Київський університет імені Бориса Грінченка

Факультет інформаційних технологій та управління

Кафедра інформаційної та кібернетичної безпеки

«ЗАТВЕРДЖУЮ»
Проректор з науково-методичної
та навчальної роботи
_____ О.Б. Жильцов
«31» 01 2019 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ПРИКЛАДНІ АСПЕКТИ ТЕСТУВАНЬ НА ПРОНИКНЕННЯ ТА ЕТИЧНОГО ХАКІНГУ»

для студентів

спеціальності	125 Кібербезпека
освітнього рівня	другого (магістерського)
освітньої програми	125.00.02 Безпека інформаційних і комунікаційних систем

КИЇВСЬКИЙ УНІВЕРСИТЕТ
ІМЕНІ БОРИСА ГРІНЧЕНКА
Ідентифікаційний код 02136554
Начальник відділу
моніторингу якості освіти
Програма № 2018/19
(підпис) (прізвище, ініціали)
«___» _____ 20 19 р.

Київ – 2019

Розробник:

Соколов Володимир Юрійович, старший викладач кафедри інформаційної та кібернетичної безпеки Факультету інформаційних технологій та управління Київського університету імені Бориса Грінченка.

Викладачі:

Соколов Володимир Юрійович, старший викладач кафедри інформаційної та кібернетичної безпеки Факультету інформаційних технологій та управління Київського університету імені Бориса Грінченка.

Робочу програму розглянуто і затверджено на засіданні кафедри інформаційної та кібернетичної безпеки

Протокол від 16.01.2019 р. № 1

Завідувач кафедри _____ В.Л. Бурячок
(підпис)

Робочу програму погоджено з гарантом освітньої програми (керівником освітньої програми 125.00.02 Безпека інформаційних і комунікаційних систем)

___.___. 20___ р.

Керівник освітньої програми _____ В.Л. Бурячок
(підпис)

Робочу програму перевірено

___.___. 20___ р.

Заступник директора/декана _____ І.Ю. Мельник
(підпис)

Пролонговано:

на 20__/20__ н.р. _____ (_____), «____»_____ 20___ р., протокол № ___
(підпис) (ПІБ)

на 20__/20__ н.р. _____ (_____), «____»_____ 20___ р., протокол № ___
(підпис) (ПІБ)

на 20__/20__ н.р. _____ (_____), «____»_____ 20___ р., протокол № ___
(підпис) (ПІБ)

на 20__/20__ н.р. _____ (_____), «____»_____ 20___ р., протокол № ___
(підпис) (ПІБ)

Опис навчальної дисципліни

Найменування показників	Характеристика дисципліни за формами навчання	
	денна	заочна
Вид дисципліни	обов'язкова	
Мова викладання, навчання та оцінювання	українська	
Загальний обсяг кредитів / годин	4 / 120	
Курс	5	
Семестр	10	
Кількість змістових модулів з розподілом:	2	
Обсяг кредитів	4	
Обсяг годин, в тому числі:	120	
Аудиторні	32	
Модульний контроль	8	
Семестровий контроль	-	
Самостійна робота	80	
Форма семестрового контролю	залік	

2. Мета та завдання навчальної дисципліни

Робоча навчальна програма з курсу «Прикладні аспекти тестувань на проникнення та етичного хакінгу» є нормативним документом Київського університету імені Бориса Грінченка, який розроблено кафедрою інформаційної та кібернетичної безпеки на основі освітньо-професійної програми підготовки здобувачів другого (магістерського) рівня відповідно до навчального плану спеціальності 125 Кібербезпека, освітньої 125.00.02 «Безпека інформаційних і комунікаційних систем».

Робочу навчальну програму укладено згідно з вимогами Європейської кредитної трансферно-накопичувальної системи (ЄКТС) організації навчання.

Програма визначає обсяги знань, якими повинен опанувати здобувач другого (магістерського) рівня відповідно до вимог освітньо-кваліфікаційної характеристики, алгоритму вивчення навчального матеріалу дисципліни «Прикладні аспекти тестувань на проникнення та етичного хакінгу» та необхідне методичне забезпечення, складові і технологію оцінювання навчальних досягнень студентів.

Навчальна дисципліна «Прикладні аспекти тестувань на проникнення та етичного хакінгу» складається з двох змістових модулів: «Методи тестування на проникнення», «Прикладні аспекти етичного хакінгу». Обсяг дисципліни — 120 год. (4 кредитів).

Метою викладання навчальної дисципліни «Прикладні аспекти тестувань на проникнення та етичного хакінгу» є формування у студентів уміння вирішувати задачі тестування на проникнення інформаційних мереж і систем, застосовувати нормативно-правові, організаційні та технічні процедури етичного хакінгу.

