МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ЗАТВЕРДЖУЮ
Декан факультету комп'ютерних інформаційних технологій
_____Ігор ЯКИМЕНКО
«__» _____ 20__ р.

ЗАТВЕРДЖУЮ
Проректора з науково-педагогічної роботи
_____Віктор ОСТРОВЕРХОВ
«__» _____ 20__ р.

РОБОЧА ПРОГРАМА

з дисципліни

«СОЦІАЛЬНА ІНЖЕНЕРІЯ»

ступінь вищої освіти - **бакалавр**
галузь знань - **12 - «Інформаційні технології»**
спеціальність – **125 - «Кібербезпека»**
освітньо-професійна програма – **«Кібербезпека»**

Кафедра кібербезпеки

Форма навчання	Курс	Семестр	Лекції (год.)	Лабор. заняття (год.)	ІРС (год.)	Тренінг (год.)	СРС (год.)	Разом (год.)	Залік (сем.)
Денна	4	7	26	12	2	6	104	150	7

30.08.2024

Тернопіль – 2024

Робочу програму склала викладач кафедри кібербезпеки Давлетова Аліна Ярославівна

Робоча програма затверджена на засіданні кафедри кібербезпеки
протокол № 1 від 26.08.2024р.

Завідувач кафедри кібербезпеки Василь ЯЦКІВ

Розглянуто та схвалено групою забезпечення спеціальності кібербезпека та захист інформації, протокол № 1 від 30.08.2024 р.

Голова групи забезпечення
спеціальності кібербезпека Василь ЯЦКІВ

Гарант ОП Михайло КАСЯНЧУК

СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

1. Опис дисципліни

Дисципліна «Соціальна інженерія»	**Галузь знань, спеціальність, СВО**	**Характеристика навчальної дисципліни**
Кількість кредитів – 5	Галузь знань 12 «Інформаційні технології»	Статус дисципліни - вибіркова Мова навчання - українська
Кількість залікових модулів – 3	Спеціальність 125 «Кібербезпека»	Рік підготовки: 4 Семестр: 7
Кількість змістових модулів – 3	Ступінь вищої освіти – бакалавр	Лекції: 26 год. Лабораторні заняття: 12 год.
Загальна кількість годин – 150		Самостійна робота: 104 год.. Тренінг: 6 год. Індивідуальна робота: 2 год.
Тижневих годин – 10, з них аудиторних – 3		Вид підсумкового контролю – залік

2. Мета й завдання вивчення дисципліни

2.1. Мета дисципліни

Формування у студентів цілісного уявлення про психологічні аспекти, методи та засоби соціальної інженерії. Отримання знань та умінь необхідних для успішної боротьби з атаками, які використовують методи соціальної інженерії.

2.2. Завдання вивчення дисципліни

Основне завдання дисципліни дати студентам теоретичну підготовку з основ соціальної інженерії та формування навиків дослідження причин, що спонукають людину до конкретної дії або прийняття рішення, обставин та середовища, що впливають на формування її системи цінностей. У результаті вивчення навчальної дисципліни студент повинен:

знати:

- основні методи та техніки соціальної інженерії,
- психологічні аспекти соціальної інженерії;
- основні етапи атаки на людину;
- інструменти та засоби соціального інженера;
- технології та засоби захисту від соціальних атак, включаючи навчання користувачів та встановлення політик безпеки

вміти:

- виявляти ознаки соціоінженерних атак та інцидентів;
- вживати заходи щодо запобігання атакам соціальної інженерії, включаючи навчання персоналу засобам ідентифікації та виявлення атак.
- аналізувати інциденти та розробляти стратегії захисту від них.
- використовувати методи соціального інженерінгу як частину етичного витоку інформації, щоб виявити слабкі місця в системах безпеки та сприяти їх вдосконаленню.

Завдання лекційних занять.

Завдання лекційних занять включає вивчення основних теоретичних понять соціальної інженерії, методів аналізу поведінки та психологічних аспектів, які використовуються для виявлення та запобігання соціально-інженерним загрозам, зокрема їх застосування в сучасному інформаційному середовищі для забезпечення кібербезпеки та захисту даних.

Завдання проведення лабораторних занять.

Проведення практичних занять забезпечує формування у студентів практичних навичок аналізу соціально-інженерних атак, розуміння етичних аспектів соціальної інженерії, виявлення та запобігання соціально-інженерним загрозам.

3. Програма навчальної дисципліни

Змістовий модуль 1. Збір та обробка інформації у соціальній інженерії.

