ЗАТВЕРДЖЕНО

Вченою радою факультету інформаційно-комп'ютерних технологій

28 серпня 2024 р., протокол №8

Голова Вченої ради

Тетяна НІКІТЧУК

РОБОЧА ПРОГРАМА
вибіркової навчальної дисципліни фахової підготовки
«Етичний хакінг»
факультет інформаційно-комп'ютерних технологій

для здобувачів вищої освіти освітнього ступеня «бакалавр»

Схвалено на засіданні кафедри комп'ютерної інженерії та кібербезпеки
26 серпня 2024 р., протокол №6

Завідувач кафедри

Андрій ЄФІМЕНКО

Розробники: старший викладач кафедри комп'ютерної інженерії та кібербезпеки Олександра ПОКОТИЛО, кандидат технічних наук, доцент, завідувач кафедри комп'ютерної інженерії та кібербезпеки Андрій ЄФІМЕНКО

Житомир
2024 – 2025 н.р.

Робоча програма навчальної дисципліни «Етичний хакінг» для здобувачів вищої освіти освітнього ступеня «бакалавр» затверджена Вченою радою факультету інформаційно-комп’ютерних технологій від 28 серпня 2024 р., протокол № 8.

1. Опис навчальної дисципліни

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, спеціальність, освітній ступінь</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td>денна форма навчання</td><td>заочна форма навчання</td></tr>
<tr><td>Кількість кредитів 4</td><td>Галузь знань
12 «Інформаційні технології»</td><td colspan="2">Вибіркова</td></tr>
<tr><td>Модулів – 1</td><td rowspan="5">Спеціальність 122
«Комп’ютерні науки»</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td rowspan="2">Змістових модулів – 2</td><td>2024</td><td>2025</td></tr>
<tr><td colspan="2">Семестр</td></tr>
<tr><td rowspan="2">Загальна кількість годин – 120</td><td>2</td><td>__</td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td rowspan="11">Тижневих годин для денної форми навчання:
аудиторних – 4
самостійної роботи – 4</td><td rowspan="11">Освітній ступінь «бакалавр»</td><td>32 год.</td><td>__ год.</td></tr>
<tr><td colspan="2">Практичні</td></tr>
<tr><td>__ год.</td><td>__ год.</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>32 год.</td><td>__ год.</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>56 год.</td><td>__ год.</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td colspan="2">Вид контролю: залік</td></tr>
</table>

Частка аудиторних занять і частка самостійної та індивідуальної роботи у загальному обсязі годин з навчальної дисципліни становить:

для денної форми навчання – 53 % аудиторних занять, 47% самостійної та індивідуальної роботи.

2. Мета та завдання навчальної дисципліни

Метою вивчення навчальної дисципліни «Етичний хакінг» є вивчення теоретичних та практичних основ етичного хакінгу і тестування на проникнення для виявлення вразливостей у сучасних інформаційних системах і мережах, отримання знань щодо методологій збору інформації, сканування, атак соціальної інженерії, експлуатації вразливостей дротових та бездротових мереж, веб-додатків, хмарних, мобільних та IoT-систем. Особлива увага приділяється постексплуатаційним технікам, складанню звітів та ефективній комунікації результатів пентесту із зацікавленими сторонами для підвищення рівня кіберзахисту.

Завданнями навчальної дисципліни є:

– надання практичних знань про методології етичного хакінгу та пентестування;

– навчання збору інформації, виявленню та експлуатації вразливостей у системах;

– розвиток навичок проведення атак соціальної інженерії;

– опанування методів експлуатації вразливостей мережевих, веб-додатків, мобільних та IoT-систем;

– формування вмінь застосування постексплуатаційних технік;

– навчання складанню звітів та ефективної комунікації з зацікавленими сторонами.