Завдання полягає у формуванні теоретичних знань та практичних умінь у сфері тестування на проникнення та етичного хакінгу, інформаційної та кібернетичної безпеки та набуття **наступних компетентностей**:

Фахова компетентність

КФ-5 — здатність до забезпечення захисту інформації, що обробляється в інформаційно-комунікаційних системах, здійснення адміністрування таких систем та проведення їх експлуатації**.**

3. **Результати навчання за дисципліною**

У результаті вивчення навчальної дисципліни студент повинен

знати:

• загальні терміни етичного хакерства: уразливості, експлуатація, корисне навантаження, нульовий день;
• методологія тестування проникнення;
• як використовувати спільні уразливості;
• як здійснювати онлайнові та автономні атаки паролів;
• як здійснювати атаки «людина в середині»;
• як працює сканер уразливостей.

уміти:

• використання інструментів для етичного злому;
• підготувати звіт із висновками та рекомендаціями.

та досягти наступних **програмних результатів навчання:**

ПРз-4 — знати методи і способи розробки та тестування програмного забезпечення з виявлення і усунення активності, що загрожує безпеці системи (антивіруси, firewalls, сніфери, сканери портів).

ПРз-5 — вміти проводити семантичний аналіз файлів; вміти виявляти злоякісне програмне забезпечення й файли за їх структурою та поведінкою; вміти відновлювати пошкоджену інформацію; вміти моделювати уразливості ПЗ та використовувати шаблони проектування для захисту ПЗ.

ПРз-9 — володіти практичними навичками проведення аудиту безпеки ІКС, їх адміністрування та експлуатації; вміти проектувати перспективні криптосистеми та застосовувати сучасні технології криптографічного захисту інформації в системах інформаційної та/або кібербезпеки.

4. Структура навчальної дисципліни

Тематичний план для денної форми навчання

Назва змістових модулів, тем	Усього	Розподіл годин між видами робіт					
		Аудиторна:					Самостійна
		Лекції	Семінари	Практичні	Лабораторні	Індивідуальні	
Змістовий модуль 1. Методи тестування на проникнення							
Тема 1. Вступ до тестування проникнення	16	2		2	2		10
Тема 2. Збір інформації	20	2		2	2		14
Тема 3. Аналіз вразливостей	20	2		2	2		14
Модульний контроль	4						
Разом	60	6		6	6		38
Змістовий модуль 2. Прикладні аспекти етичного хакінгу							
Тема 4. Експлуатація веб-додатків	30	4		2	2		22
Тема 5. Соціальна інженерія та підтримка доступу	26	2		2	2		20
Модульний контроль	4						
Разом	60	6		4	4		42
Усього	120	12		10	10		80

5. Програма навчальної дисципліни

Змістовий модуль 1. Методи тестування на проникнення

Основні питання:

- Основні терміни тестування на проникнення.
- Хто такі хакери та етичні хакери?
- Що роблять справжні хакери?
- Методології тестування на проникнення: OSTMM та ISSAF.
- Управління проектами проникнення.
- Огляд інструментів злому.
- Законодавча база в галузі хакінгу.
- Методи відкритої розвідки.
- Огляд структурованих аналітичних методів.
- Типи інформації.
- Виявлення джерел інформації.
- Принципи роботи пошукових ботів.
- Оператори розширеного пошуку Google.
- Виявлення IP-адрес.
- Трасування маршрутів.
- Використання Maltego.
- Використання theHarvester.
- Підміна зони DNS.
- Примусове використання DNS.
- Типи вразливостей.
- Пошук уразливостей вручну.
- Автоматизований пошук уразливостей.
- Інструменти аналізу вразливостей.

- Використовувати бази даних паролів для підбору.
- Google для тестів на проникнення.
- Локальні та віддалені експлойти.
- Особливості фреймворка Metasploit.
- Атака людина по середині.
- Онлайн і офлайн атаки на паролі.
- Ручний підбір паролів.
- Проведення атаки на хеші.

Змістовий модуль 2. Прикладні аспекти етичного хакінгу

Основні питання:

- Робота з третіми особами.
- Визначення соціальної інженерії.
- Типова структура веб-додатків.
- Загальні веб-уразливості.
- Проекти OWASP.
- Огляд фреймворка з тестування OWASP.
- Google Hacking Database (GHDB).
- Засоби тестування веб-безпеки.
- Підтримка методів доступу.
- Використання Meterpreter.
- Етичний злом.
- Kali Linux.
- Сканери портів.
- Сканери вразливостей.

6. Контроль навчальних досягнень

Навчальні досягнення студентів з дисципліни оцінюються за модульно-рейтинговою системою, в основу якої покладено принцип поопераційної звітності, обов'язковості модульного контролю, накопичувальної системи оцінювання рівня знань, умінь та навичок, розширення кількості підсумкових балів до 100.

