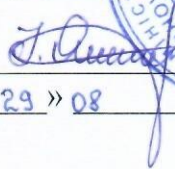


МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ЗАТВЕРДЖУЮ
Декан факультету комп'ютерних
інформаційних технологій


Ігор ЯКИМЕНКО
«29» 08 2025 р.



ЗАТВЕРДЖУЮ
Проректора з науково-педагогічної
роботи

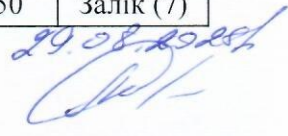

Віктор ОСТРОВЕРХОВ
«29» 08 2025 р.

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 /екзамен (семестр)
Денна	4	7	30	14	3	6	97	150	Залік (7)

29.08.2025

Тернопіль – 2025

Робочу програму склала викладач кафедри кібербезпеки Аліна ДАВЛЕТОВА

Робоча програма затверджена на засіданні кафедри кібербезпеки
протокол № 1 від 26.08.2025р.

Завідувач кафедри кібербезпеки



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: 30 год. Лабораторні заняття: 14 год.
Загальна кількість годин – 150		Самостійна робота: 97 год.. Тренінг: 6 год. Індивідуальна робота: 3 год.
Тижневих годин – 10, з них аудиторних – 3		Вид підсумкового контролю – залік

2. Мета й завдання вивчення дисципліни

2.1. Мета вивчення дисципліни

Формування 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 здобувачам 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 здобувач 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 проведення лекційних занять. Лекційні заняття включають 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 здобувачів 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.

Тема 2. Психологія соціальної інженерії.

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

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.

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.

Змістовий модуль 2. Наступальна соціальна інженерія.

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.

Тема 6. Основні етапи соціоінженерної атаки.

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

Тема 7. Методи соціальної інженерії

1. Наживка. 2. Залякування. 3. Попереднє тестування. 4. Фішинг.

Тема 8. Інструменти соціальної інженерії.

1. Фізичні засоби. 2. Програмні засоби. 3. Атака на людину.

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

Тема 9. Профілактика та пом'якшення наслідків атак соціальної інженерії.

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

Тема 10. Аудит соціальної інженерії.

1. Створення культури поінформованості про особисту безпеку. 2. Усвідомлення цінності інформації. 3. Аудит безпеки персоналу та процесів від соціальної інженерії.

Тема 11. Стратегія захисту від соціоінженерних атак.

1. Захист від соціальної інженерії. 2. Навчання персоналу. 3. Віддзеркалення атаки. 4. Аналіз реакцій. 5. Вдосконалення захисту.

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		8	1	2	Поточне опитування
Тема 2. Психологія соціальної інженерії.	4	2	8			
Тема 3. Основні схеми впливу соціальної інженерії.	2	2	9			
Тема 4. Методи та джерела для збору інформації	4	2	9			
Змістовий модуль 2. Наступальна соціальна інженерія.						
Тема 5. Визначення цілі атаки соціального інженера.	2	2	9	1	2	Поточне опитування
Тема 6. Основні етапи соціоінженерної атаки	4	2	9			
Тема 7. Методи соціальної інженерії.	2	2	9			
Тема 8. Інструменти соціальної інженерії.	2		9			
Змістовий модуль 3. Організація захисту від атак з використанням соціальної інженерії						
Тема 9. Профілактика та пом'якшення наслідків атак соціальної інженерії	2		9	1	2	Поточне опитування
Тема 10. Аудит соціальної інженерії	2		9			
Тема 11. Стратегія захисту від соціоінженерних атак.	4	2	9			

Разом	30	14	97	3	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.

Лабораторна робота №2

Тема: Схеми впливу у соціальній інженерії.

Мета: Навчитися визначати основні методи та засоби впливу соціоінженерних атак.

Питання для обговорення: 1. Психологічні методи впливу на людей. 2. Нейролінгвістичне програмування. 3. Вплив. 4. Переконавання. 5. Довіра та авторитет. 6. Маніпуляція.

Лабораторна робота №3

Тема: Інструменти збору інформації.

Мета: Отримати навички збору та аналізу інформації з відкритих джерел.

Питання для обговорення: 1. Інструменти збору інформації в Інтернеті. 2. Інструменти соціальної інженерії для імітації атак. 3. Принципи OSINT. 4. Аналіз та інтерпретація інформації.

Лабораторна робота №4

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 категорії осіб. 3. Вразливі категорії людей та організацій. 4. Специфіка атак.

Лабораторна робота №5

Тема: Визначення атаки соціальної інженерії.

Мета: Отримання навичок визначення етапів атак соціальної інженерії.

Питання для обговорення: 1. Збір та вилучення інформації. 2. Привід, створення легенди. 3. Ознаки атак. 4. Визначення етапів атаки.

Лабораторна робота №6

Тема: Оцінка вразливостей методами соціальної інженерії.

