СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Соціальна інженерія

Рівень вищої освіти	Перший (бакалаврський)
Код та назва спеціальності	F6 Інформаційні системи та технології;
Галузь знань	F Інформаційні технології
Тип та назва освітньої програми	Освітньо-професійна програма «Прикладні інформаційні системи та технології»
Статус навчальної дисципліни	Обов'язкова компонента (ОК-9)
Курс, семестр викладання	1 курс, 2 семестр
Трудомісткість навчальної дисципліни	4 кредити ЄКТС (120 академічних годин), з них: Денна (очна) форма навчання: лекц. – 20 год., практ. зан. – 24 год., самост. роб. – 76 год.; Заочна форма навчання: лекц. – 12 год., практ. зан. – 12 год., самост. роб. – 96 год.
Мова викладання	Українська
Кафедра	Кіберпсихологія та реабілітація
Факультет	Бізнесу та соціальних комунікацій

Розробники / викладачі

СТАЙКУЦА Сергій Володимирович,
доцент кафедри кібербезпеки та технічного захисту інформації (КБ та ТЗІ),
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)

Загальна інформація про дисципліну	
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-2**. Здатність застосовувати знання у практичних ситуаціях. **ЗК-6.** Здатність до пошуку, оброблення та аналізу інформації з різних джерел. **ЗК-9.** Здатність реалізовувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні. **СК-6.** Здатність використовувати сучасні інформаційні системи та технології (виробничі, підтримки прийняття рішень, інтелектуального аналізу даних та інші), методики й техніки кібербезпеки під час виконання функціональних завдань та обов'язків.
Програмні результати навчання	**ПРН-19**. Застосовувати у професійній комунікації державну й іноземні мови та розуміти вплив технічних рішень в суспільному, економічному, соціальному і екологічному контексті.

Програма навчальної дисципліни	
Тема 1. ***Концептуальні основи соціальної інженерії***	Сутність феномену «соціальна інженерія». Історія розвитку соціальної інженерії. Місце соціальної інженерії у системі інформаційної безпеки. Принципи соціальної інженерії. Сфери застосування концепції OSINT. Етичні аспекти соціальної інженерії. Розуміння 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. ***Особистісно-психологічний захист: методи та техніки***	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 стійкості. Емоційний самоконтроль. Стратегії захисту від атак. Етичні та правові аспекти особистісного захисту.
Тема 4. ***Симуляційні ігри як метод***	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:

формування навичок протидії соціоінженерним атакам	«Фішинг-полювання», «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 другому 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 (А) – від 90 до 100 балів** – здобувач вільно володіє всіма теоретичними поняттями та методами соціальної інженерії, демонструє глибоке розуміння психологічних механізмів впливу; усі (або не менше 90%) завдання виконує самостійно, без суттєвих помилок, із творчим підходом та обґрунтованими висновками; вміє аналізувати складні кейси, пропонує оригінальні рішення, впевнено застосовує набуті знання на практиці; демонструє високий рівень комунікативних навичок, ефективну роботу в команді, бере активну участь у дискусіях, аргументовано захищає власну позицію; виявляє ініціативу, відповідальність, здатність до самостійної роботи, дотримується етичних норм. **Дуже добре (В) – від 82 до 89 балів** – здобувач упевнено володіє знаннями основних понять і методів, здатен застосовувати їх у типових і складних ситуаціях; виконує переважну більшість завдань (82-89%), можливі незначні неточності, які не впливають на загальний результат; аргументовано аналізує ситуації, демонструє здатність до критичного мислення та самостійного прийняття рішень; вміє працювати у групі, бере участь у дискусіях, може презентувати результати роботи; виявляє відповідальність та ініціативу, дотримується академічної доброчесності. **Добре (С) – від 74 до 81 балів –** здобувач володіє знаннями основних понять, уміє застосовувати їх у стандартних ситуаціях; завдання виконує переважно вірно (74-81%), є окремі помилки або неточності, що виправляються після зауважень; може аналізувати прості кейси, пропонувати стандартні рішення; бере участь у груповій роботі, але потребує підтримки; виконує вимоги щодо самостійності та етики, але не проявляє ініціативу.

