926 66-12/П21

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
СИСТЕМА УПРАВЛІННЯ ЯКІСТЮ
Система забезпечення якості освітньої діяльності та якості вищої освіти
сертифікована на відповідність ДСТУ ISO 9001:2015 / ISO 9001:2015
Кафедра інженерії програмного забезпечення та кібербезпеки

ЗАТВЕРДЖЕНО
вченою радою КНТЕУ
(пост. п. 9 від "23" 12 2021 р.)
Ректор
_____А.А. Мазаракі

ЕТИЧНИЙ ХАКІНГ /
ETHICAL HACKING

ПРОГРАМА/
COURSE SUMMARY

Київ 2021

Автори: В.П. ЗВЕРЕВ, кандидат технічних наук, доцент кафедри інженерії програмного забезпечення та кібербезпеки,
Н.О. КОТЕНКО, кандидат педагогічних наук, доцент кафедри інженерії програмного забезпечення та кібербезпеки,
О.В. КРИВОРУЧКО, доктор технічних наук, завідувач кафедри інженерії програмного забезпечення та кібербезпеки,
В.І. ПАШОРІН, кандидат технічних наук, професор кафедри інженерії програмного забезпечення та кібербезпеки,
В.І. ЧУБАЄВСЬКИЙ кандидат політичних наук, доцент кафедри інженерії програмного забезпечення та кібербезпеки

Програму розглянуто і затверджено на засіданні кафедри інженерії програмного забезпечення та кібербезпеки 15 листопада 2021 р., протокол № 12.

Рецензенти: С.В. ДЕМЕДЮК, канд. юрид. наук, заступник Секретаря Ради національної безпеки і оборони України
Н.В. ЛУКОВА-ЧУЙКО, д.т.н., проф., зав. кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка

ЕТИЧНИЙ ХАКІНГ /
ETHICAL HACKING

ПРОГРАМА /
COURSE SUMMARY

ВСТУП

Дисципліна «Етичний хакінг» є обов'язковою дисципліною навчальних планів підготовки студентів КНТЕУ денної форми навчання освітнього ступеня «магістр» галузі знань 12 «Інформаційні технології» спеціальності 125 «Кібербезпека» спеціалізації «Безпека систем електронних комунікацій в економіці».

Програму підготовлено відповідно до Стандарту вищої освіти України із зазначеної спеціальності та відповідної освітньо-професійної програми підготовки магістрів КНТЕУ.

Програма складається з таких частин:

1. Мета, завдання та предмет дисципліни.
2. Передумови вивчення дисципліни як вибіркової компоненти освітньої програми.
3. Результати вивчення дисципліни.
4. Зміст дисципліни.
5. Список рекомендованих джерел.

1. МЕТА, ЗАВДАННЯ ТА ПРЕДМЕТ ДИСЦИПЛІНИ

Метою викладання навчальної дисципліни «Етичний хакінг» є підвищення професійного рівня студентів у рамках своєї кваліфікації шляхом удосконалення наявних та формування у них нових компетенцій (знань та умінь), необхідних їм для виконання функцій у рамках професійної діяльності із забезпечення кібербезпеки інформаційних систем.

Завдання дисципліни «Етичний хакінг» – придбання теоретичних знань і практичних навичок необхідних професіоналу з захисту інформації у сфері технологій збору інформації про комп'ютерні системи, проведення аудиту і пентестингу інформаційних систем, планування та здійснення атаки на захисні механізми операційних систем і додатків; роботі із засобами виявлення вразливостей та виконання аналізу захищеності інформаційних систем.

Предметом дисципліни «Етичний хакінг» є технології здійснення професійної діяльності з питань безпеки інформаційних систем: методи та інструменти збору інформації про інформаційні системи, аналізу вразливостей інформаційних систем, аудиту захищеності та тестуванню на проникнення в інформаційні системи.

