МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КОМП’ЮТЕРНИХ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ЗАТВЕРДЖУЮ
Декан факультету
_____ Інна КОНДЮС
«29» серпня 2026 р.

ЗАТВЕРДЖУЮ
Перший проректор
_____ Надія КОВАЛЬЧУК
«29» серпня 2026 р.

СИЛАБУС

з освітнього компонента «Соціальна інженерія»
ступінь вищої освіти – бакалавр
галузь знань – 12 Інформаційні технології
спеціальність – 123 Комп'ютерна інженерія
освітня програма – Комп'ютерна інженерія

Кафедра кібербезпеки

Силабус склав(ла) старший викладач кафедри кібербезпеки Оксана МІСКЕВИЧ

Силабус затверджений на засіданні кафедри кібербезпеки, протокол № 2 від «29» серпня 2026 р.

Завідувач кафедри к.т.н., доцент Сергій КОСТЮЧКО

Розглянуто та схвалено групою забезпечення освітньої програми «Комп'ютерна інженерія», протокол № 2 від «27» серпня 2026 р.

Гарант ОП «Комп'ютерна інженерія» к.т.н., доцент Світлана ЛАВРЕНЧУК

Схвалено науково-методичною радою університету, протокол № 1/а від «29» серпня 2026 р.

Затверджений силабус онлайн:
https://e.lntu.edu.ua/syllabus/2063

Луцьк – 2026

СИЛАБУС ОСВІТНЬОГО КОМПОНЕНТА «Соціальна інженерія»

Освітня програма	Комп'ютерна інженерія
Галузь знань / Спеціальність	12 Інформаційні технології / 123 Комп'ютерна інженерія
Рівень вищої освіти	перший (бакалаврський)
Статус дисципліни	вибіркова
Мова викладання	українська
Обсяг	5 кредитів ECTS / 150 годин
Форма контролю	залік
Викладач(і)	старший викладач Оксана МІСКЕВИЧ електронна пошта: miskevych.o@lutsk-ntu.com.ua

1. Мета і завдання дисципліни

Мета: формування у студентів цілісного уявлення про психологічні аспекти, методи та засоби соціальної інженерії. Отримання знань та умінь необхідних для успішної боротьби з атаками, здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності.

Завдання: дати студентам 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. Студент повинен чітко 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.

Пререквізити: іноземна мова за професійним спрямуванням, правознавство.

2. Компетентності

СК01 — Здатність застосовувати законодавчу та нормативно правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі комп’ютерної інженерії.

СК18 — Здатність аналізувати безпеку мереж та вживати заходів для захисту даних

3. Структура дисципліни, розподіл годин, зв'язок тем з компетентностями

№	Назва теми	**Лекції** денна/ заочна	**Практ./ Семін./ лаб** денна/ заочна	**Самост. робота** денна/ заочна	**Разом**	**Методи навчання**	**Методи оцінювання**	**СК**
Змістовий модуль 1. Теоретико-методологічні основи соціальної інженерії								
1	Тема 1. Поняття, сутність та класифікація соціальної інженерії	4/1	4/1	10/10	18/12	МН1, МН2, МН4, МН6	МО2, МО4, МО9	СК01, СК18
2	Тема 2. Психологічні основи впливу	2/0,5	2/0,5	10/10	14/11	МН1, МН2, МН4, МН6	МО2, МО4, МО9	СК01, СК18

№	Назва теми	Лекції денна/ заочна	Практ./ Семін./ лаб денна/ заочна	Самост. робота денна/ заочна	Разом	Методи навчання	Методи оцінювання	СК
3	Тема 3. Класифікація атак і основні вектори	4/0,5	4/0,5	10/10	18/11	МН1, МН2, МН4, МН6	МО2, МО4, МО9	СК18
4	Тема 4. Життєвий цикл атаки та розвідка	4/0,5	4/0,5	10/10	18/11	МН1, МН2, МН4, МН6	МО2, МО4, МО9	СК01, СК18
5	Тема 5. Технічний вимір соціальної інженерії	2/0,5	2/0,5	10/10	14/11	МН1, МН2, МН4, МН6	МО2, МО4, МО9	СК18
Змістовий модуль 2. Захист, протидія та штучний інтелект в соціальній інженерії								
6	Тема 6. Захист, протидія та культура безпеки	4/0,5	4/0,5	10/10	18/11	МН1, МН2, МН4, МН6	МО2, МО4, МО9	СК18
7	Тема 7. Правові та етичні аспекти	2/0,5	2/0,5	5/20	9/21	МН1, МН2, МН4, МН6	МО2, МО4, МО9	СК01, СК18
8	Тема 8. Оцінювання та моделювання ризику соціальної інженерії	4/0,5	4/0,5	5/20	13/21	МН1, МН2, МН4, МН6	МО2, МО4, МО9	СК18
9	Тема 9. Соціальна інженерія та штучний інтелект	2/1	2/1	10/20	14/22	МН1, МН2, МН4, МН6	МО2, МО4, МО9	СК18
10	Тема 10. Заходи протидії соціальній інженерії	2/0,5	2/0,5	10/18	14/19	МН1, МН2, МН4, МН6	МО2, МО4, МО9	СК01
	Разом	**30/6**	**30/6**	**90/138**	**150/150**			

Легенда: СК — спеціальна (фахова) компетентність (номер за п. 2). Повне формулювання кожного коду наводиться в ОП / стандарті спеціальності.

Методи навчання: МН1 — словесний метод (лекція, дискусія, співбесіда тощо); МН2 — практичний метод (лабораторні та практичні заняття); МН4 — робота з навчально-методичною літературою (конспектування, тезування, анотування, рецензування, складання реферату); МН6 — самостійна робота (розв'язання завдань).

