СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Соціальна інженерія

Рівень вищої освіти	Перший (бакалаврський)
Код та назва спеціальності, галузь знань	**С4** Психологія, **С** Соціальні науки, журналістика, інформація та міжнародні відносини
Тип та назва освітньої програми	Освітньо-професійна програма «Психологія»
Статус навчальної дисципліни	Обов'язкова компонента (ОК-25)
Курс, семестр викладання	4 курс, 8 семестр
Трудомісткість навчальної дисципліни	5 кредитів ЄКТС (150 академічних годин), з них: денна (очна) форма навчання: лекц. – 20 год., практ. зан. – 34 год., самост. роб. – 96 год.; заочна форма навчання: лекц. – 10 год., практ. зан. – 18 год., самост. роб. – 122 год.
Мова викладання	Українська
Кафедра	Кіберпсихології та реабілітації
Факультет	Бізнесу та соціальних комунікацій

Розробники / викладачі

СТАЙКУЦА Сергій Володимирович,
доцент кафедри кібербезпеки та технічного захисту інформації,
кандидат філософських наук, доцент

E-mail: s.v_staikutsa@suitt.edu.ua
Тел.: +380679625151

Консультації: щосереди з 14^{30} до 15^{30} год., ауд. 250

ВОРОНОВА Світлана Віталіївна,
доцент кафедри кіберпсихології та реабілітації
кандидат педагогічних наук

E-mail: deisyflower3@gmail.com
Тел.: +380673932600

Консультації: щосереди з 14^{00} до 15^{00} год., каб. 310 (головний корпус)

Мета дисципліни	– сформувати у здобувачів вищої освіти цілісне уявлення про соціальну інженерію як сучасний інструмент впливу в інформаційному суспільстві, навчити розпізнавати, аналізувати та протидіяти соціально-інженерним атакам, розвивати критичне мислення, навички комунікації та особистісної стійкості до маніпуляцій.
Компетентності, формуванню яких сприяє дисципліна	**ЗК-3**.Навички використання інформаційних і комунікаційних технологій. **СК-2.** Здатність до ретроспективного аналізу вітчизняного та зарубіжного досвіду розуміння природи виникнення, функціонування та розвитку психічних явищ. **СК-4.** Здатність самостійно збирати та критично опрацьовувати, аналізувати та узагальнювати психологічну інформацію з різних джерел.
Програмні результати навчання	**ПРН-3**.Здійснювати пошук інформації з різних джерел, у т.ч. із використанням інформаційно-комунікаційних технологій, для вирішення професійних завдань. **ПРН-4**.Обґрунтовувати власну позицію, робити самостійні висновки за результатами власних досліджень і аналізу літературних джерел. **ПРН-10**.Формулювати думку логічно, доступно, дискутувати, обстоювати власну позицію, модифікувати висловлювання відповідно до культуральних особливостей співрозмовника. **ПРН-11**.Складати та реалізовувати план консультативного процесу з урахуванням специфіки запиту та індивідуальних особливостей клієнта, забезпечувати ефективність власних дій. **ПРН-12**.Складати та реалізовувати програму психопрофілактичних та просвітницьких дій, заходів психологічної допомоги у формі лекцій, бесід, круглих столів, ігор, тренінгів, тощо, відповідно до вимог замовника.

Програма навчальної дисципліни

Тема 1. ***Концептуальні основи соціальної інженерії***	Сутність феномену «соціальна інженерія». Історія розвитку соціальної інженерії. Місце соціальної інженерії у системі інформаційної та психологічної безпеки. Принципи соціальної інженерії. Сфери застосування концепції OSINT. Сучасні теоретичні підходи, класифікація та аналіз поведінки людей. Вплив, навіювання та переконання. Шість принципів впливу Р. Чалдіні. Інженерія довіри та авторитету. Маніпуляція. Вплив на громадську думку.
Тема 2. ***Класифікація атак та їх ідентифікація в соціальній інженерії***	Методи та джерела для збору інформації: технічні, не технічні, відкриті джерела, інсайдинг. Основні цілі та етапи соціоінженерної атаки. Підготовка до атаки. Послідовні фази атаки на основі загроз соціальної інженерії. Види атак із використанням соціальної інженерії: фішинг (Phishing) (цільовий фішинг (spear phishing), голосовий фішинг (vishing, voice phishing), смішинг (smishing), «Китобійний» фішинг (whale phishing), клон-фішинг (clone phishing)), лякалка (scareware), приманка (baiting), «водопій» (water-holing), «атака з приводом» (pretexting), «послуга за послугу» (quid pro quo), «медова пастка» (honey trap), шахрайська атака (rogue attack), крадіжка з диверсією (diversion theft), вішинг (vishing), тейлгейт (tailgating), газлайтинг (gaslighting). Комунікації для управління масами.
Тема 3. ***Кіберхейт у вимірах соціальної інженерії***	Поняття кіберхейту: від агресії до маніпуляції. Соціально-психологічні механізми впливу хейту. Віктимологія та психологія агресора. Психологічні наслідки для індивіда й спільнот. Копінг-стратегії у протистоянні кіберхейту.
Тема 4. ***Особистісно-психологічний захист:***	Культура поінформованості про особисту безпеку. Оцінка готовності до атак. Аналіз помилок. Роль особистісних якостей в успішності або вразливості до атак. Емоційні пастки. Соціальні тригери. Когнітивно-поведінкові техніки емоційної