Під час вивчення навчальної дисципліни здобувачі вищої освіти зможуть отримати додатково наступні Soft skills:

- *комунікативні навички*: письмове, вербальне й невербальне спілкування; уміння грамотно спілкуватися по e-mail; вести дискусію і відстоювати свою позицію; навички працювати в команді;

- *керування часом:* уміння справлятися із завданнями вчасно;

- *гнучкість і адаптивність:* гнучкість, адаптивність і здатність змінюватися; уміння аналізувати ситуацію, орієнтування на вирішення проблеми;

- *лідерські якості*: уміння спокійно працювати в напруженому середовищі; уміння ухвалювати рішення; уміння ставити мету, планувати діяльність;

- *особисті якості:* креативне й критичне мислення; етичність, чесність, терпіння, повага до оточуючих.

3. Програма навчальної дисципліни

Модуль 1

Змістовий модуль 1. Основи етичного хакінгу та тестування на проникнення

Тема 1. Вступ до етичного хакінгу

Поняття етичного хакінгу та тестування на проникнення. Загрози та типи зловмисників. Вивчення методології тестування на проникнення. Типи тестів на проникнення. Створення власної лабораторії: вимоги та вказівки. Відновлення лабораторного середовища.

Тема 2. Планування та визначення обсягу тесту на проникнення

Порівняння та протиставлення концепцій управління, ризику та комплаєнсу. Правові поняття та відмова від відповідальності. Важливість визначення обсягу та організаційних вимог або вимог замовника. Документ з правилами взаємодії. Етичне хакерське мислення.

Тема 3. Збір інформації та сканування вразливостей

Виконання пасивної розвідки. DNS Lookups. Ідентифікація технічних та адміністративних контактів. Репутація та безпека компанії. Збір розвідувальних даних з відкритих джерел (OSINT) Проведення активної розвідки. Типи сканування Nmap. Перевірка пакетів і прослуховування. Мистецтво сканування вразливостей. Аналіз результатів сканування вразливостей.

Тема 4. Атаки соціальної інженерії

Видавання себе за іншу особу. Атаки соціальної інженерії. Фішинг електронної пошти. Вішинг. SMS фішинг. USB Drop Key. Атака Watering Hole. Фізичні атаки. Tailgating, Dumpster Diving, Shoulder Surfing, Badge Cloning. Набір інструментів соціального інженера (SET). Browser Exsploitation Framework (BeEF). Методи впливу.

Тема 5. Використання вразливостей дротових та бездротових мереж

Використання вразливостей мережі. Розпізнавання імен Windows і атаки SMB. Отруєння кешу DNS. Експлойти SNMP, SMTP, FTP. Атаки передачі хешів, Kerberos і LDAP. Атаки на шляху, маніпуляції маршрутом. DoS- і DDoS-атаки. Обхід контролю доступу до мережі (NAC). Використання вразливостей бездротового зв’язку. Несанкціоновані точки доступу. Атаки роз’єднання, списку

пріорітетних мереж, KARMA, Bluejacking і Bluesnarfing, Bluetooth Low Enrtgy (BLE).

Змістовий модуль 2. Експлуатація вразливостей, постексплуатаційні техніки та звітність у пентестингу

Тема 6. Експлуатація вразливостей веб-додатків

Огляд атак на основі веб-додатків для професіоналів із безпеки та 10 найкращих OWASP. Створення власної лабораторії веб-додатків. Недоліки бізнес-логіки. Вразливості на основі ін'єкцій, автентифікації, авторизації. Вразливості міжсайтового сценарію (XSS). Атаки підробки міжсайтових запитів (CRFX/XSRF) і підробки запитів на стороні сервера. Клікджекінг. Використання неправильних конфігурацій безпеки. Вразливості запуску файлів. Використання небезпечних практик коду.

Тема 7. Безпека хмарних, мобільних та IoT-систем

Дослідження векторів атак і здійснення атак на хмарні технології. Збір облікових даних. Підвищення привілеїв. Захоплення облікового запису. Атаки на службу метаданих. Вичрпання ресурсів і DoS-атаки. Інструменти та комплекти розробки програмного забезпечення (SDK). Поширені атаки і вразливості проти спеціалізованих систем: атаки на мобільні пристрої, на пристрої інтернету речей (IoT). Використання віртуальних машин.