У результаті вивчення навчальної дисципліни студент повинен

знати:

- теоретичні основи і сучасні інформаційні технології етичного хакінгу;
- особливості проведення збору інформації по методиці OSINT;
- основні засоби та методи аналізу вразливостей;
- методику та особливості проведення аналізу захищеності;
- методики проведення тестування на проникнення (Penetration Test);
- принципи роботи інструментів етичного хакінгу ***Kali Linux (PentestBox)***;

- сучасний стан і шляхи розвитку методів та технологій етичного хакінгу;

вміти:

- встановлювати і настроювати програмне забезпечення для етичного хакінгу;
- самостійно виконувати збір та аналіз інформації для етичного хакінгу;
- виконувати пошук та аналіз вразливостей інформаційних систем;
- застосовувати для пентесту ***Kali Linux (PentestBox)***;
- розробляти методи реагування на випадки порушень кібербезпеки;
- застосовувати інструменти тестування для захисту даних і безпеки інформаційних систем.

2. ПЕРЕДУМОВИ ВИВЧЕННЯ ДИСЦИПЛІНИ ЯК ВИБІРКОВОЇ КОМПОНЕНТИ ОСВІТНЬОЇ ПРОГРАМИ

знання:

- технологій безпеки інформаційних систем;
- технологій безпеки мереж і мережевої інфраструктури;
- технології безпеки Web-ресурсів.

вміння: вільно працювати:

- з операційними системами Microsoft Windows і Linux;
- з хмарними сервісами Microsoft Office 365;
- з пошуковими сервісами Інтернет.

3. РЕЗУЛЬТАТИ ВИВЧЕННЯ ДИСЦИПЛІНИ

Дисципліна «Етичний хакінг», як обов'язкова компонента забезпечує оволодіння студентами загальними та фаховими компетентностями і досягнення ними програмних результатів навчання за відповідною освітньо-професійною програмою:

«Безпека систем електронних комунікацій в економіці».
(ОС магістр, ОП 2022р.)

Номер в освітній програмі	Зміст компетентності	Номер теми, що розкриває зміст компетентності
Загальні компетентності за освітньою програмою		
КЗ-1	Здатність застосовувати знання у практичних ситуаціях.	1-11
КЗ-2	Здатність проводити дослідження на відповідному рівні.	1-11
КЗ-3	Здатність до абстрактного мислення, аналізу та синтезу.	1-11

Номер в освітній програмі	Зміст компетентності	Номер теми, що розкриває зміст компетентності
КЗ-5	Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).	1-11
Спеціальні (фахові, предметні) компетентності (СК) за освітньою програмою		
КФ1	Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.	1-11
КФ2	Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки.	1-11
КФ3	Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.	1-11
КФ4	Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.	1-11
КФ5	Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес / операційних процесів з метою визначення	1-11

Номер в освітній програмі	Зміст компетентності	Номер теми, що розкриває зміст компетентності
	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.	
КФ9	Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому.	1-11
КФ10	Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.	1-11
Програмні результати навчання за освітньою програмою		
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.	1-11
РН2	Інтегрувати фундаментальні та спеціальні знання для розв’язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.	1-11
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.	1-11
РН4	Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні	1-11

Номер в освітній програмі	Зміст компетентності	Номер теми, що розкриває зміст компетентності
	інформаційні технології, фізичні та математичні методи і моделі в сфері 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.	1-11
РН9	Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.	1-11
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.	1-11
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.	1-11
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.	1-11
РН15	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.	1-11

Номер в освітній програмі	Зміст компетентності	Номер теми, що розкриває зміст компетентності
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.	1-11
РН18	Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.	1-11
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.	1-11

4. ЗМІСТ ДИСЦИПЛІНИ

Тема 1. Введення в етичний хакінг

Хакінг: концепція, види і стадії. Складові етичного хакінгу. Основні терміни і поняття хакінгу. Сертифікація хакінгу.

Список рекомендованих джерел:
Основний: 1-3
Додатковий: 5-7,9,11
Інтернет-ресурси: 12-15,17-18

Тема 2. Хакерські атаки і фази хакінгу

Види хакерскіх атак. Фази хакінгу (ланцюг кібервбивства): підготовка, проникнення, поширення та закріплення в системі, досягнення цілей атаки, замітання слідів. Таргетовані та АТР–атаки. Техніки і інструменти DoS/DDoS атак: SYNFlood, ICMP Flood, UDP Flood. Атаки на Web-додатки. Проект OWASP. Міжсайтове виконання сценаріїв (Cross-site Scripting, XSS). Використання операторів SQL (SQL Injection). Використання серверних розширень (SSI Injection).

