



Теорія і методи соціальної інженерії в кібербезпеці  
Робоча програма навчальної дисципліни  
(Силабус)

Реквізити навчальної дисципліни

Рівень вищої освіти	<i>Другий (освітньо-професійний)</i>	
Галузь знань	11	
Спеціальність	113	
Освітня програма		
Статус дисципліни	Вибіркова	
Форма навчання	очна(денна)	
Рік підготовки, семестр	1 -(5)-курс,	
Обсяг дисципліни	5 кредитів , 150 ., (36 годин лекцій, 18 годин .(комп. практ.) , 96	
Семестровий контроль/ контрольні заходи	Екзамен,	
Розклад занять	<a href="http://rozklad.kpi.ua/">http://rozklad.kpi.ua/</a>	
Мова викладання	Українська	
Інформація про керівника курсу / викладачів	Лектор: кандидат технічних наук, Стьопочкіна Ірина Валеріївна, telegram: @ivst1113, e-mail: <a href="mailto:irst-ipt@ill.kpi.ua">irst-ipt@ill.kpi.ua</a>  Практичні: Войцеховський Андрій Валерійович	
Розміщення курсу	Посилання на дистанційний ресурс (Платформа "Сікорський": курс Теорія та методи соціальної інженерії в кібербезпеці <a href="https://do.ipk.kpi.ua/course/view.php?id=1713">https://do.ipk.kpi.ua/course/view.php?id=1713</a> ,	

Програма навчальної дисципліни

**1. Опис навчальної дисципліни, її мета, предмет вивчення та результати навчання**

Соціальна інженерія є одним із найуспішніших напрямків здійснення атак на об'єкти різного типу. Слабкою ланкою кожної системи захисту є людина, саме з участю людського фактору соціальний інженер досягає своєї мети. Уміння та знання, набуті в цьому курсі, можуть бути використані там, де передбачається діяльність із кіберзахисту інформації, в тому числі із використанням наукоємних технологій, на стику із методиками HR-менеджмента.

Навчальна дисципліна «Теорія та методи соціальної інженерії в кібербезпеці» розглядає теоретичні основи відповідних атак. В тому числі, розглянуто моделі атак соціальної інженерії, моделі їх виявлення, сценарії різних видів атак соціальної інженерії, ПЗ, яке використовується при цьому та способи протидії цим атакам. Ці знання дають змогу зрозуміти фактори успіху відповідних атак, та попередити їх.

Теоретичні матеріали курсу дають студенту знання про:

- Моделі та сценарії атак та їх виявлення;
- Поведінковий та психологічний портрет потенційних жертв соціального інженера, сценарії поведінки які призводять до успіху подібних атак;

- Механізми здійснення різних атак соціальної інженерії;
- Нові технології та засоби соціальної інженерії, засновані на ML та AI, в тому числі DeepFake та інші.
- Рішення кіберзахисту та підходи до попередження атак соціальної інженерії.

Також за дисципліною передбачено 5 комп'ютерних практикумів, які доповнюють теоретичний матеріал і поглиблюють його за практичним напрямом. Передбачається, що практикуми повинні бути здані вчасно, в разі перевищення дедлайну встановлений штраф: практикум захищається на мінімальну позитивну оцінку. Дати дедлайнів обговорюються зі студентами на першому занятті. В результаті виконання практикумів студент набуває такі уміння:

- Розробляти сценарії та моделі атак соціальної інженерії та здійснювати імітаційне моделювання;
- Уміння розробляти програму тестування на проникнення із використанням різних підходів;
- Використовувати наявні програмні засоби, за допомогою яких може діяти соціальний інженер, в цілях тестування на проникнення;
- Уміння розробляти методики оцінки персоналу на чутливість до різних атак соціальної інженерії;
- Уміння розробляти елементи засобів тестування на проникнення із використанням підходів соціальної інженерії.