Оцінка за кожний змістовий модуль включає бали за поточну роботу студента на практичних та лабораторних заняттях, за виконання індивідуальних завдань, за модульну контрольну роботу. Виконання модульних контрольних робіт здійснюється в електронному вигляді. Модульний контроль знань студентів здійснюється після завершення вивчення навчального матеріалу змістового модуля.

У процесі оцінювання навчальних досягнень студентів застосовуються такі методи:

- *Методи усного контролю*: індивідуальне опитування, фронтальне опитування, співбесіда, залік.
- *Комп'ютерного контролю:* програми-емулятори.
- *Методи самоконтролю:* уміння самостійно оцінювати свої знання, самоаналіз.

Кількість балів за роботу з теоретичним матеріалом, на практичних заняттях, під час виконання самостійної роботи залежить від дотримання таких вимог:

- систематичність відвідування занять;
- своєчасність виконання навчальних і індивідуальних завдань;
- повний обсяг їх виконання;
- якість виконання навчальних і індивідуальних завдань;
- самостійність виконання;
- творчий підхід у виконанні завдань;
- ініціативність у навчальній діяльності;
- виконання тестових завдань.

Контроль успішності студентів з урахуванням поточного і підсумкового оцінювання здійснюється відповідно до навчально-методичної карти дисципліни, де зазначено види контролю і кількість балів за видами. Систему рейтингових балів для різних видів контролю та порядок їх переведення у національну (4-бальну) та європейську (ECTS) шкалу подано нижче у таблицях.

Розрахунок рейтингових балів за видами поточного (модульного) контролю

Вид діяльності студента	Максимальна к-сть балів за одиницю	Модуль 1		Модуль 2	
		кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів
Відвідування лекцій	1	3	3	3	3
Відвідування семінарських занять	1				
Відвідування практичних занять	1	3	3	2	2
Відвідування лабораторних занять	1	3	3	2	2
Робота на семінарському занятті	10				
Робота на практичному занятті	10	3	30	2	20
Лабораторна робота (в тому числі допуск, виконання, захист)	10	3	30	2	20
Виконання завдань для самостійної роботи	5	2	10	2	10
Виконання модульної роботи	25	1	25	1	25
Виконання ІНДЗ	20				
	Разом	–	104	–	82
Максимальна кількість балів: 186					
Розрахунок коефіцієнта: 186/100=1,86					

Завдання для самостійної роботи та критерії її оцінювання

Самостійна робота є видом поза аудиторної індивідуальної діяльності студента, результати якої використовуються у процесі вивчення програмового матеріалу навчальної дисципліни та містить результати дослідницького пошуку, відображає певний рівень його навчальної компетентності.

Перелік тем та оцінювання самостійної роботи студента

№ з/п	Назва теми	Кількість годин	Бали
Змістовий модуль 1. Методи тестування на проникнення		38	10
1	Атаки на паролі • хеші паролів; • мистецтво ручного вгадування паролів; • атаки на хеш.	38	10
Змістовий модуль 2. Прикладні аспекти етичного хакінгу		42	10
2	Експлуатація з використанням атак на стороні клієнта: • експлуатація клієнтів; • огляд можливостей експлуатації браузера.	42	10
	Разом	80	20

Критерії оцінювання самостійної роботи студента

№ п/п	Критерії оцінювання роботи	Максимальна кількість балів за кожним критерієм
1	Критичний аналіз суті та змісту першоджерел. Виклад фактів, ідей, результатів досліджень в логічній послідовності. Аналіз сучасного стану дослідження проблеми, розгляд тенденцій подальшого розвитку даного питання.	2 бали
2	Доказовість висновків, обґрунтованість власної позиції, пропозиції щодо розв'язання проблеми, визначення перспектив дослідження	2 бали
3	Дотримання вимог щодо технічного оформлення	1 бал
	Разом	5 балів

Форми проведення модульного контролю та критерії оцінювання

Модульний контроль здійснюється відповідно до навчально-методичної карти дисципліни та перевіряє рівень досягнення результатів навчання студентів. Форма проведення – тест, що складається 3 комплексних запитань.

Модульна контрольна робота оцінюється у 25 балів.

Форми проведення семестрового контролю та критерії оцінювання

Семестрове (підсумкове) оцінювання здійснюється у формі заліку, умовою отримання якого є отриманням студентом 60 балів (з врахуванням коефіцієнту) за результатами поточного контролю.