	Задовільно (D) – від 64 до 73 балів – здобувач базово розуміє основні поняття; частково володіє методами соціальної інженерії; завдання виконує частково (64-73%), є суттєві помилки, які впливають на якість результату; аналізує кейси поверхнево; приймає рішення типово, без глибокого обґрунтування; може працювати у групі лише за підтримки викладача чи одногрупників; самостійність та відповідальність на мінімальному рівні. **Задовільно (E) – від 60 до 63 балів –** здобувач має знання та навички на межі допустимого рівня, значну кількість помилок у виконанні завдань; завдання виконані лише частково (60-63%), багато пропусків, поверхневий аналіз; відсутні самостійність, ініціатива, слабка участь у груповій роботі; потребує постійного контролю та допомоги з боку викладача. **Незадовільно з можливістю повторного складання (FX) – від 35 до 59 балів –** здобувач виявляє недостатній рівень знань і навичок, більшість завдань виконано неправильно або не виконано (35-59%); не розуміє ключових понять, не здатен аналізувати навіть прості ситуації; не бере участі у груповій роботі, не проявляє відповідальності; потребує суттєвого доопрацювання матеріалу та повторного вивчення окремих тем. **Незадовільно з обов'язковим повторним вивченням дисципліни (F) – від 0 до 34 балів –** здобувач виявляє відсутність знань і навичок з дисципліни, завдання не виконані або виконані формально (0-34%); не розуміє основних понять, не здатен виконати навіть найпростіші завдання; відсутня участь в освітньому процесі, ігнорує вимоги викладача; не дотримується принципів академічної доброчесності.
Форма та методи контролю навчальних досягнень	Контроль успішності навчання здобувачів освіти здійснюється на засадах відкритості та академічної доброчесності. В межах даної дисципліни передбачено два види контролю: поточний (*тематичний, рубіжний*) та підсумковий *(семестровий)*. ***Поточний контроль*** здійснюється протягом семестру під час проведення практичних занять; виконання завдань самостійної роботи; складання тематичних контрольних робіт, тестів тощо. Поточний контроль спрямований на перевірку: рівня підготовленості здобувача до занять; активності під час обговорення навчального матеріалу; якості виконання індивідуальних, практичних і тестових завдань; своєчасності та повноти виконання самостійної роботи. Результат поточного оцінювання є середньоарифметичним значенням отриманих балів за всі виконані завдання під час аудиторних (практичні, семінарські) занять та завдання, що виконуються під час самостійної роботи. До підсумкового контролю допускаються здобувачі, які за результатами поточного оцінювання набрали не менше 60 балів. ***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 залік. Також важливо своєчасно виконувати індивідуальні завдання, передбачені програмою дисципліни в рамках самостійної роботи.
Дотримання принципів академічної	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

доброчесності	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 / С. Хаджирадєва, Ю. Левін, М. Тодорова, М. Атанасов, В. Кононович, Ю. Кузьменко, М. Пальчинська, С. Стайкуца, Н. Шиліна, О. Чукурна, Л. Цибух, Г. Ятвецька; ред.: С. Хаджирадєва. Одеса : Астропринт, 2024. 239 с.
- Соціальна інженерія та кібербезпека : монографія / Авт. кол. : В. Г. Кононович, С. В. Стайкуца, М. М. Тодорова, С. В. Воронова, О. М. Рябуха. Одеса : ДУІТЗ, 2025. 320 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 «Інженерія програмного забезпечення», «Комп'ютерні науки», «Кібербезпека та захист інформації», «Прикладні інформаційні системи та технології», «Комп'ютерні мережі та Інтернет» зі спеціальності F2 Інженерія програмного забезпечення, F3 Комп'ютерні науки, F5 Кібербезпека та захист інформації, F6 Інформаційні системи та технології, F7 Комп'ютерна інженерія; 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 — Роман ЦАРЬОВ

Викладачі: Сергій СТАЙКУЦА

Світлана ВОРОНОВА