За курсом передбачено модульну контрольну роботу для контролю засвоєння практичного та теоретичного матеріалу.

. **Предметом** дисципліни є моделі та методи соціальної інженерії в кібербезпеці.

#### **Програмні результати<sup>1</sup> навчання**

Демонструвати знання й розуміння основних концепцій, принципів теорій прикладної математики і використовувати їх на практиці.

Після вивчення дисципліни студент володітиме **знаннями** щодо теоретичних моделей та методів соціальної інженерії, **уміннями**: застосовувати відповідні методи до виявлення атак соціальної інженерії, складати програми та методики тестування на проникнення із використанням відповідних методів.

---

<sup>1</sup> Для нормативних дисциплін зазначається згідно матриці відповідності програмних компетентностей та результатів навчання в освітній програмі.

## **2. Пререквізити та постреквізити дисципліни (місце в структурно-логічній схемі навчання за відповідною освітньою програмою)**

Дисципліна не містить суттєвих взаємозв'язків із попередніми та наступними дисциплінами. Для виконання завдань необхідне володіння інформаційними технологіями загального характеру.

Результати вивчення даної дисципліни можуть бути застосовані у професійній діяльності за фахом та для написання магістерської дипломної роботи.

## **3. Зміст навчальної дисципліни**

1. Поняття соціальної інженерії, приклади. Основні вихідні припущення, які гарантують успіх атаки.
2. Життєвий цикл атак соціальної інженерії різного типу. Контрзаходи.
3. Основні вектори атак соціальної інженерії. Способи протидії соціальній інженерії у організаціях та підприємствах.
4. Моделі соціальної інженерії. Моделі виявлення атак соціальної інженерії. SEADM, психологічні тригери. Суб'єктивна теорія корисності та здатність приймати раціональні рішення. Приклади.
5. Особистісні фактори, які впливають на успішність атак соціальної інженерії. Психологічний портрет жертви соціального інженера. Модель виявлення емоційного стану потенційної жертви соціального інженера.
6. Побудова сценаріїв атак та розпізнавання атак на основі автоматизованих засобів. Модель виявлення атаки
7. Автоматизовані засоби соціальної інженерії: можливості та призначення. Збір інформації про жертву та її використання. Тестування на проникнення із використанням деяких автоматизованих засобів.
8. Обхід двохфакторної автентифікації як популярний засіб соціальної інженерії. Шляхи заволодіння факторами. Підходи до автентифікації. Схеми та приклади атак. Типи зворотніх проксі та атаки з їх використанням.
9. Спам-листи як носій запитів соціальної інженерії. Архітектура поштового сервісу. Способи автоматизованої генерації спам-листів на основі машинного навчання. Обхід спам-фільтрів.
10. Налаштування спам-фільтрів. Генерація повідомлень для автоматизованого пентесту.
11. Техніки роботи спам-фільтрів. Методи підвищення роботи класифікатора спаму, виділення суттєвих ознак. Поведінкові шаблони, контентні та неконентні ознаки.
12. Порівняльний аналіз існуючих спам-фільтрів та принципів їх роботи. Спам у вигляді посилань. Зловмисні інфраструктури переспрямувань.
13. Розпізнавання фішингових сайтів. Визначення фішингу та його сучасні різновиди. Життєвий цикл виявлення та протидії атакам фішингу. Фішинг із використанням сайтів. Виділення класифікаційних ознак фішингових сайтів. Алгоритм виявлення фішингового сайту: датасети, підготовка даних, обробка результатів. Приклад
14. Засоби генерації фейкових зображень, голосу та відео на основі технології DeepFake. Алгоритмічні, програмні основи технологій підробки. Види атак соціальної інженерії де використовується підробка голосу. Технологія клонування голосу. Проблеми розпізнавання дідфейків. Візуальні ознаки дідфейку. Споріднені задачі по виявленню фейків, зокрема виявлення фейкових профілів.