Мета: Дослідити та оцінити вразливості організаційної або інформаційної системи шляхом застосування методів соціальної інженерії.

Питання для обговорення: 1. Організація претекстингу. 2. Комунікаційний канал для атаки. 3. Фіктивна особа. 4. Сценарій. 5. Вразливості користувачів і систем.

Лабораторна робота №7

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.

6. Організація та проведення тренінгу з дисципліни.

Порядок проведення тренінгу:

1. Вступна частина проводиться з метою ознайомлення з темою тренінгу.
2. Організаційна частина полягає у створенні робочого настрою у колективі.
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: сформувати розуміння механізмів застосування сучасних методів соціальної інженерії, їх впливу на інформаційну та кібербезпеку, а також ознайомити зі стратегіями захисту.

Завдання тренінгу: презентувати результати аналізу і дослідження методів соціальної інженерії, їх впливу на безпеку та стратегії протидії; надати здобувачам знання про потенційні

загрози та ефективні методи захисту; щодо актуальних викликів у сфері кібербезпеки, пов'язаних із соціальною інженерією. Кожен здобувач обирає одну тему із запропонованого переліку або погоджує власну в межах курсу, готує коротку доповідь із висвітленням сутності проблеми, прикладом застосування методу соціальної інженерії та його наслідками для подальшої колективної дискусії та обміну думками.

Орієнтовна тематика завдання тренінгу:

1. Погляд у світ соціальної інженерії.
2. Психологічні принципи, що використовуються в соціальній інженерії.
3. Нейролінгвістичне програмування (НЛП).
4. Переповнення «інформаційного буфера» користувача.
5. Основи впливу та переконання у соціальній інженерії.
6. Підміна реальності та маніпулятивні технології.
7. Методи вилучення інформації з відкритих джерел.
8. Принципи атак соціального інженера.
9. Тактики впливу на цільову аудиторію.
10. Маніпуляція в соціальній інженерії.
11. Тематичні кейси діяльності соціальних інженерів.
12. Наслідки атак соціальної інженерії для організацій та людей.
13. Засоби захисту від атак соціальної інженерії.
14. Культура поінформованості про кібербезпеку.
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.
20. Актуальні виклики кібербезпеки, пов'язані з соціальною інженерією.

7. Тематика самостійної роботи

Самостійна робота з курсу «Соціальна інженерія» є однією з обов'язкових складових частин модуля залікового кредиту. Виконується у вигляді презентації тематичного звіту, підготовленого здобувачами самостійно на основі сформованого завдання.

Мета: сформувати у здобувачів практичні вміння та теоретичні знання з ідентифікації, аналізу та протидії атакам соціальних інженерів, а також розвинути навички самостійного опрацювання літератури, критичного мислення та презентації результатів.

Завдання:

1. Обрати тему із запропонованого переліку або узгодити власну тему у межах курсу.
2. Опрацювати навчальні та наукові джерела з обраної теми.
3. Підготувати презентацію, яка включає: короткий теоретичний огляд теми; приклади практичної реалізації або застосування; висновки та узагальнення.

4. Представити результати у формі доповіді та взяти участь у обговоренні з колегами.

Орієнтовна тематика:

1. Історія розвитку соціальної інженерії.
2. Основні схеми та моделі впливу соціальної інженерії.
3. Соціальне програмування та відмінності від соціальної інженерії.
4. Галузі застосування соціальної інженерії (корпоративна безпека, онлайн-середовище, державні структури).
5. Методи збору інформації про об'єкт (OSINT, соціальні мережі, інструменти Maltego/SET).
6. Типи атак соціальної інженерії (фішинг, вішинг, смс-атаки, BEC тощо).
7. Методи захисту від атак соціальної інженерії.
8. Приклади соціального програмування у сучасних інформаційних системах.
9. Психологічні засади соціального програмування та впливу.
10. Соціальні «фаєрволи» та механізми обмеження впливу на користувачів.
11. Психологічна підготовка соціальних хакерів.

12. Типологія особистості та її використання в атаках.
13. Трансактний аналіз у контексті маніпуляцій та впливу.
14. Техніки нейролінгвістичного програмування (НЛП) у соціальній інженерії.
15. Етичні та правові аспекти соціальної інженерії.
16. Витік інформації та інциденти безпеки.
17. Наслідки соціоінженерних атак для організацій і користувачів.
18. Сучасні технології захисту від атак соціальних інженерів.
19. Принципи оцінки ефективності засобів захисту та навчання користувачів.
20. Актуальні виклики та тенденції у сфері соціальної інженерії та кібербезпеки.

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. Політика оцінювання

Політика щодо дедлайнів і перескладання. Для всіх видів навчальних завдань і контрольних заходів встановлюються чіткі дедлайни. Роботи, здані із порушенням термінів без поважних причин, оцінюються на нижчу оцінку (-10 балів). Перескладання проводиться у встановленому порядку.