Тема 8. Постексплуатаційні техніки

Створення точки опори та підтримка стійкості після компрометації системи. Утиліти командування та керування (C2). Спеціальні демони, процеси та додаткові бекдори. Сканування після експлуатації.

Тема 9. Звітність та комунікація

Важливі компоненти письмових звітів. Час зберігання звітів і безпечне розповсюдження. Аналіз висновків і рекомендацій щодо виправлень у звіті. Технічні засоби контролю. Адміністративний, операційний контроль. Фізичні елементи керування. Важливість спілкування під час процесу тестування на проникнення. Дії після публікації звіту.

Тема 10. Інструменти та аналіз коду

Основні концепції створення сценаріїв і розробки програмного забезпечення. Логічні конструкції, структури даних. Бібліотеки, процедури, функції, класи. Оболонка Bash. Ресурси для вивчення Python, Ruby, PowerShell, Perl, JavaScript, Різні випадки використання інструментів тестування на проникнення та аналіз

коду експлойтів. Загальні інструменти для розвідки, сканування вразливостей, атак облікових даних, Software Assurance.

4. Структура (тематичний план) навчальної дисципліни

Змістові модулі і теми	Кількість годин							
	денна форма				заочна форма			
	усього	лекції	лабораторні	самостійна робота	усього	лекції	практичні (лабораторні)	самостійна робота
Модуль 1								
Змістовий модуль 1. Основи етичного хакінгу та тестування на проникнення								
Тема 1. Вступ до етичного хакінгу	8	2	2	4	-	-	-	-
Тема 2. Планування та визначення обсягу тесту на проникнення	10	2	2	6	-	-	-	-
Тема 3. Збір інформації та сканування вразливостей	14	4	4	6	-	-	-	-
Тема 4. Атаки соціальної інженерії	16	4	6	6	-	-	-	-
Тема 5. Використання вразливостей дротових та бездротових мереж	12	4	2	6	-	-	-	-
Разом за змістовий модуль 1	60	16	16	28	-	-	-	-
Змістовий модуль 2. Експлуатація вразливостей, постексплуатаційні техніки та звітність у пентестингу								
Тема 6. Експлуатація вразливостей веб-додатків	14	4	4	6	-	-	-	-
Тема 7. Безпека хмарних, мобільних та IoT-систем	16	4	6	6	-	-	-	-
Тема 8. Постексплуатаційні техніки	10	2	2	6	-	-	-	-
Тема 9. Звітність та комунікація	8	2	2	4	-	-	-	-
Тема 10. Інструменти та аналіз коду	12	4	2	6	-	-	-	-
Разом за змістовий модуль 2	60	16	16	28	-	-	-	-

Змістові модулі і теми	Кількість годин							
	денна форма				заочна форма			
	усього	лекції	лабораторні	самостійна робота	усього	лекції	практичні (лабораторні)	самостійна робота
ВСЬОГО	120	32	32	56	-	-	-	-

5. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
Модуль 1			
Змістовий модуль 1. Основи етичного хакінгу та тестування на проникнення			
1	Порівняння технологій тестування на проникнення	2	-

2	Створення угоди про тестування на проникнення	2	-
3	Використання інструментів OSINT	2	-
4	Сканування мережі з використанням Wireshark	2	-
5	Дослідження джерел інформації про вразливості	2	-
6	Ознайомлення з набором інструментів соціального інженера (SET)	2	-
7	Використання браузера Exploitation Framework (BeEF)	2	-
8	On-Path атаки з використанням Ettercap	2	-
Змістовий модуль 2. Експлуатація вразливостей, постексплуатаційні техніки та звітність у пентестингу			
9	Сканування вразливостей веб-сайту	2	-
10	Використання сканера вразливостей GVM	2	-
11	Атаки ін’єкцій	2	-
12	Використання інструментів для роботи з паролями	2	-
13	Міжсайтовий скриптинг	2	-
14	Використання посібника з тестування безпеки OWASP	2	-
15	Дослідження звітів пентесту	2	-
16	Аналіз сценаріїв і зразків коду для використання в тестуванні на проникнення	2	-
	РАЗОМ	**32**	