## **4. Навчальні матеріали та ресурси**

*Базова література.*

1. Стьопочкіна І.В. Теорія та методи соціальної інженерії. Матеріали дистанційного курсу [Режим доступу]: <https://do.ipk.kpi.ua/course/view.php?id=1713>
2. Теорія та методи соціальної інженерії в кібербезпеці. Методичні вказівки до комп'ютерного практикуму /Стьопочкіна І.В. [Режим доступу]: <https://do.ipk.kpi.ua/course/view.php?id=1713>
3. C. Hadnagy, *Social engineering: The art of human hacking*. – [Режим доступу: <https://www.oreilly.com/library/view/social-engineering-the/9780470639535/>]
4. K.Mitnick, *The art of deception*. - [Режим доступу: [https://repo.zenk-security.com/Magazine%20E-book/Kevin\\_Mitnick\\_-\\_The\\_Art\\_of\\_Deception.pdf](https://repo.zenk-security.com/Magazine%20E-book/Kevin_Mitnick_-_The_Art_of_Deception.pdf)]

Додаткова література.

1. Maltego. [Електронний ресурс]. – Режим доступу: <https://www.maltego.com/maltego-community/> (1)
2. Recon-ng. [Електронний ресурс]. – Режим доступу: <https://github.com/lanmaster53/recon-ng> (1)
3. How to use Burp-suite for penetration testing. [Електронний ресурс]. – Режим доступу: <https://portswigger.net/burp/documentation/desktop/penetration-testing>
4. Shodan. [Електронний ресурс]. – Режим доступу: <https://developer.shodan.io/>
5. ISO/IEC 27032 . - Режим доступу: <https://www.iso.org/standard/44375.html>
6. ISO/IEC 27004 . – Режим доступу: <https://www.iso.org/obp/ui/#iso:std:iso-iec:27004:ed-2:v1:en> (3)
7. K. Krombholz, *Social Engineering Attackson the Knowledge Worker*. – Режим доступу: [https://www.researchgate.net/publication/262393147\\_Social\\_engineering\\_attacks\\_on\\_the\\_knowledge\\_worker](https://www.researchgate.net/publication/262393147_Social_engineering_attacks_on_the_knowledge_worker) (4)
8. M. Turner, J. Banas et al. *The Effects of Altercasting and Counterattitudinal Behavior on Compliance: A Lost Letter Technique Investigation*. – Режим доступу: [https://www.researchgate.net/publication/233074668\\_The\\_Effects\\_of\\_Altercasting\\_and\\_Counterattitudinal\\_Behavior\\_on\\_Compliance\\_A\\_Lost\\_Letter\\_Technique\\_Investigation](https://www.researchgate.net/publication/233074668_The_Effects_of_Altercasting_and_Counterattitudinal_Behavior_on_Compliance_A_Lost_Letter_Technique_Investigation)
9. *Social Engineering Toolkit*. [Електронний ресурс]. – Режим доступу: <https://github.com/trustedsec/social-engineer-toolkit>
10. *Google IP address ranges for outbound mail servers*.- Режим доступу: <https://support.google.com/a/answer/60764>
11. *About DMARC*. – Режим доступу: <https://support.google.com/a/answer/2466580>
12. Eleuther. [Електронний ресурс]. – Режим доступу: <https://www.wired.com/story/ai-generate-convincing-text-anyone-use-it/>
13. W. Fan et al. *Social Engineering: I-E based Model of Human Weakness for Attack and Defense Investigations*. – Режим доступу: [https://www.researchgate.net/publication/312020665\\_Social\\_Engineering\\_I-E\\_based\\_Model\\_of\\_Human\\_Weakness\\_for\\_Attack\\_and\\_Defense\\_Investigations](https://www.researchgate.net/publication/312020665_Social_Engineering_I-E_based_Model_of_Human_Weakness_for_Attack_and_Defense_Investigations)
14. A. Bhowmick, S. Hazarika. *E-Mail Spam Filtering: A Review of Techniques and Trends*. – Режим доступу: [https://www.researchgate.net/publication/320703241\\_E-Mail\\_Spam\\_Filtering\\_A\\_Review\\_of\\_Techniques\\_and\\_Trends](https://www.researchgate.net/publication/320703241_E-Mail_Spam_Filtering_A_Review_of_Techniques_and_Trends)
15. J.-H. Hoernan, J. Van Nieuwenhuizen, F. D. Garcia. *Spam filter analysis*. – Режим доступу: [https://www.researchgate.net/publication/46298891\\_Spam\\_Filter\\_Analysis](https://www.researchgate.net/publication/46298891_Spam_Filter_Analysis).
16. *Deep Insights of Deepfake Technology : A Review*. – Режим доступу: [https://www.researchgate.net/publication/351300442\\_Deep\\_Insights\\_of\\_Deepfake\\_Technology\\_A\\_Review](https://www.researchgate.net/publication/351300442_Deep_Insights_of_Deepfake_Technology_A_Review)