Тема 1. Концепції та принципи соціальної інженерії.

1. Історія та розвиток соціальної інженерії. 2. Основні поняття та визначення. 3. Етичні аспекти соціальної інженерії.

Література: 1-10.

Тема 2. Психологія соціальної інженерії.

1. Типологія особистості. 2. Психологічні методи впливу на людей. 3. Нейролінгвістичне програмування.

Література: 1-10.

Тема 3. Основні схеми впливу соціальної інженерії.

1. Вплив та переконання. 2. Інженерія довіри та авторитету.3. Маніпуляція. 4. Вплив на громадську думку. 5. Зміна реальності.

Література: 1-10.

Тема 4. Методи та джерела для збору інформації.

1. Технічні методи збору даних. 2. Не технічні методи збору даних. 3. Збір даних з відкритих джерел. 4. Інсайдинг.

Література: 1-10.

Тема 5. Визначення цілі атаки соціального інженера.

1. Основні галузі застосування соціальної інженерії. 2. Інформація, як предмет захисту. 3. Вразливі категорії людей та організацій. 4. Персонал вищого рівня та фінансовий персонал. 5. Літні люди.

Література: 1-10.

Змістовий модуль 2. Наступальна соціальна інженерія.

Тема 6. Основні етапи соціоінженерної атаки.

1. Принципи та етапи планування атаки. 2. Активна та пасивна розвідка. 3. Юридичні аспекти претекстінгу.

Література: 1-10.

Тема 7. Методи та інструменти соціальної інженерії.

1. Наживка. 2. Залякування. 3. Попереднє тестування. 4. Фішинг. 5. Фізичні засоби. 6. Програмні засоби. 7. Атака на людину.

Література: 1-10.

Змістовий модуль 3. Організація захисту від атак з використанням соціальної інженерії

Тема 8. Профілактика та пом'якшення наслідків атак соціальної інженерії.

1. Навчання ідентифікувати атаки соціальної інженерії. 2. Оновлення програмного забезпечення. 3. Навчання з аудиту соціальної інженерії.

Література: 1-10.

Тема 9. Аудит соціальної інженерії.

1. Створення культури поінформованості про особисту безпеку. 2. Усвідомлення цінності інформації.

Література: 1-10.

Тема 10. Стратегія захисту від атак.

1. Захист від соціальної інженерії. 2. Навчання персоналу. 3. Віддзеркалення атаки.

4. Структура залікового кредиту дисципліни

	Кількість годин					
	Лекції	Лабор. заняття	СРС	ІРС	Тренінг	Контрольні заходи
Змістовий модуль 1. Збір та обробка інформації у соціальній інженерії.						
Тема 1. Концепції та принципи соціальної інженерії	2		10	1	2	Поточне опитування
Тема 2. Психологія соціальної інженерії.	2	2	10			
Тема 3. Основна схема впливу соціальної інженерії.	2		10			
Тема 4. Методи та джерела для збору інформації	2	2	10			
Тема 5. Визначення цілі атаки соціального інженера.	2	2	12			
Змістовий модуль 2. Наступальна соціальна інженерія.						

Тема 6. Основні етапи соціоінженерної атаки	4	2	10	1	2	Поточне опитування
Тема 7. Методи та інструменти соціальної інженерії.	4	2	10			
Змістовий модуль 3. Організація захисту від атак з використанням соціальної інженерії						
Тема 8. Профілактика та пом'якшення наслідків атак соціальної інженерії	2		10		2	Поточне опитування
Тема 9. Аудит соціальної інженерії	2		10			
Тема 10. Стратегія захисту від атак	4	2	12			
Разом	**26**	**12**	**104**	**2**	**6**	

5. Тематика лабораторних занять.

Лабораторна робота №1

Тема: Ідентифікація атак із застосуванням соціальної інженерії.

Мета: Навчитися визначати основні прийоми соціально-інженерних атак.

Питання для обговорення: 1. Основні терміни. 2. Ознаки поведінки соціального інженера. 3. Психологічні типи особистості. 4. Типові психологічні методи впливу.

Література: 1-10.

Лабораторна робота №2

Тема: Інструменти збору інформації.

Мета: Отримати навики збору відкритої інформації.

Питання для обговорення: 1. Інструменти збору інформації в Інтернеті. 2. Отримання особистих даних для доступу до соціальних мереж з використанням Social Engineering Toolkit (SET) та Credential Harvest method. 3. Принципи OSINT. 4. Аналіз та інтерпретація інформації.

Література: 1-10.