6. Завдання для самостійної роботи

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
Модуль 1			
Змістовий модуль 1. Основи етичного хакінгу та тестування на проникнення			

1	Аналіз нормативно-правових аспектів етичного хакінгу та тестування на проникнення	4	-
2	Оцінка ризиків під час планування тесту на проникнення	4	-
3	Дослідження методологій збору інформації та їх порівняльний аналіз	4	-
4	Виявлення специфічних вразливостей у внутрішніх корпоративних мережах	4	-
5	Роль соціальної інженерії у цільових атаках на корпоративні середовища	6	-
6	Порівняння методів захисту від атак на дротові та бездротові мережі	6	-
Змістовий модуль 2. Експлуатація вразливостей, постексплуатаційні техніки та звітність у пентестингу			
7	Оцінка вразливостей веб-додатків із використанням нестандартних методів тестування	6	-
8	Захист хмарних інфраструктур: аналіз стратегій безпеки від сучасних загроз	4	-
9	Постексплуатаційні техніки для підтримки тривалого доступу в мережах з підвищеною безпекою	4	-
10	Дослідження методів приховування слідів під час тестування на проникнення	4	-
11	Створення звітів на основі специфіки галузевих стандартів безпеки (ISO/IEC 27001, NIST тощо)	4	-
12	Аналіз ефективності використання автоматизованих інструментів для написання звітів пентесту	6	-
	РАЗОМ	**56**	**-**

7. Індивідуальні самостійні завдання

Індивідуальні самостійні завдання курсом не передбачені.

8. Методи навчання

Під час викладання навчальної дисципліни використовуються наступні методи навчання:

– Вербальні методи (лекція, пояснення)

– Наочні методи (спостереження, демонстрація, ілюстрація)

– Практичні методи (виконання різних видів вправ, практичних завдань, кейсів)

– Дискусійний метод

– Методи самостійної роботи (анотування опрацьованого матеріалу, вирішення задач, проведення розрахунків)

9. Методи контролю

Перевірка досягнення результатів навчання здійснюється з використанням наступних методів:

- Усне опитування, участь у дискусії, відповіді на проблемні запитання
- Перевірка виконання практичних завдань, вправ, кейсів
- Перевірка виконання та захист лабораторних робіт
- Експрес-тестування
- Залік

10. Оцінювання результатів навчання здобувачів вищої освіти

Оцінювання результатів навчання здобувачів вищої освіти з навчальної дисципліни здійснюється відповідно до Положення про оцінювання результатів навчання здобувачів вищої освіти у Державному університеті «Житомирська політехніка» та розподілу балів, що наведений нижче.

Система оцінювання результатів навчання здобувачів вищої освіти з навчальної дисципліни включає поточний та підсумковий контроль.

Поточний контроль проводиться для оцінювання рівня засвоєння знань, формування умінь і навичок здобувачів вищої освіти впродовж вивчення ними змістових модулів навчальної дисципліни. Поточний контроль здійснюється під час проведення навчальних занять.

Підсумковий контроль проводиться для підсумкового оцінювання результатів навчання здобувачів вищої освіти з навчальної дисципліни. Підсумковий контроль здійснюється після завершення вивчення навчальної дисципліни. Підсумковий контроль проводиться у формі заліку. Процедура складання заліку визначена у Положенні про організацію освітнього процесу у Державному університеті «Житомирська політехніка».

Розподіл балів з навчальної дисципліни

Види робіт здобувача вищої освіти	Кількість балів за семестр	
	денна форма	заочна форма
Виконання завдань поточного контролю	100	-
Підсумкова семестрова оцінка	**100**	**-**

Розподіл балів за виконання завдань поточного контролю

Види робіт здобувача вищої освіти	Кількість балів за семестр	
	денна форма	заочна форма