## 5. Методика опанування навчальної дисципліни (освітнього компонента)

В рамках дисципліни заплановано наступні види навчальних занять:

- лекції;
- комп'ютерні практикуми;
- самостійна робота.

На лекціях розкриваються найбільш суттєві теоретичні питання, які дозволяють забезпечити аспірантам можливість глибокого самостійного вивчення всього програмного матеріалу. Теми та порядок самостійної роботи сформовано у відповідності із матеріалами лекцій і повністю узгоджуються з метою дисципліни та здійснюються з використанням рекомендованої літератури та глобальної мережі Internet. На заняттях використовуються звичайна дошка, а також презентації лекцій з використанням мультимедіа-проектора. В дистанційному режимі використовуються засоби Google Meet та відповідні слайди лекцій, а також матеріали дистанційного курсу, викладені на платформі Сікорський.

Теми та порядок освоєння дисципліни «Теорія та методи соціальної інженерії в кібербезпеці» наведений нижче.

№ з/п	Назви тем і питань, що виносяться на заняття	Кількість годин		
		Лекції	Практичні заняття	Самостійна робота
1	<b>Вступ.</b> PCO, предмет та об'єкт курсу. <b>Тема 1.</b> Поняття соціальної інженерії, приклади. Основні вихідні припущення, які гарантують успіх атаки. Основна література: [1, 3]. Додаткова література: [1,2].	2		4
2	<b>Тема 2.</b> Життєвий цикл атак соціальної інженерії різного типу. Контрзаходи. Основна література: [1-4]. Додаткова література: [3-6]	2	2	4
3	<b>Тема 3.</b> Основні вектори атак соціальної інженерії. Способи протидії соціальній інженерії у організаціях та підприємствах. Основна література: [1-3]. Додаткова література: [7]	2	4	4
4	<b>Тема 4.</b> Моделі соціальної інженерії. Моделі виявлення атак соціальної інженерії. SEADM, психологічні тригери. Суб'єктивна теорія корисності та здатність приймати раціональні рішення. Приклади. Основна література: [1-3]. Додаткова література: [8]	2	2	4
5	<b>Тема 5.</b> Особистісні фактори, які впливають на успішність атак соціальної інженерії. Психологічний портрет жертви соціального інженера. Модель виявлення емоційного стану потенційної жертви соціального інженера. Основна література: [1,3-5]. Додаткова література: [8]	4		4
6	<b>Тема 6.</b> Побудова сценаріїв атак та розпізнавання атак на основі автоматизованих засобів. Модель виявлення атаки. Основна література: [1,2]. Додаткова література: [4-7,9]	4	2	4
7	<b>Тема 7.</b> Автоматизовані засоби соціальної інженерії: можливості та призначення. Збір інформації про жертву та її використання. Тестування на проникнення із використанням деяких	2	4	4