методи та техніки	стійкості. Емоційний самоконтроль. Стратегії захисту від атак. Етичні та правові аспекти особистісного захисту.
Тема 5. ***Симуляційні ігри як метод формування навичок протидії соціоінженерним атакам***	Поняття симуляційних ігор та їхні відмінності від гейміфікації. Освітній потенціал ігор: навчання через досвід та помилки. Класифікація симуляційних ігор для протидії соціоінженерії. Дизайн ігор для навчання. Практичні моделі симуляцій: «Фішинг-полювання», «День у хакера», «Телефон довіри», «Соцмережевий спрут», «Інсайдер», «Злам довіри». Оцінювання ефективності симуляційних ігор.

Методи навчання

При вивченні навчальної дисципліни використовуються наступні методи навчання:

Інтерактивні	• Дискусії та дебати: обговорення актуальних проблем соціальної інженерії, висловлювання власних думок та аргументація позицій, що сприяє розвитку критичного мислення та комунікативних навичок. • Симуляційні ігри: моделювання типових ситуацій, пов'язаних із соціально-інженерними атаками, де здобувачі вищої освіти виступають у ролі атакуючих, жертв або захисників. Це дозволяє краще зрозуміти мотиви та механізми дій різних сторін. • Групова робота та мозковий штурм: використовується для спільного аналізу проблем, генерування ідей щодо захисту від атак, розробки стратегій протидії та обміну досвідом. • Аналіз кейсів (case-study): розгляд реальних або змодельованих випадків соціальної інженерії, розбір помилок, обговорення можливих шляхів розв'язання проблем. • Інтерактивна лабораторія (Capture the Flag): відпрацювання захисту та виявлення соціально-інженерних методів. • Mind Map або концептуальні карти: створення карти понять, що показують зв'язки між методами атак, мотиваціями, захистом. • Культурна OSINT-аналітика (Open Source Intelligence): використання відкритих джерел (фільмів, серіалів, відео) для аналізу соціальних інженерних тактик. • Checklist-аудит поведінки: усвідомлення векторів атаки через персональні слабкості.
Практичні	• Практичні завдання: вправи з ідентифікації соціально-інженерних атак, аналізу фішингових листів, створення сценаріїв атак і захисту. • Індивідуальні та групові міні-проєкти: розробка власних стратегій захисту, підготовка презентацій, створення інформаційних матеріалів для підвищення обізнаності щодо соціальної інженерії.
Методи дистанційного навчання	• Онлайн-лекції або онлайн-практичні заняття: залучення сучасних платформ (Zoom, Moodle, Google Meet та ін.) для проведення лекцій у синхронному чи асинхронному режимі, що забезпечує доступність матеріалів для здобувачів вищої освіти незалежно від місця перебування. • Використання електронних навчальних ресурсів: доступ до інтерактивних навчальних модулів, тестів для самоперевірки, груп для обговорення актуальних питань з викладачем чи здобувачами вищої освіти. • Віртуальні лабораторії: можливість виконувати практичні завдання та симуляції в онлайн-середовищі, що моделює реальні ситуації соціальної інженерії. • Індивідуальне і групове онлайн-консультування: спільнодія викладача та здобувачів вищої освіти щодо виконання практичних та самостійних завдань через чати та e-mail-надсилання.