Політика щодо академічної доброчесності. Студент зобов'язаний виконувати усі роботи та завдання самостійно. Під час контрольного заходу він може користуватися лише дозволеними допоміжними матеріалами або засобами; йому забороняється в будь-якій формі обмінюватися інформацією з іншими студентами, а також використовувати, розповсюджувати або збирати варіанти чужих робіт чи контрольних завдань.

Політика щодо відвідування. За об'єктивних причин (наприклад, карантин, воєнний стан, хвороба, закордонне стажування) навчання може відбуватись у дистанційній формі за погодженням із керівником курсу та з дозволу дирекції факультету.

11. 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	Тренінги	Самостійна робота
Середнє арифметичне оцінок, отриманих за виконання та захист лабораторних робіт 1-7	Середнє арифметичне оцінок, отриманих за поточне опитування та підсумкове модульне тестування за темами 1-11.	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.

Виконання лабораторних робіт:

90–100 балів – робота виконана самостійно, без помилок, усі етапи задокументовано, правильне використання інструментів.

75–89 балів – виконання із незначними помилками, що не вплинули на результат; часткова потреба в підказках.

60–74 бали – виконання із суттєвими помилками; поверхнєве розуміння завдань.

1–59 балів – робота не виконана або результат неправильний; відсутність навичок.

Поточне опитування:

90–100 балів – повне володіння матеріалом, аргументовані й логічні відповіді, глибоке

розкриття змісту.

75–89 балів – загалом повне володіння матеріалом, але окремі відповіді поверхневі або з незначними неточностями.

65–74 бали – знання основного змісту без достатньої глибини та аргументації, суттєві неточності.

60–64 бали – фрагментарне володіння матеріалом, недостатнє розкриття питань.

1–59 балів – відсутність знань, нездатність розкрити зміст теоретичних питань.

Тренінг, самостійна робота:

90–100 балів – повне володіння матеріалом, аргументоване застосування знань, правильне виконання завдань, наявність елементів власного дослідження, творчий підхід.

75–89 балів – здебільшого правильне виконання, незначні помилки, достатньо аргументоване використання матеріалу, частково присутні елементи власного дослідження.

65–74 бали – розв'язання завдань з помилками, недостатня аргументація, поверхневе опрацювання теми, обмежена самостійність.

60–64 бали – часткове або фрагментарне виконання завдань, відсутність повного обґрунтування, мінімальний авторський внесок.

1–59 балів – завдання практично не виконано, повністю неправильне розв'язання, відсутність дослідницького або творчого підходу.

Підсумкове модульне тестування:

90–100 балів – правильно виконано 90–100% завдань тесту.

75–89 балів – правильно виконано 75–89% завдань тесту.

60–74 бали – правильно виконано 60–74% завдань тесту.

1–59 балів – правильно виконано менше 60% завдань тесту.

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)

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

№	Найменування	Тема
1	Мультимедійний проектор та проєкційний екран, персональні комп'ютери	1-10
2	Наявність доступу до мережі Інтернет	1-10
3	Комунікаційне програмне забезпечення для проведення занять у режимі он-лайн (Zoom) та організації дистанційного навчання(Moodle) (за необхідності)	1-10
4	Електронний варіант лекцій та інструкції до виконання лабораторних робіт	1-10
5	Спеціалізовані програмні продукти та сервіси Maltego, Netcraft, PhishTank, Social Engineering Toolkit, Credential Harvest method, WhoIs, TinEye, InVid, Social Blade	1-10

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1. Яцків В.В., Давлетова А.Я. Опорний конспект лекцій з дисципліни «Соціальна інженерія» для студентів освітньо-кваліфікаційного рівня «бакалавр» галузі знань: 12 – Інформаційні технології. – Тернопіль 2025. – 54.

2. Соціальна інженерія. Навч. посібник. В. Петрик, В. Курганевич та ін. Київ, 2019 – 200 с.

3. Митник К., Вемосі Р. Мистецтво залишатись непоміченим, Наш Формат, 2020.- 278 с.

4. Кіт Мелтон, Роберт Уоллес. Секретна інструкція ЦРУ з техніки обманних трюків та введення в оману, 2023.- 298с.

5. Чалдині Р., Кенрика Д., Нейберг С. Соціальна психологія, вид. 5-те, 2021.- 848с.

6. Роберт Чалдині Психологія впливу. Оновлено та доповнено, КСД, 2022.- 608с.
7. Michael Bazzell. Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information Paperback – 2021- 666 p.
8. Ethical Hacking: 3 in 1- Beginner's Guide+ Tips and Tricks+ Advanced and Effective measures of Ethical Hacking Paperback – July 23, 2020 – 456 p.
9. 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/>
10. 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>
11. 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/>