Види робіт здобувача вищої освіти	Кількість балів за семестр	
	денна форма	заочна форма
Виконання завдань під час навчальних занять	100	-
Виконання та захист індивідуальних самостійних завдань	-	-
Виконання науково-дослідної роботи та інших видів робіт (**додаткові – заохочувальні бали**)[3]: 1. Участь у студентських предметних олімпіадах, Всеукраїнському конкурсі студентських наукових робіт, грантах, науково-дослідних проектах 2. Підготовка наукових статей, тез доповідей наукових конференцій 3. Інші види робіт (наводиться перелік інших видів робіт)	-	-
Разом за виконання завдань поточного контролю	**100**	**100**

Розподіл балів за виконання завдань під час навчальних занять

Види робіт здобувача вищої освіти[1]	Кількість балів за семестр	
	денна форма	заочна форма
Виконання тестових завдань	40	-
Виконання та захист лабораторних робіт	60	-
Разом за виконання завдань під час навчальних занять	**100**	**-**

З метою застосування цілих чисел для оцінювання результатів роботи здобувачів вищої освіти під час навчальних занять протягом семестру використовується 100-бальна шкала оцінювання кожного окремо виду робіт. Розрахунок набраних здобувачем вищої освіти балів за виконання завдань під час навчальних занять за семестр проводиться за формулою:

$$Р_{НЗ} = (Р_{ТЗ^{100}} \times ВК_{ТЗ} + Р_{ЛР^{100}} \times ВК_{ЛР}) \times К_{НЗ}, \qquad (1)$$

де $Р_{НЗ}$ – кількість набраних здобувачем вищої освіти балів за виконання завдань під час навчальних занять за семестр;

$Р_{ТЗ^{100}}$, $Р_{ЛР^{100}}$ – кількість набраних здобувачем вищої освіти балів за семестр відповідно за виконання тестових завдань, виконання та захист лабораторних робіт (за 100-бальною шкалою);

$ВК_{ТЗ}$, $ВК_{ЛР}$ – вагові коефіцієнти відповідно за відповіді (виступи) на заняттях, за участь у дискусії, за виконання іншого виду робіт, визначеного викладачем. Значення вагових коефіцієнтів розраховуються шляхом ділення кількості балів, які встановлені за виконання окремого виду робіт під час навчальних занять, на сумарну кількість балів за виконання цих робіт (дані для розрахунку вагових коефіцієнтів наведено в табл. «Розподіл балів за виконання завдань під час

навчальних занять»);

$К_{НЗ}$ – коригувальний коефіцієнт, який визначається шляхом ділення кількості балів, що встановлені за виконання завдань під час навчальних занять, на 100 балів.

Якщо здобувач вищої освіти набрав за поточний контроль 60 балів або більше, він може погодити дану оцінку в електронному кабінеті і вона стане семестровою оцінкою за вивчення навчальної дисципліни.

Якщо здобувач вищої освіти під час вивчення навчальної дисципліни набрав 60 балів або більше і бажає покращити свій результат успішності, він проходить процедуру підсумкового контролю у формі заліку. За складання заліку здобувач вищої освіти може набрати 100 балів. Семестрова оцінка з навчальної дисципліни формується за результатами підсумкового контролю.

Здобувач вищої освіти допускається до процедури підсумкового контролю у формі заліку, якщо за виконання завдань поточного контролю набрав 50 балів або більше.

Якщо здобувач вищої освіти за результатами поточного контролю набрав 35□49 балів, він отримує право за власною заявою повторно опанувати окремі теми (змістові модулі) навчальної дисципліни понад обсяги, встановлені навчальним планом освітньої програми. Повторне вивчення окремих складових навчальної дисципліни понад обсяги, встановлені навчальним планом освітньої програми, здійснюється у вільний від занять здобувача вищої освіти час.

Якщо здобувач вищої освіти за результатами поточного контролю набрав від 0 до 34 балів (включно), він вважається таким, що не виконав вимоги робочої програми навчальної дисципліни та має академічну заборгованість. Здобувач вищої освіти отримує право за власною заявою повторно опанувати навчальну дисципліну у наступному семестрі понад обсяги, встановлені навчальним планом освітньої програми.