Лабораторна робота №3

Тема: Процес визначення цілей соціоінженерної атаки

Мета: Отримати розуміння основних кроків та методик, які використовуються для визначення цілей соціальних інженерів.

Питання для обговорення: 1. Потенційна ціль. 2. Фактори впливу на певні категорій осіб. 3. Вразливі категорії людей та організацій. 4. Специфіка атак.

Література: 1-10.

Лабораторна робота №4

Тема: Визначення атаки соціальної інженерії.

Мета: Отримання навиків виявлення фішингових веб сайтів.

Питання для обговорення: 1. Використання програмного забезпечення Netcraft та PhishTank. 2. Дослідження веб сайтів. 3. Ознаки атак. 4. Визначення етапів атаки.

Література: 1-10.

Лабораторна робота №5

Тема: Створення додаткового навантаження використовуючи SET.

Мета: Навчитися виявляти атаки типів Trojan та Backdoor.

Питання для обговорення: 1. Створення сервера. 2. Організація атаки мережі типу Backdoor. 3. Характеристика атаки типу Trojan. 4. Спостереження за системою.

Література: 1-10.

Лабораторна робота №6

Тема: Комплексна стратегія запобігання атакам соціальної інженерії.

Мета: Навчитися вибирати та застосовувати способи та засоби захисту від атак соціальної інженерії.

Питання для обговорення: 1. Основна тактика соціальної інженерії. 2. Методи протидії. 3. Стратегія запобігання атак соціальної інженерії. 4. Захист від соціотехнічних атак.

Література: 1-10.

6. Самостійна робота

Самостійна робота студентів (СРС) з курсу «Соціальна інженерія» є однією з обов'язкових складових частин модуля залікового кредиту. Виконується у вигляді презентації тематичного звіту, підготовленого студентами самостійно на основі сформованого завдання. Метою виконання СРС є оволодіння навичками ідентифікації та протистояння атакам соціальних інженерів. Орієнтовна

тематика досліджень:

1. Історія розвитку соціальної інженерії.
2. Основна схема впливу соціальної інженерії.
3. Соціальне програмування та його відмінність від соціальної інженерії.
4. Основні галузі застосування соціальної інженерії.
5. Збір інформації про об'єкт.
6. Типи атак соціальної інженерії.
7. Захист від соціальної інженерії.
8. Приклади соціального програмування.
9. Психологічні засади соціального програмування.
10. Соціальні фаєрволи.
11. Аспекти психологічної підготовки соціальних хакерів.
12. Типологія особистості.
13. Трансактний аналіз.
14. Техніки НЛП.
15. Етична складова соціальної інженерії.
16. Витік інформації.
17. Наслідки соціоінженерних атак.
18. Технології захисту від соціальних інженерів.
19. Принципи оцінки ефективності засобів захисту.

7 . Організація та проведення тренінгу з дисципліни.

Порядок проведення тренінгу:

1. Вступна частина проводиться з метою ознайомлення студентів з темою тренінгу.

2. Організаційна частина полягає у створенні робочого настрою у колективі студентів.

3. Практична частина реалізується шляхом виконання завдань з певних проблемних питань теми тренінгу.

4. Підведення підсумків. Обговорення результатів виконаних завдань. Обмін думками з питань, що виносяться на тренінг.

Тематика тренінгу: «Соціальна інженерія - виклик сьогодення.»

Мета тренінгу: надати розуміння сучасних методів соціальної інженерії, їх потенційних загроз та стратегій захисту, а також підвищити обізнаність про актуальні виклики у сфері кібербезпеки, що виникають внаслідок цих методів.

Завдання тренінгу: презентувати результати аналізу і дослідження методів соціальної інженерії, їх впливу на безпеку та стратегії протидії.

Орієнтовна тематика завдання тренінгу:

1. Погляд у світ соціальної інженерії.
2. Психологічні принципи, що використовуються в соціальній інженерії.
3. Нейролінгвістичне програмування (НЛП).
4. Переповнення буфера людини.
5. Основи впливу та переконання.
6. Підміна реальності.
7. Вилучення інформації.
8. Розуміння принципів атаки соціального інженера.
9. Тактика впливу.
10. Маніпуляція в соціальній інженерії.
11. Тематичні дослідження: аналіз діяльності соціального інженера.
12. Наслідки атак соціальної інженерії.
13. Засоби захисту від атак соціальної інженерії.
14. Культура поінформованості про особисту безпеку.
15. Усвідомлення цінності інформації.
16. Програмні засоби соціальної інженерії: Maltego.
17. Програмні засоби соціальної інженерії: Social engineer toolkit (SET).
18. Програмні засоби атак соціальної інженерії: Google.
19. Технічні засоби атак соціальної інженерії: Caller ID spoofing.