Стратегія оцінювання результатів навчання	
Змістовий контент результатів навчання з дисципліни	Результати навчання з даної дисципліни, які здобувач може продемонструвати та які можна ідентифікувати, оцінити і виміряти, розглядаються у вимірах 6-го рівня Національної рамки кваліфікацій, що відповідає першому циклу вищої освіти Рамки кваліфікацій Європейського простору вищої освіти, а саме: ***Знання*** – сутності, принципів і основних понять соціальної інженерії; класифікації, типових сценаріїв та методів соціально-інженерних атак; усвідомлення психологічних механізмів впливу, маніпуляцій, соціальних тригерів; знання сучасних інструментів, технологій та методів захисту від соціальної інженерії; орієнтація в етичних і правових аспектах соціально-інженерної діяльності. ***Уміння/навички*** – ідентифікувати та аналізувати різні види соціально-інженерних атак у реальних та змодельованих ситуаціях; застосовувати методи аналізу поведінки, розпізнавати ознаки маніпуляцій та впливу; розробляти та впроваджувати стратегії особистого й організаційного захисту від соціальної інженерії; оцінювати ризики, прогнозувати можливі наслідки та приймати обґрунтовані рішення у сфері інформаційної безпеки. ***Комунікація*** – підвищення рівня комунікативної компетентності у сфері соціальної інженерії через роботу в команді, участь у групових дискусіях, розробку спільних стратегій захисту. ***Відповідальність та автономія*** – спонукання до усвідомленої особистої відповідальності за інформаційну безпеку та захист від соціально-інженерних атак.
Критерії оцінювання	Академічні успіхи здобувачів вищої освіти в межах даної дисципліни оцінюються за бально-рейтинговою шкалою (максимальна кількість – 100 балів), що прийнята в ДУІТЗ, з обов'язковим переведенням кількості балів в оцінки за національною шкалою та за шкалою ECTS. **Відмінно (A) – від 90 до 100 балів** – здобувач у повному обсязі володіє навчальним матеріалом, вільно самостійно та аргументовано його викладає під час усних виступів та письмових відповідей, глибоко та всебічно розкриває зміст теоретичних питань та практичних завдань, використовуючи при цьому обов'язкову та додаткову літературу. Правильно вирішив усі або не менше 90% завдань, передбачених програмою навчальної дисципліни. **Дуже добре (B) – від 82 до 89 балів** – здобувач досить повно володіє навчальним матеріалом, обґрунтовано його викладає під час усних виступів та письмових відповідей, в основному розкриває зміст теоретичних питань та практичних завдань, використовуючи при цьому обов'язкову літературу. Однак під час викладання деяких питань допускаються при цьому окремі несуттєві неточності. Правильно вирішив 82-89% письмових завдань. **Добре (C) – від 74 до 81 балів** – здобувач достатньо повно володіє навчальним матеріалом, обґрунтовано його викладає під час усних виступів та письмових відповідей, в основному розкриває зміст теоретичних питань та практичних завдань, використовуючи при цьому обов'язкову літературу. Однак під час викладання деяких питань не вистачає достатньої глибини та аргументації, допускаються при цьому окремі несуттєві неточності та незначні помилки. Правильно вирішив 74-81% письмових завдань. **Задовільно (D) – від 64 до 73 балів** – здобувач в цілому володіє навчальним матеріалом, викладає його основний зміст під час усних та письмових відповідей, але з не зовсім глибоким та всебічним аналізом, обґрунтуванням та аргументацією, з недостатнім використанням необхідної літератури, допускаючи при цьому окремі неточності та помилки. Правильно вирішив 64-73% письмових завдань.

	Задовільно (E) – від 60 до 63 балів – здобувач в цілому володіє навчальним матеріалом, викладає його основний зміст під час усних та письмових відповідей, але без глибокого всебічного аналізу, обґрунтування та аргументації, без використання необхідної літератури, допускаючи при цьому окремі суттєві неточності та помилки. Правильно вирішив 60-63% письмових завдань. **Незадовільно (FX) – від 35 до 59 балів, з можливістю повторного складання** – здобувач не в повному обсязі володіє навчальним матеріалом. Фрагментарно, стисло без аргументації та обґрунтування викладає його під час усних виступів та письмових відповідей, поверхово розкриває зміст теоретичних питань та практичних завдань, допускаючи при цьому суттєві неточності. Правильно вирішив 35-59% письмових завдань. **Незадовільно (F) – від 0 до 34 балів, з обов'язковим повторним вивченням дисципліни** – здобувач частково володіє навчальним матеріалом, не у змозі викласти зміст більшості питань теми під час усних виступів та письмових відповідей, допускаючи при цьому суттєві помилки. Правильно вирішив 1-34% письмових завдань.
Форма та методи контролю начальних досягнень	Оцінювання знань здобувачів з даної навчальної дисципліни здійснюється під час проведення поточного і підсумкового контролю. ***Поточний контроль*** здійснюється під час проведення лекцій, практичних занять, перевірки виконання завдань самостійної роботи, перевірки виконання поточних контрольних робіт та має на меті оцінювання рівня засвоєння здобувачем навчального матеріалу освітнього компоненту освітньо-професійної програми. ***Підсумковий контроль*** проводиться у формі **екзамену**, який передбачає перевірку рівня теоретичних знань, практичних умінь і навичок, а також здатності їх застосовувати у професійній діяльності.