Орієнтовний перелік питань для самоконтролю

1. Основні терміни тестування на проникнення.
2. Хто такі хакери та етичні хакери?
3. Що роблять справжні хакери?
4. Методології тестування на проникнення: OSTMM та ISSAF.
5. Управління проектами проникнення.
6. Огляд інструментів злому.
7. Законодавча база в галузі хакінгу.
8. Методи відкритої розвідки.
9. Огляд структурованих аналітичних методів.
10. Типи інформації.
11. Виявлення джерел інформації.
12. Принципи роботи пошукових ботів.
13. Оператори розширеного пошуку Google.
14. Виявлення IP-адрес.
15. Трасування маршрутів.
16. Використання Maltego.
17. Використання theHarvester.
18. Підміна зони DNS.
19. Примусове використання DNS.
20. Типи вразливостей.
21. Пошук уразливостей вручну.
22. Автоматизований пошук уразливостей.
23. Інструменти аналізу вразливостей.
24. Використовувати бази даних паролів для підбору.
25. Google для тестів на проникнення.
26. Локальні та віддалені експлойти.

27. Особливості фреймворка Metasploit.
28. Атака людина по середині.
29. Онлайн і офлайн атаки на паролі.
30. Ручний підбір паролів.
31. Проведення атаки на хеші.
32. Робота з третіми особами.
33. Визначення соціальної інженерії.
34. Типова структура веб-додатків.
35. Загальні веб-уразливості.
36. Проекти OWASP.
37. Огляд фреймворка з тестування OWASP.
38. Google Hacking Database (GHDB).
39. Засоби тестування веб-безпеки.
40. Підтримка методів доступу.
41. Використання Meterpreter.
42. Етичний злом.
43. Kali Linux.
44. Сканери портів.
45. Сканери вразливостей.

Шкала відповідності оцінок

Рейтингова оцінка	**Сума балів за всі види навчальної діяльності**	**Значення оцінки**
A	90-100	Відмінно — відмінний рівень знань (умінь) в межах обов'язкового матеріалу з, можливими, незначними недоліками
B	82-89	Дуже добре — достатньо високий рівень знань (умінь) в межах обов'язкового матеріалу без суттєвих (грубих) помилок
C	75-81	Добре — в цілому добрий рівень знань (умінь) з незначною кількістю помилок
D	69-74	Задовільно — посередній рівень знань (умінь) із значною кількістю недоліків, достатній для подальшого навчання або професійної діяльності
E	60-68	Достатньо — мінімально можливий допустимий рівень знань (умінь)
FX	35-59	Незадовільно з можливістю повторного складання — незадовільний рівень знань, з можливістю повторного перескладання за умови належного самостійного доопрацювання
F	1-34	Незадовільно з обов'язковим повторним вивченням курсу — досить низький рівень знань (умінь), що вимагає повторного вивчення дисципліни

7. Навчально-методична картка дисципліни

Разом: 120 год., лекції – 12 год., практичні заняття – 10 год., лабораторні роботи – 10 год., модульний контроль – 8 год., самостійна робота – 80 год.

Модулі (назви, бали)	**Змістовий модуль 1. Методи тестування на проникнення (104 балів)**			**Змістовий модуль 2. Прикладні аспекти етичного хакінгу (82 бали)**	
Лекції (теми, бали)	Вступ до тестування проникнення (1 бали)	Збір інформації (1 бали)	Аналіз вразливостей (1 бали)	Експлуатація веб-додатків (2 бал)	Соціальна інженерія та підтримка доступу (1 бал)
Практичні, семінарські заняття (теми, бали)	Google для тестів на проникнення (11 балів)	Структуровані підходи до збору інформації (11 балів)	Методики оцінки вразливості (11 балів)	Огляд інструментів етичного злому (11 бали)	Інструментарій для соціальної інженерії (11 балів)
Лабораторні заняття (теми, бали)	Методології тестування на проникнення: OSTMM і ISSAF (11 балів)	Інструменти аналізу вразливостей (11 балів)	Збір технічної інформації (11 балів)	Metasploit фреймворк (11 балів)	Використання експлойтів (11 бали)
Самостійна робота	Самостійна робота (10 балів)			Самостійна робота (10 балів)	
Поточний контроль (вид, бали)	Модульна контрольна робота 1 (25 балів)			Модульна контрольна робота 2 (25 балів)	
Підсумковий контроль (вид, бали)	залік				

8. Рекомендовані джерела

Основна (базова):

1. Rafay Baloch. Ethical Hacking and Penetration Testing Guide, 2014.

2. Georgia Weidman. Penetration testing, A Hands-On Introduction to Hacking, San Francisco, ISBN:978-1-59327-564-8.

Додаткова

1. Article EXIN Ethical Hacking Foundation (www.exin.com).

2. Stuart McClure, Joel Scambray, George Kurtz. Hacking Exposed 7: Network Security Secrets & Solutions, ISBN: 978-0071780285.

9. Додаткові ресурси

1. OS Kali Linux.