8. Методи навчання.

У навчальному процесі застосовуються: лекції, в тому числі з використання мультимедійного проектора та інших ТЗН; практичні роботи, індивідуальні заняття; робота в Інтернет.

9. Засоби оцінювання та методи демонстрування результатів навчання.

У процесі вивчення дисципліни «Соціальна інженерія» використовуються наступні методи оцінювання та методи демонстрування результатів навчання:

- поточне тестування та опитування;
- підсумкове тестування за кожним змістовним модулем;
- оцінювання виконання лабораторних робіт;
- оцінювання тренінгів;
- оцінювання результатів самостійної роботи.

10. Критерії, форми поточного та підсумкового контролю

Підсумковий бал (за 100 – бальною шкалою) з дисципліни «Соціальна інженерія» визначається як середньозважена величина, в залежності від питомої ваги кожної складової залікового кредиту:

Модуль 1		Модуль 2	Модуль 3
40%	40%	5%	15%
Поточне оцінювання	Модульний контроль 1	Тренінги	Самостійна робота
Середнє арифметичне з оцінок, отриманих за теоретичне опитування на заняттях (1-10 теми)	Середнє арифметичне оцінок, отриманих за виконання та захист лабораторних робіт 1-6	Середнє арифметичне з оцінок, отриманих за виконання та презентацію 1 завдання тренінгу	Середнє арифметичне оцінок, отриманих за виконання 1 завдання самостійної роботи (реферат, есе, тощо) та їх презентацію.

Шкала оцінювання:

За шкалою університету	**За національною шкалою**	**За шкалою ECTS**
90-100	відмінно	**A** (відмінно)
85-89	добре	**B** (дуже добре)
75-84		**C** (добре)
65-74	задовільно	**D (**задовільно**)**
60-64		**E** (достатньо)
35-59	незадовільно	**FX** (незадовільно з можливістю повторного складання)
1-34		**F** (незадовільно з обов'язковим повторним курсом)

11. Інструменти, обладнання та програмне забезпечення, використання яких передбачає навчальна дисципліна

№	Найменування	Номер теми
1	Мультимедійний проектор та проєкційний екран	1-10
2	Персональні комп'ютери	1-10
3	Наявність доступу до мережі Інтернет	1-10
4	Комунікаційне програмне забезпечення (Zoom) для проведення занять у режимі он-лайн (за необхідності)	1-10
5	Комунікаційна навчальна платформа (Moodle) для організації дистанційного навчання (за необхідності)	1-10
6	Спеціалізовані програмні продукти Netcraft, PhishTank	1-10

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1. Соціальна інженерія. Навчальний посібник. В. Петрик, В. Курганевич та ін. Київ, 2019 – 200 с.

2. Кевін Митник, Роберт Вемосі Мистецтво залишатись непоміченим, Наш Формат, 2020.- 278 с.

3. Кіт Мелтон, Роберт Уоллес. Секретна інструкція ЦРУ з техніки обманних трюків та введення в оману, 2023.- 298с.
4. Роберт Чалдіні, Дуглас Кенрика, Стівен Нейберг Соціальна психологія, вид. 5-те, 2021.- 848с.
5. Роберт Чалдині Психологія впливу. Оновлено та доповнено, КСД, 2022.- 608с.
6. Michael Bazzell. Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information Paperback – 2021- 666 p.
7. Ethical Hacking: 3 in 1- Beginner's Guide+ Tips and Tricks+ Advanced and Effective measures of Ethical Hacking Paperback – July 23, 2020 – 456 p.
8. Gray Hat Hacking The Ethical Hackers Handbook Fourth Edition. [Електронний ресурс] – Режим доступу: https://www.booksfree.org/gray-hat-hacking-the-ethical-hackers-handbook-fourth-edition-pdf/
9. Joe Gray Practical Social Engineering: A Primer for the Ethical Hacker. [Електронний ресурс] – Режим доступу: https://ebin.pub/practical-social-engineering-a-primer-for-the-ethical-hacker-171850098x-9781718500983.html
10. Christopher Hadnagy Social Engineering The Art of Human Hacking . [Електронний ресурс] – Режим доступу: https://www.booksfree.org/social-engineering-the-art-of-human-hacking-by-christopher-hadnagy-pdf/