Список рекомендованих джерел:
Основний: 1-3
Додатковий: 5-7,9,11
Інтернет-ресурси: 12-15,17-18

Тема 3. Збір інформації і попереднє вивчення об'єкта атаки

Методологія, інструмент та способи збирання інформації. Збір інформації без явного підключення до об'єкта атаки (footprinting). Аналіз публічно доступних ресурсів про об'єкт атаки. Використання пошукових систем. Інструментарій Google: Google Hacking Database (GHDB). Збір інформації реєстраційного характеру. Методика збору інформації OSINT. Протидія збиранню інформації.

Список рекомендованих джерел:
Основний: 1-3
Додатковий: 5-7,9,11
Інтернет-ресурси: 12-15,17-18

Тема 4. Сканування мережі

Алгоритми та способи сканування мережі. Ідентифікація вузлів мережі. Ідентифікація відкритих портів. Інструменти сканування: утиліта ***nmap***. Ідентифікація сервісів та додатків. Ідентифікація операційних систем. Визначення топології мережі. Отримання інформації з бази серверів DNS. Прийоми скритого сканування і ухиляння від систем виявлення вторгнень IDS.

Список рекомендованих джерел:
Основний: 1-3
Додатковий: 5-7,9,11
Інтернет-ресурси: 12-15,17-18

Тема 5. Збір інформації за допомогою сервісів прикладного рівня

Використання NetBIOS. Отримання облікових даних. Збір інформації за допомогою SNMP. Основні запити до LDAP-серверів. Отримання інформації із бази серверів DNS. Використання протоколу NTP. Збір банерів для визначення віддаленої системи.

Список рекомендованих джерел:
Основний: 1-3
Додатковий: 5-7,9,11
Інтернет-ресурси: 12-15,17-18

Тема 6. Засоби проникнення на об’єкт атаки

Шпигунське програмне забезпечення. Способи зараження систем. Способи обходу антивірусного захисту. Руткіти, їх різновиди, принципи роботи, методи виявлення. Атаки на механізми реєстрації подій: чищення журналів реєстрації, спотворення результатів аудиту. Управління скомпрометованими системами (використання троянів і «бекдорів»). Сховані та відкриті канали взаємодії. Способи приховування слідів.

Список рекомендованих джерел:
Основний: 1-3
Додатковий: 5-7,9,11
Інтернет-ресурси: 12-15,17-18

Тема 7. Засоби закріплення та поширення на об’єкті атаки

Інструменти та техніки підбору облікових даних і паролів користувачів. Підвищення привілеїв. Програмні та апаратні кейлоггери. Методи аудиту парольного захисту. Використання техніки тунелювання для створення прихованих каналів взаємодії.

Список рекомендованих джерел:
Основний: 1-3
Додатковий: 5-7,9,11
Інтернет-ресурси: 12-15,17-18

Тема 8. Мережеві аналізатори

Аналіз трафіку мережі. Концепція і інструменти сніфінгу. Принципи роботи мережного аналізатора. Прослуховування трафіку в мережах з VLAN. SPAN-порт. Використання вразливостей комутаторів. Аналізатор протоколів ***Wireshark***. Підміна мережевих адрес (спуфинг). Атаки на протокол DHCP. Вразливості протоколу ARP. Атаки на протокол DNS. Спосіб виявлення мережевих аналізаторів.

Список рекомендованих джерел:
Основний: 1-3
Додатковий: 5-7,9,11
Інтернет-ресурси: 12-15,17-18

Тема 9. Методи виявлення вразливостей

Аналіз захищеності інформаційних систем. Пошук і експлуатація вразливостей системи. Сканери безпеки: ***Nessus Security Scanner*** і ***LANguard Network Security Scanner.*** Аудит безпеки інформаційних систем. Перевірка відповідності використовуваних механізмів захисту заданим вимогам.

Список рекомендованих джерел:
Основний: 1-3
Додатковий: 5-7,9,11
Інтернет-ресурси: 12-15,17-18

Тема 10. Виконання тесту на проникнення, пентестінг

Стандарт і концепція виконання тесту на проникнення. Типи, техніки та фази пентесту. Підготовка до пентесту: договір про проведення робіт, дозвіл на тестування. Сбір даних. Моделювання загроз. Аналіз і експлуатація вразливостей. Перевірка стійкості систем до атак. Атестація системи. Підготовка звіту.