Процедура надання додаткових освітніх послуг здобувачу вищої освіти з метою повторного вивчення навчальної дисципліни чи її окремих складових частин визначена у Положенні про надання додаткових освітніх послуг здобувачам вищої освіти в Державному університеті «Житомирська політехніка».

Визнання результатів навчання, набутих у неформальній та/або інформальній освіті

Визнання результатів навчання, набутих у неформальній та/або інформальній освіті в рамках окремих тем навчальної дисципліни, здійснюється викладачем за зверненням здобувача вищої освіти та представленням документів, які підтверджують результати навчання (сертифікати, свідоцтва, скріншоти тощо).

Рішення про визнання та оцінка за відповідну частину освітнього компонента приймається викладачем за результатами співбесіди зі здобувачем вищої освіти.

Визнання результатів навчання, набутих у неформальній та/або інформальній освіті в рамках цілого освітнього компонента, здійснюється за процедурою, яка визначена у Положенні про організацію освітнього процесу у Державному університеті «Житомирська політехніка».

Шкала оцінювання

Шкала ЄКТС	Національна шкала	100-бальна шкала
A	Зараховано	90-100
B	Зараховано	82-89
C		74-81
D	Зараховано	64-73
E		60-63
FX	Не зараховано	35-59
F	Не зараховано	0-34

11. Глосарій

№ з/п	Термін державною мовою	Відповідник англійською мовою
1	Атака зловмисного програмного забезпечення	Malware attack
2	Атака соціальної інженерії	Social engineering attack
3	Аутентифікація	Authentication
4	Авторизація	Authorization
5	Віддалений доступ	Remote access
6	Вразливість	Vulnerability
7	Двофакторна аутентифікація	Two-factor authentication (2FA)
8	Експлуатація вразливості	Exploitation
9	Захист інформації	Information protection
10	Зловмисник	Attacker
11	Ін'єкційна атака	Injection attack
12	Мережева безпека	Network security
13	Міжсайтовий скриптинг	Cross-site scripting (XSS)
14	Мобільна безпека	Mobile security
15	Пентестер	Pentester
16	Перевірка безпеки	Security audit
17	Перехоплення даних	Data interception
18	Тест на проникнення	Penetration test (Pentest)
19	Шифрування	Encryption
20	Хмарні системи	Cloud systems

12. Рекомендована література

Основна література

1. Бобало Ю.Я., Горбатий І.В. (ред.) Інформаційна безпека. Навчальний посібник. — Львів : Видавництво Львівської політехніки, 2019. — 580 с. — ISBN 978-966-941-339-0.
2. Allen J. The Hacker Playbook 3: Practical Guide To Penetration Testing. CreateSpace Independent Publishing Platform, 2020, – 350 p.
3. Simpson M., Backman K., Corley J. Hands-On Ethical Hacking and Network Defense. Cengage Learning, 2019, – 480 p.

Допоміжна література

1. Aaron Philipp, David Cowen, Chris Davis. Hacking exposed computer forensics. Second edition. The McGraw-Hill Companies, 2010.
2. Wilhelm, Thomas. Professional penetration testing: Creating and learning in a hacking lab. Newnes, 2013, 525 p.
3. Messier R. Bug Bounty Bootcamp: The Guide to Finding and Reporting Web Vulnerabilities. No Starch Press, 2021, – 420 p.
4. 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

13. Інформаційні ресурси в Інтернеті

1. Ethical Hacker [Електронний ресурс] – Режим доступу: https://www.netacad.com/ipd/sessions/ipd-increasing-cybersecurity-resilience-using-a-new-ethical-hacker-course?courseLang=en-US
2. OWASP Foundation [Електронний ресурс] – Режим доступу: https://owasp.org
3. Offensive Security [Електронний ресурс] – Режим доступу: https://www.kali.org/tools/
4. Rapid7. Metasploit Project [Електронний ресурс] – Режим доступу: https://www.metasploit.com
5. EC-Council. Certified Ethical Hacker (CEH) Program [Електронний ресурс] – Режим доступу: https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/

6. SANS Institute [Електронний ресурс] – Режим доступу: https://www.sans.org/pen-testing/