	автоматизованих засобів. Основна література: [1,2]. Додаткова література: [1-4]			
8	<b>Тема 8.</b> Обхід двохфакторної автентифікації як популярний засіб соціальної інженерії. Шляхи заволодіння факторами. Підходи до автентифікації. Схеми та приклади атак. Типи зворотніх проксі та атаки з їх використанням. Основна література [1-3].	2		4
9	<b>Тема 9.</b> Спам-листи як носій запитів соціальної інженерії. Архітектура поштового сервісу. Способи автоматизованої генерації спам-листів на основі машинного навчання. Обхід спам-фільтрів. Основна література: [1,2]. Додаткова література: [10,11,15]	2		4
10	<b>Тема 10.</b> Налаштування спам-фільтрів. Генерація повідомлень для автоматизованого пентесту. Основна література: [1,2]. Додаткова література: [10,11,15]	2		4
11	<b>Тема 11.</b> Техніки роботи спам-фільтрів. Методи підвищення роботи класифікатора спаму, виділення суттєвих ознак. Поведінкові шаблони, контентні та неконтентні ознаки. Основна література: [1]. Додаткова література: [14]	2		4
12	<b>Тема 12.</b> Порівняльний аналіз існуючих спам-фільтрів та принципів їх роботи. Спам у вигляді посилань. Зловмисні інфраструктури переспрямувань. Основна література: [1]. Додаткова література: [14,15]	2		4
13	<b>Тема 13.</b> Розпізнавання фішингових сайтів. Визначення фішингу та його сучасні різновиди. Життєвий цикл виявлення та протидії атакам фішингу. Фішинг із використанням сайтів. Виділення класифікаційних ознак фішингових сайтів. Алгоритм виявлення фішингового сайту: датасети, підготовка даних, обробка результатів. Приклад. Основна література: [1,2]. Додаткова література: [5,6]	2	4	4
14	<b>Тема 14.</b> Засоби генерації фейкових зображень, голосу та відео на основі технології DeepFake. Алгоритмічні, програмні основи технологій підробки. Види атак соціальної інженерії де використовується підробка голосу. Технологія клонування голосу. Проблеми розпізнавання дідфейків. Візуальні ознаки дідфейку. Споріднені задачі по виявленню фейків, зокрема виявлення фейкових профілів. Основна література: [1,3]. Додаткова література: [16]	4		4
	<b>Всього</b>	34	18	56
	<b>Модульна контрольна робота</b>	2		10
	<b>Екзамен</b>			30
	<b>Разом годин: 150</b>	36	18	96

Теми практичних занять (зміст наведено у [2]). Допускається проходження практичного курсу "Теорія та методи соціальної інженерії в кібербезпеці" від НТУУ "КПІ ім. Ігоря

Сікорського” на платформі RangeForce, максимальна оцінка за цей курс дорівнює максимально можливій оцінці за лабораторні роботи; або інших курсах неформальної освіти (за умови співпадіння тем курсу із даним та узгодження із викладачем). Такий курс може бути зарахований як еквівалент лабораторних робіт, повністю або частково.

№ КП	Теми практичних занять	Кількість ауд. годин
1.	Пошук електронної адреси як основного контакту для дій соціального інженера. Одержання інформації облікових записів в Facebook	2
2.	Використання можливостей Google Dorking для пошуку інформації у відкритому доступі	4
3.	Налаштування роботи веб-ресурсу для упередження індексації деяких розділів сайту пошуковими сервісами	4
4.	Виявлення фішингових сайтів методами машинного навчання	4
5.	Сценарії пошуку інформації по цільовому об'єкту засобами відкритої розвідки	4
Всього		18

## 6. Самостійна робота здобувача

Самостійна робота здобувача складається із опанування та засвоєння відповідних лекційних матеріалів, підготовки до МКР та екзамену. Також здобувачі самостійно доопрацьовують результати комп'ютерних практикумів та готуються до їх захисту, допоміжні контрольні питання надано в [2].