Список рекомендованих джерел:
Основний: 1-3
Додатковий: 5-7,9,11
Інтернет-ресурси: 12-15,17-18

Тема 11. Інструменти етичного хакінгу

Спеціалізована операційна система для етичного хакінгу Kali Linux. Набір утиліт етичного хакера PentestBox for Windows. Методологія атаки на веб-ресурси. Інструменти зламу веб-ресурсів.

Список рекомендованих джерел:
Основний: 1-3
Додатковий: 5-7,9,11
Інтернет-ресурси: 12-15,17-18

5. СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

Основний

1. Weidman G. Penetration Testing: A Hands-On Introduction to Hacking. – NY.: Press.Inc, 2014, – 478 с.
2. Ярошенко А.А.ХАКІНГ на прикладах. Вразливості, взлом, захист. Посібник. К.: Наука і техніка, 2021. – 320с.
3. Інформаційна безпека: навчальний посібник / Ю.Я. Бобало, І.В. Горбатий, М.Д. Кіселичник, А. П. Бондарєв та інші; за заг. ред. д-ра техн. наук, проф. Ю.Я. Бобала та д-ра техн. наук, доц. І. В. Горбатого. – Львів : Видавництво Львівської політехніки, 2019. – 580 с.
4. *Хорошко О.В. Захист систем електронних комунікацій: навч.посіб./ В.О. Хорошко, О.В. Криворучко, М.М. Браіловський та ін. – Київ: Київ. нац. торг.-екон. ун-т, 2019. – 164 с.*

Додатковий

5. Сайко В.Г. Мережі бездротового широкосмугового доступу / В.Г.Сайко, В.Я. Казіміренко, Ю.М. Літвінов. – К.: ДУТ, 2015. – 196 с.
6. Довгий С.О. Сучасні телекомунікації: Мережі, технології, безпека, економіка, регулювання / С.О. Довгий, П.П. Воробієнко, К.Д. Гуляєв. – 2-ге вид. – К.: «Азимут Україна», 2013. – 608 с.
7. Інформаційна безпека держави: методичні вказівки до виконання лабораторних робіт/ уклад. О.А. Смірнов, О.К. Конопліцька-Слободенюк, В.Д. Хох, С.А. Смірнов/ – Кропивницький: ЦНТУ – 2017. – 90 с.
8. Комп’ютерні мережі та Інтернет. Навчальний посібник/ В.М. Франчук. – К.: НПУ імені М.П. Драгоманова, 2015 р. – 141 с.
9. Комплексна безпека інформаційних мережевих систем. Навчальний посібник/ А.Г. Микитишин, М.М. Митник, П.Д. Стухляк. – Львів, «Магнолія 2006», 2016. – 256 с.
10. Бурячок В.Л. Основи інформаційної та кібернетичної безпеки. [Навчальний посібник] / В.Л. Бурячок, Р.В. Киричок, П.М. Складанний – К., 2018. – 320 с.
11. Соколов, В.Ю. Безпека безпроводових і мобільних мереж : Лабораторний практикум / В.Ю. Соколов, М. Тадж-Діні / ред. перекл. О.П. Райтер. – К. : ДУТ, 2018. – 122 с.

Інтернет-ресурси

12. Продукти ESET для бізнесу. https://www.eset.com/ua/business/entry-protection-bundle/
13. Засоби захисту інформації − Режим доступу: http://allref.com.ua/uk/skachaty/Zasobi_zahistu_informaciyi?page=7

14. Десять правил безпеки мобільних пристроїв. https://blog.allo.ua/ua/desyat-pravil-bezpeki-mobilnih-pristroyiv_2020-01-39/
15. Хмарна система контролю доступом. Режим доступу – https://www.samekey.com/?lang=uk&gclid=EAIaIQobChMI84Xtg4HR8wIVweeyCh0Mrw4IEAAYASAAEgICAvD_BwE
16. Mobile Policy Handbook [Електронний ресурс] https://www.gsma.com/latinamerica/wp-content/uploads/2019/03/GSMA_Mobile-Policy-Handbook_2019_ENG.pdf
17. Вступ до систем виявлення вторгнень (IDS) – Home | 2021 https://uk.go-travels.com/95456-introduction-to-intrusion-detection-systems-ids-2486799-3152184
18. Захист інформації в операційних системах, базах даних і мережах. https://ppt-online.org/482411

**Курсивом зазначені джерела, що є в наявності в бібліотеці КНТЕУ*