Політика навчальної дисципліни

Відвідування	Відповідальність за відвідування лекцій, згідно з академічним розкладом, покладається на здобувача вищої освіти. Водночас, обов'язковою є присутність на всіх практичних заняттях та контрольних заходах, включаючи екзамен. Також важливо своєчасно виконувати індивідуальні завдання, передбачені програмою дисципліни в рамках самостійної роботи.
Дотримання принципів академічної доброчесності	Усі завдання, письмові роботи та інші види навчальної діяльності в межах дисципліни здобувач вищої освіти виконує самостійно відповідно до принципів академічної доброчесності. Викладач має право здійснювати перевірку виконаних робіт, використовуючи різні програмні інструменти.
Умови зарахування пропущених занять	Відпрацювання академічної заборгованості з дисципліни можливо до початку екзаменаційної сесії. Процедура узгоджується з викладачем, згідно його розкладу консультацій.
Інші умови	Навчально-методичні матеріали дисципліни розміщені на платформі Moodle

Рекомендовані джерела інформації

Базові підручники та навчальні посібники	• Берн Е. Ігри, у які грають люди ; пер. з англ. К. Меньшикової. Харків : Книжковий Клуб «КСД», 2016. 256 с. • Свідоме і несвідоме у груповій взаємодії : монографія / П. П. Горностай, О. Л. Коробанова, О. Т. Плетка, Г. В. Циганенко, Л. Г. Чорна ; за наук. ред. П. П. Горностая. Кропивницький : Імекс-ЛТД, 2018. 244 с. • Соціальна інженерія (системний аналіз): навч. посіб. / В. М. Петрик, В. І. Курганевич, В. Г. Кононович та ін. / за заг.

	ред. В. І. Курганевича та В. М. Петрика. Київ, 2019. 200 с. • Соціальна інженерія в контексті кібернетичної безпеки України (сучасні технології та шляхи захисту): навч. посіб. / Ю. Г. Куцан, О. М. Богданов, В. М. Петрик, Д. В. Пахольченко, А. В. Давидюк / за заг. ред. В. М. Петрика. Київ, 2017. 80 с. • Чалдіні Р. Психологія впливу. Книжковий клуб «КСД», 2022. 608 с.
Методичні рекомендації та розробки викладачів дисципліни	• Кіберпсихологія у вимірах сучасного наукового дискурсу: монографія / авт. кол.: С. Хаджирадєва, Ю. Левін, М. Тодорова (та ін.); за заг. ред. С. К. Хаджирадєвої. Одеса: Астропринт, 2024. 240 с. • Соціальна інженерія та кіберпсихологія : монографія / Авт. кол. : В. Г. Кононович, С. В. Стайкуца, М. М. Тодорова, С. В. Воронова, О. М. Рябуха. Одеса : ДУІТЗ, 2025. 387 с. • Стайкуца С. В., Гомінар В. І. Кібергігієна як основа формування безпеки особистості, підприємства та держави: мат. VI Міжнар. наук.-практ. конф. «Спільні дії військових формувань і правоохоронних органів держави: проблеми та шляхи вирішення в умовах воєнного стану». 2024. • Стайкуца С. В., Воронова С. В. Соціальна інженерія : навчально-методичний комплекс дисципліни [ОПП «Психологія» зі спеціальності С4 Психологія; для здобувачів першого (бакалаврський) рівня вищої освіти]. Одеса : ДУІТЗ, 2025. • Khadzhyradieva, S., Todorova, M., Staikutsa, S., Tsybukh, L., & Lukiianchuk, A. N. Analysis of Cyber-psychological Protection Programs in the Education System: Role, Limitations and Prospects. Salud, Ciencia y Tecnología-Serie de Conferencias 2024. # 3. 648 p.
Інформаційні ресурси	• Агентство Європейського Союзу з кібербезпеки (ENISA) https://www.enisa.europa.eu/ • Уповноважений ВР України з прав людини (Омбудсмен) https://ombudsman.gov.ua/uk/zayavniku • Кіберполіція України – поради щодо захисту від шахрайства https://cyberpolice.gov.ua/ • Nadiyno. Гаряча лінія з цифрової безпеки https://nadiyno.org/

Рік введення силабусу – 2025 р.	Затверджено рішенням кафедри кіберпсихології та реабілітації (Протокол від 26 серпня 2025 р. № 1)	
	В.о. завідувача кафедри	Людмила СНІГУР
	Гарант освітньої програми	Маріанна ТОДОРОВА
	Викладачі:	Сергій СТАЙКУЦА Світлана ВОРОНОВА