Силабус курсу

СОЦІАЛЬНА ІНЖЕНЕРІЯ

Ступінь вищої освіти – бакалавр
Рік навчання: 4,
Семестр: 1
Кількість кредитів: 5**,**
Мова викладання: українська

Керівник курсу

ПІП	Аліна Давлетова
Контактна інформація	a.davletova@wunu.edu.ua

Опис дисципліни

Курс «Управління інформаційною безпекою» орієнтований на формування у студентів цілісного уявлення про про психологічні аспекти, методи та інстременти соціальної інженерії. Отримання знань та умінь необхідних для успішної боротьби з атаками, які використовують методи соціальної інженерії. Вивчення курсу вимагає цілеспрямованої роботи над вивченням спеціальної літератури, активної роботи на лекціях та практичних заняттях, самостійної роботи та виконання індивідуальних завдань. Метою курсу є формування комплексу знань, що включає основні теоретичні поняття соціальної інженерії, методи аналізу поведінки та психологічні техніки, які використовуються для виявлення та запобігання соціальноінженерним загрозам, зокрема їх застосування в сучасному інформаційному середовищі для забезпечення кібербезпеки та захисту даних.

Структура курсу

Години лек/пр	Тема	Результати навчання	Завдання
2/0	Концепції та принципи соціальної інженерії.	Володіти поняттями та визначеннями. Розуміти історію розвитку соціальної інженерії Усвідомлювати етичні аспекти соціальної інженерії.	Поточне опитування
2/2	Психологія соціальної інженерії.	Розуміти поняття типології особистості. Знатність визначати психологічні методи впливу на людей та інструменти нейролінгвістичного програмування.	Поточне опитування
2/0	Основні схеми впливу соціальної інженерії	Розуміти поняття вплив, переконання, маніпуляція. Розуміти принципи інженерії довіри та авторитету та механізми впливу на громадську думку.	Поточне опитування
2/2	Методи та джерела для збору інформації	Здатність здійснювати пошук інформації з відкритих джерел	Поточне опитування
2/2	Визначення цілі атаки соціального інженера	Знати галузі застосування соціальної інженерії. Розуміння інформації як предмета захисту. Вміти визначати вразливі категорії людей та організацій. Розуміти мехінізми атаки на персонал вищого рівня та фінансовий персонал, літніх людей.	Поточне опитування
4/2	Основні етапи	Розуміти принципи та етапи планування атаки.	Поточне

	соціоінженерної атаки	Володіти поняттями активна та пасивна розвідка. Усвідомлювати юридичні аспекти претекстінгу.	опитування
4/2	Методи та інструменти соціальної інженерії	Володіти основними поняттями та вміти визначати методи соціальної інженерії та розуміти мехінізми дії інструментів соціоінженерної атаки	Поточне опитування
2/0	Профілактика та пом'якшення наслідків атак соціальної інженерії	Здатність здійснювати професійну діяльність, ідентифікувати атаки соціальної інженерії, розробляти та впроваджувати політики і правила безпеки.	Поточне опитування
2/0	Аудит соціальної інженерії	Вміти ідентифікувати потенційні вразливості та ризики та розробляти заходи для їх запобігання. Здатність проводити оцінку та аналіз інцидентів.	Поточне опитування
4/2	Стратегія захисту від атак	Володіти основними поняттями. Здатність забезпечувати неперервність бізнес-процесів. Навчання персоналу.	Поточне опитування

Літературні джерела

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 Чалдини 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/

Політика оцінювання

Політика щодо дедлайнів та перескладання: Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку (-20 балів). Перескладання модулів відбувається із дозволу деканату за наявності поважних причин (наприклад, лікарняний).

Політика щодо академічної доброчесності: Списування під час контрольних робіт та екзаменів заборонені (в т.ч. із використанням мобільних девайсів).

Політика щодо відвідування: Відвідування занять є обов'язковим компонентом оцінювання, за яке нараховуються бали. За об'єктивних причин (наприклад, хвороба, міжнародне стажування) навчання може відбуватись в он-лайн формі за погодженням із керівником курсу.

Оцінювання

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 університуту	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)