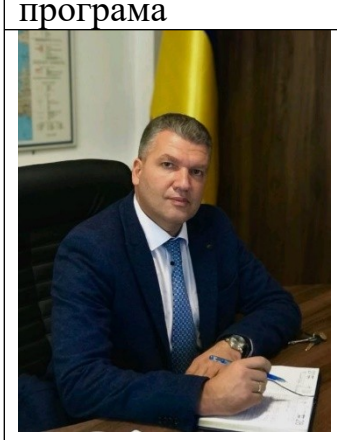
ДЕРЖАВНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
СИСТЕМА УПРАВЛІННЯ ЯКІСТЮ
Система забезпечення якості освітньої діяльності та якості вищої освіти
сертифікована на відповідність ДСТУ ISO 9001:2015 / ISO 9001:2015
Кафедра інженерії програмного забезпечення та кібербезпеки

ЕТИЧНИЙ ХАКІНГ /
ETHICAL HACKING

СИЛАБУС/
SILABUS

ЗАТВЕРДЖЕНО
засіданням кафедри
(протокол №. 1
від «04» серпня 2024 р.)
завідувач кафедри
_____Олена КРИВОРУЧКО

Київ 2024

Назва освітньої компоненти	**ЕТИЧНИЙ ХАКІНГ** / ETHICAL HACKING
Спеціальність	125 «Кібербезпека та захист інформації»
Освітній ступінь	Другий (магістерський)
Освітньо-професійна програма	**БЕЗПЕКА СИСТЕМ ЕЛЕКТРОННИХ КОМУНІКАЦІЙ В ЕКОНОМІЦІ**
	Лектор: **Чубаєвський Віталій** -професор кафедри інженерії програмного забезпечення та кібербезпеки -доктор економічних наук -професор Резюме викладача: https://knute.edu.ua/blog/read/?pid=43646&uk е-пошта: chubaievskyi_vi@knute.edu.ua
	Лектор: **Звєрєв Володимир** -доцент кафедри інженерії програмного забезпечення та кібербезпеки -кандидат технічних наук -доцент Резюме викладача: https://knute.edu.ua/blog//read/?pid=43658&uk е-пошта: zvieriev_vp@knute.edu.ua
Консультації	https://knute.edu.ua/blog/read/?pid=47103&uk
Програма освітньої компоненти	https://knute.edu.ua/blog/read/?pid=48216
ЗМІСТ ОСВІТНЬОЇ КОМПОНЕНТИ	
Тема 1. Введення в етичний хакінг.	Хакінг: концепція, види і стадії. Складові етичного хакінгу. Основні терміни і поняття хакінгу. Сертифікація хакінгу.
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).
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.
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.
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.
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.
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.
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.
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.
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.
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 ОСНОВНИХ РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

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.*

РЕЗУЛЬТАТИ ВИВЧЕННЯ ОСВІТНЬОЇ КОМПОНЕНТИ

Дисципліна забезпечує оволодіння здобувачами вищої освіти загальними та фаховими компетентностями і досягнення ними програмних результатів навчання:

КЗ-01.	Здатність застосовувати знання у практичних ситуаціях.
КЗ-02.	Здатність проводити дослідження на відповідному рівні.
КЗ-03.	Здатність до абстрактного мислення, аналізу та синтезу.
КЗ-05.	Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).
КФ-01.	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.
КФ-02.	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.
КФ-03.	Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
КФ-04.	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.
КФ-05.	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.
КФ-09.	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.
КФ-10.	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.
КФ-12	*Здатність виконувати обов'язки внутрішнього консультанта і радника у своїй експертній області.*
КФ-13	*Здатність проводити дослідно-експериментальну роботу щодо процедури сканування вразливостей та їх розпізнавання в системах безпеки*
РН-01	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.
РН-02	Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.
РН-03	Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.

РН-04	Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.
РН-08	Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.
РН 09	Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.
РН-10	Забезпечувати безперервність бізнес / операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.
РН-11	Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
РН-13	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.
РН-15	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.
РН-17	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.
РН-18	Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.
РН-20	Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.
РН - 25	*Виконувати обов’язки внутрішнього консультанта/ радника в технічній сфері та галузі авторського права щодо електронних носіїв інформації.*
РН - 27	*Проводити сканування систем безпеки інформаційних ресурсів на вразливості.*
РН - 28	*Застосовувати принципи забезпечення безпеки інформації – збереження конфіденційності, цілісності та доступності.*

ОЦІНЮВАННЯ ЗНАНЬ ЗДОБУВАЧІВ ОСВІТИ

Сума балів, накопичених здобувачем вищої освіти за виконання всіх видів поточних навчальних завдань (робіт) на лабораторних/практичних заняттях, свідчить про

ступінь оволодіння ним програмою освітньої компоненти на конкретному етапі її вивчення. Протягом семестру здобувачі освіти можуть набрати від 0 до 100 балів, що переводяться у національну шкалу оцінювання і відповідно у шкалу ЄКТС. Кількість балів відповідає певному рівню засвоєння дисципліни

Довідник з розподілу оцінок ДТЕУ (Шкала ЄКТС):

Бали ДТЕУ	Відсоток балів відносно загальної кількості одержаних прохідних балів	Кумулятивний відсоток отриманих прохідних балів
90-100	20	20
82-89	10	зо
75-81	20	50
69-74	10	60
60-68	40	100

Розподіл балів за видами робіт:

Вид роботи	**Бали**	**Вид роботи**	**Бали**
Лабораторна робота 1	3	Самостійна робота 1	2
Лабораторна робота 2	3	Самостійна робота 2	2
Лабораторна робота 3	3	Самостійна робота 3	2
Лабораторна робота 4	3	Самостійна робота 4	2
Лабораторна робота 5	3	Самостійна робота 5	2
Лабораторна робота 6	3	Самостійна робота 6	3
Лабораторна робота 7	4	Самостійна робота 7	3
Лабораторна робота 8	5	Самостійна робота 8	3
Лабораторна робота 9	5	Самостійна робота 9	3
Лабораторна робота 10	5	Самостійна робота 10	3
Лабораторна робота 11	5	Самостійна робота 11	3
Додаткові бали + Захист проєкту	20	Наукова робота	10

Вимоги до критеріїв оцінювання самостійної роботи студента (оцінювання одного завдання у відсотковому еквіваленті)

40%	Детальний розгляд сутності та вмісту основних джерел. Подання фактів, ідей і результатів досліджень у логічній послідовності. Правильно проаналізовано поточний стан дослідження проблеми та зроблено огляд перспектив подальшого розвитку даного питання.
40%	Обґрунтованість аргументів, підтвердження особистого ставлення, пропозиції стосовно вирішення завдання, встановлення напрямків аналізу.
20%	Оформлення звіту у відповідності вимог

Критерії оцінювання самостійної роботи студента (оцінювання одного завдання у відсотковому еквіваленті)	
100%	В повному обсязі володіє навчальним матеріалом, вільно самостійно та аргументовано його викладає під час усних виступів та письмових відповідей, глибоко та всебічно розкриває зміст теоретичних питань та лабораторних завдань, використовуючи при цьому обов'язкову та додаткову літературу. Правильно вирішив усі тестові завдання.
80%	Достатньо повно володіє навчальним матеріалом, обґрунтовано його викладає під час усних виступів та письмових відповідей, в основному розкриває зміст теоретичних питань та лабораторних завдань, використовуючи при цьому обов'язкову літературу. Але при викладанні деяких питань не вистачає достатньої глибини та аргументації, допускаються при цьому окремі несуттєві неточності та незначні помилки. Правильно вирішив більшість тестових завдань
60%	В цілому володіє навчальним матеріалом викладає його основний зміст під час усних виступів та письмових відповідей, але без глибокого всебічного аналізу, обґрунтування та аргументації, без використання необхідної літератури допускаючи при цьому окремі суттєві неточності та помилки. Правильно вирішив половину тестових завдань.
40%	Не в повному обсязі володіє навчальним матеріалом. Фрагментарно, поверхово (без аргументації та обґрунтування) викладає його під час усних виступів та письмових відповідей, недостатньо розкриває зміст теоретичних питань та лабораторних завдань, допускаючи при цьому суттєві неточності, правильно вирішив меншість тестових завдань.
20%	Частково володіє навчальним матеріалом не в змозі викласти зміст більшості питань теми під час усних виступів та письмових відповідей, допускаючи при цьому суттєві помилки. Правильно вирішив окремі тестові завдання.
0%	Не володіє навчальним матеріалом та не в змозі його викласти, не розуміє змісту теоретичних питань та практичних завдань. Не вирішив жодного тестового завдання.

ОСНОВНІ ПОЛОЖЕННЯ, ЩО РЕГЛАМЕНТУЮТЬ ОСВІТНІЙ ПРОЦЕС	
діючі положення	https://knute.edu.ua/blog/read/?pid=44402
нормативно-правова база організації освітнього процесу	https://knute.edu.ua/blog/read/?pid=7330&uk

студенту	https://knute.edu.ua/#forstudent
НЕФОРМАЛЬНА ОСВІТА Рекомендовані сертифікаційні програми, курси, посібники користувача	
European Union Agency for Cybersecurity (Агентство Європейського Союзу з питань кібербезпеки)	https://www.enisa.europa.eu
The EU Cyberdiplomacy Toolbox	https://www.cyber-diplomacy-toolbox.com/
MS AZURE	https://learn.microsoft.com/uk-ua/training/azure/
Cloud Native Computing Foundation	https://www.cncf.io/
Isaca	https://www.isaca.org/training-and-events
CSA (Cloud security alliance)	https://cloudsecurityalliance.org/research/artifacts

ПОЛІТИКА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ:

Відвідування лекційних та лабораторних занять: відвідування	Відвідування лекційних та лабораторних занять є обов'язковим. Допускаються пропуски занять з таких поважних причин, як хвороба (викладачу надається копія довідки від медичного закладу), участь в олімпіаді, творчому конкурсі тощо за попередньою домовленістю та згодою викладача за умови дозволу деканату (надаються документи чи інші матеріали, які підтверджують заявлену участь у діяльності студента).
Відпрацювання пропущених занять:	відпрацювання пропущених занять є обов'язковим незалежно від причини пропущеного заняття. Лекційне заняття має бути відпрацьоване до наступної лекції на консультації викладача з використанням ПЗ 365 Office Teams. Відпрацювання лекційного матеріалу передбачає вивчення пропущеного теоретичного матеріалу та складання тесту за цим матеріалом. Лабораторне заняття відпрацьовується під час консультації викладача (розклад консультацій на сайті).
Правила поведінки під час занять	обов'язковим є дотримання техніки безпеки в комп'ютерних лабораторіях. Студенти повинні приймати активну участь в обговоренні навчально матеріалу ознайомившись з ним напередодні (навчальний матеріал надається викладачем). Мобільні пристрої дозволяється використовувати лише під час он-лайн тестування та підготовки практичних завдань в процесі заняття. Задля зручності, дозволяється використання ноутбуків та інших електронних пристроїв під час навчання в комп'ютерних аудиторіях (за взаємною згодою всіх учасників освітнього процесу)
Політика академічної	https://knute.edu.ua/blog/read/?pid=38987&uk

доброчесності ДТЕУ	