепція експлойтів і корисного навантаження, локальна та віддалена експлуатація, огляд Metasploit, робота з базами експлойтів (Exploit-DB), атаки типу "людина посередині".	2
Тема 6. Тестування веб-застосунків і методи захисту (OWASP). Структура веб-додатків, поширені веб-уразливості (XSS, SQLi тощо), методика тестування OWASP, інструменти веб-тестування, проксі та спеціалізовані браузери.	2
Тема 7. Атаки на паролі, клієнтські платформи та бездротові мережі. Онлайн/офлайн атаки на паролі, робота з хешами, експлойти на стороні клієнта, тестування бездротових мереж (WEP/WPA/WPA2/WPA3), методи збереження й підтримки доступу.	2
Тема 8. Стрес-тести, соціальна інженерія та підготовка звіту пентесту. Інструменти стрес-тестування (DoS/DDoS-сценарії в навчальних лабораторіях), методики соціальної інженерії, підтримка доступу, оформлення звітів за результатами тестування та підготовка фахівця як свідка/експерта.	2
Загальна кількість годин	**16**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти a
Тема 1. Базова конфігурація Kali Linux та Metasploitable 2. Розгортання ізольованого лабораторного середовища для навчання (віртуальні машини), налаштування інструментів і політик безпеки; перевірка коректності середовища перед виконанням практик.	2	-
Тема 2. Використання Google для OSINT у проектах тестування на проникнення. Технічна розвідка IT-інфраструктури. Використання Maltego. Практика збору відкритої інформації (OSINT) для формування розвідданих про об'єкт тестування; застосування інструментів для картування інфраструктури й побудови легальних розвідувальних звітів.	2	0,1
Тема 3 Аналіз уразливостей: сканування портів. Ручна оцінка вразливості. Використання сканерів уразливостей. Вивчення принципів сканування мережі та сервісів, порівняння результатів ручного та автоматичного аналізу; інтерпретація звітів сканерів і підготовка рекомендацій із пом'якшення ризиків.	2	0,1
Тема 4. Експлуатація: ARP-спуфінг, Metasploit, Armitage. Атаки на паролі сервісів. Дослідження концепцій експлуатації у контрольованому середовищі з акцентом на розуміння механізмів атак і їх наслідків; вивчення етичних меж тестування й процедур документування виявлених ризиків.	2	0,1
Тема 5. Експлуатація веб-застосунків: сканування, підбір паролів, виконання команд ОС через веб-сервер (демонстраційні кейси). Виявлення та інтерпретація типових веб-артефактів і вразливостей у тестовому середовищі; підготовка рекомендацій для безпечної розробки й налаштування серверів (без шкідливих інструкцій).	2	0,1
Тема 6. Експлуатація веб-застосунків: SQL-ін'єкція, XSS і офлайн-аналіз паролів (на навчальних прикладах). Демонстрація природи поширених веб-уразливостей і методів їх виявлення; акцент на способах захисту, валідації введення та безпечній обробці даних.	2	0,1
Тема 7. Експлуатація з використанням атак клієнтів: використання BeEF (демонстраційні сценарії). Вивчення ризиків, пов'язаних із вразливими клієнтськими додатками та браузерами; аналіз механізмів захисту клієнтської зони й процедур реагування в організації.	2	0,1
Тема 8. Підтримка доступу: принципи та захист (огляд руткітів у навчальному середовищі, етичні аспекти). Розбір технік, що використовуються для утримання несанкціонованого доступу, з акцентом на виявлення, видалення та запобігання; розробка плану реагування й відновлення після	2	0,1

інциденту.		
Загальна кількість годин	**16**	$\sum_{i=1}^{n} a_i = 0{,}8$

Контрольні роботи

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Методологія та етапи тестування на проникнення. Оцінювання знань студентів щодо етапів проведення тестування на проникнення — від збору інформації (OSINT) до виявлення й аналізу вразливостей. Розгляд правових та етичних аспектів діяльності етичного хакера, застосування методологій OSTMM, ISSAF та принципів звітності.	0,1
Тема 2. Практичні аспекти експлуатації та захисту інформаційних систем. Перевірка практичних знань з використання інструментів етичного хакінгу (Kali Linux, Metasploit, OWASP, сканери портів і вразливостей). Аналіз сценаріїв атак на веб-додатки, паролі та бездротові мережі, а також підготовка звіту за результатами пентесту.	0,1
Загалом	$\sum_{i=1}^{m} b_i$=0,2

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

Опрацювання теоретичного матеріалу

Теми для самостійного вивчення	Кількість годин
Тема 1. Реверс-інжиніринг і аналіз бінарних файлів. Принципи розбору виконуваних файлів (статичний і динамічний аналіз), інструменти для реверсу (загальний огляд), застосування при пошуку вразливостей і аналізі шкідливого ПЗ.	10
Тема 2. Мережевий форензик і аналіз трафіку. Методи збору й інтерпретації мережевих логів і PCAP-файлів, ідентифікація індикаторів компрометації, кореляція подій та підготовка артефактів для звітування й розслідування.	8
Тема 3. Безпека хмарних середовищ і тестування хмарних сервісів. Архітектурні моделі IaaS/PaaS/SaaS, типові вектори атак у хмарі, особливості аудиту хмарних конфігурацій і рекомендації для захисту (включаючи IAM і конфігураційні помилки).	8
Тема 4. Апаратна безпека та вбудовані системи (Embedded / IoT). Принципи роботи вбудованих пристроїв, типові вразливості апаратного й прошивочного рівня, методи оцінки ризиків і практики захисту пристроїв Інтернету речей.	8
Тема 5. Red Team / Blue Team практики і моделювання атак. Відмінності ролей Red/Blue, підходи до сценарного тестування, організація навчальних вправ (tabletop, purple team) для підвищення готовності організації.	8
Тема 6. Secure coding і інтеграція безпеки в SDLC. Принципи безпечної розробки (input validation, secure defaults, секрети в коді), інструменти SAST/DAST і процеси інтеграції тестування безпеки в життєвий цикл розробки.	8

Тема 7. Bug bounty, відповідальне розкриття вразливостей та кар'єрні шляхи. Практики етичного розкриття, робота з платформами bug bounty, складання коректного репорту вразливості, етичні та юридичні аспекти, можливі кар'єрні маршрути для пентестера.	8
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.
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

4. 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
5. 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** Сергій ЄВСЕЄВ
	30.08.2025		**Гарант ОП** Ольга КОРОЛЬ