## Політика та контроль

### 7. Політика навчальної дисципліни (освітнього компонента)

Відвідування занять не оцінюється, але рекомендується. Контроль відвідування проводиться викладачем вибірково.

Завдання практичних занять виконуються та захищаються у відповідності до встановлених дедлайнів на протязі семестру.

Під час виконання практичних робіт а також під час контрольних заходів здобувачами повинна дотримуватись політика академічної доброчесності, згідно Кодексу Честі НТУУ “КПІ”.

### 8. Види контролю та рейтингова система оцінювання результатів навчання (PCO)

Поточний контроль: виконання та захист комп'ютерних практикумів.

Календарний контроль: атестація проводиться двічі на семестр як моніторинг поточного стану виконання вимог силабусу.

1. Комп'ютерні практикуми сформовані таким чином, що їх завдання сприяють одержанню практичних навичок та засвоєнню матеріалу за темами дисципліни. Комп'ютерні практикуми передбачають їх виконання та захист.

2. Екзамен. Умовою допуску до семестрового контролю є виконання усіх поточних контрольних заходів та рейтинг більший за 35 балів ( $RD \geq 35$ ). Максимальна кількість балів за семестр – 60. Оцінювання відповідей на екзамені:

- вичерпна відповідь – 35-40 балів;
- вичерпна відповідь з незначними помилками – 30-34 балів;
- неповна відповідь та помилки – 20 – 29 балів;

- *грубі помилки – 8-19*
- *незадовільна відповідь – 0 балів.*

Поточний контроль:

№ з/п	Контрольний захід	Макс. бал	Ваговий коеф.	Кіл-ть	Всього
1.	Комп'ютерні практикуми	8	1	5	40
2.	Модульна контрольна робота	5	4	1	20
2.	Екзамен	40	1	1	40
	Всього				100

Таблиця переведення рейтингових балів до оцінок за університетською шкалою:

Рейтингові бали, RD	Оцінка за університетською шкалою	Можливість отримання оцінки «автоматом»
$95 \leq RD \leq 100$	Відмінно	-
$85 \leq RD \leq 94$	Дуже добре	-
$75 \leq RD \leq 84$	Добре	-
$65 \leq RD \leq 74$	Задовільно	-
$60 \leq RD \leq 64$	Достатньо	-
$RD < 60$	Незадовільно	-
Невиконання умов допуску	Не допущено	-

### Екзамен та робота в семестрі

Екзамен є обов'язковим контрольним заходом. Рейтингова оцінка роботи за семестр складається з результатів роботи в семестрі (RD) (в рамках 60 балів). На екзамені здобувач одержує білет, відповідь на який оцінюється по 40-бальній шкалі.

*Штрафні бали:*

Заохочувальні бали		Штрафні бали	
Критерій	Ваговий бал	Критерій	Ваговий бал
Участь у олімпіадних змаганнях спорідненої тематики	+5 балів	Невчасне здання практичної роботи	-2 бали

### Семестровий контроль: екзамен.

Умови допуску до семестрового контролю: мінімальна позитивна оцінка за комп'ютерні практикуми / семестровий рейтинг більше 35 балів/ написана на позитивну оцінку МКР.

### 9. Додаткова інформація

Питання, що виносяться на екзамен, повністю відповідають змісту дисципліни. Необхідною умовою роботи здобувача є його реєстрація на курсі "Теорія та методи соціальної інженерії в кібербезпеці" на платформі Сікорський <https://do.ipr.kpi.ua/course/view.php?id=1713>

**Робочу програму навчальної дисципліни (силабус):**

**Склав:** доц. каф. Інформаційної безпеки Стьопочкіна Ірина Валеріївна, ас. Войцеховський Андрій Валерійович

**Ухвалено кафедрою (протокол №6/2024 від 19.06.2024)**

**Погоджено Методичною комісією НН ФТІ (протокол №6/2024 від 27.06.2024)**