Методи оцінювання: МО2 — усне або письмове опитування; МО4 — тестування; МО9 — залік.

4. Цілі сталого розвитку

ЦСР 4 – Якісна освіта

5. Неформальна освіта

Рекомендовані курси, тренінги, стажування та інші: результати навчання, здобуті у формальній, неформальній чи інформальній освіті, можуть бути визнані відповідно до процедур ЛНТУ. Підтвердженнями можуть бути сертифікати тематичних тренінгів, вебінарів чи онлайн-курсів разом з описом досягнутих результатів навчання та, за потреби, коротке верифікаційне завдання або портфоліо.

6. Критерії та форми контролю

Оцінювання — за 100-бальною шкалою (національна шкала / ЄКТС). Підсумковий бал = поточний контроль (60 %) + модульний контроль (40 %).

Академічна доброчесність: самостійне виконання завдань; коректне посилання на джерела; позначення частин тексту, згенерованих засобами ШІ. Порушення академічної доброчесності не толеруються.

7. Зміст тем

Тема 1. Поняття, сутність та класифікація соціальної інженерії

1.Соціальна інженерія: визначення, сутнісні ознаки, місце в системі загроз.
2.Історичний контекст становлення дисципліни.
3.Базові терміни.
4. Формальна модель соціоінженерного впливу.
5. Психологічні передумови результативності (оглядово).

Тема 2. Психологічні основи впливу

1.Психологічна природа соціоінженерного впливу.
2.Принципи впливу за Р. Чалдіні.
3.Двосистемна модель ухвалення рішень.
4.Емоційні тригери.
5.Когнітивні упередження.
6.Модель імовірності опрацювання та контекстна відповідність.
7.Індивідуальні та ситуативні чинники сприйнятливості.

Тема 3. Класифікація атак і основні вектори

1.Підстави класифікації соціоінженерних атак.
2.Фішинг та його різновиди.
3.Компрометація ділового листування (BEC).
4.Атаки поза фішингом.
5.Фізичні вектори.
6.Сучасні вектори: квішинг, ClickFix, «зловмисник посередині».
7.Багатоканальність як визначальна тенденція.
8.Універсальні ознаки шахрайського звернення.

Тема 4. Життєвий цикл атаки та розвідка

1.Атака як багатоходовий процес: чотири етапи.
2.Зіставлення з моделями ланцюга ураження.
3.Етап 1. Розвідка: завдання, види, джерела.
4.Техніки розвідки в матриці ATT&CK та проблема їх невидимості.
5.Витоки даних як джерело розвідки.
6.Мінімізація цифрового сліду організації та персоналу.
7.Етап 2. Встановлення контакту та верифікація особи.
8.Етап 3. Експлуатація: технічні бар’єри та пауза на перевірку.
9.Етап 4. Завершення: журналювання, аномалії, звітування.
10.Практика: самооцінка поверхні розвідки.

Тема 5. Технічний вимір соціальної інженерії

1.Навіщо соціальній інженерії технічний шар.

2.Підроблені домени.
3. Гомогліфи та інтернаціоналізовані доменні імена.
4.Спуфінг відправника: три рівні поля «Від».
5.SPF і DKIM: механізми та їх межі.
6.DMARC і поняття узгодження.
7.Чому автентифікація пошти не зупиняє фішинг.
8.Автентифікація користувача: чому не всі методи рівні.
9.Загрози, що обґрунтовують перехід до фішинг-стійких методів.
10.Практичний мінімум для організації.

Тема 6. Захист, протидія та культура безпеки

1.Багаторівнева модель захисту.
2.Технічні контролі: функція та межі.
3.Процедури верифікації.
4.Навчання й обізнаність: що показують дослідження.
5.Симульовані фішингові кампанії: як робити правильно.
6.Система метрик.
7.Реагування на інциденти.
8.Культура безпеки та психологічна безпека.

Тема 7. Правові та етичні аспекти

1.Чому правова основа є обов’язковою частиною дисципліни.
2.Чотири принципи етичного тестування.
3.Кримінально-правовий контекст України.
4.Законодавство про захист інформації та персональних даних.
5.Міжнародні вимоги.
6.Документальне оформлення соціотехнічного тестування.
7.Пропорційність і мінімізація впливу.
8.Приватність учасників.
9.Відповідальне розкриття.
10.Етика в навчальному процесі.

Тема 8. Оцінювання та моделювання ризику соціальної інженерії

1.Від якісного оцінювання до вимірюваного.
2.Поведінковий напрям: предиктори сприйнятливості.
3.Стохастичний напрям: атака як імовірнісний процес.
4.Побудова марковської моделі соціоінженерного сценарію.
5.Числовий приклад: обчислення ймовірності компрометації.
6.Порівняння захисних заходів у межах моделі.
7.Чутливість ризику до окремих переходів.
8.Калібрування на реальних даних та його проблеми.
9.Неспостережність станів і приховані марковські моделі.
10.Суміжні підходи та межі застосування моделей.

Тема 9. Соціальна інженерія та штучний інтелект

1.Що саме змінює штучний інтелект.
2.Текстовий вимір: генерація переконливих повідомлень.
3.Спеціалізовані зловмисні інструменти: тверезий погляд.
4.Голос і відео: синтетичні медіа.
5.Чому «відчуття підробки» більше не працює.
6.Зміщення надійності до незалежного каналу.
7.Окремий випадок: відеозв’язок.
8.Агентні системи як наступний етап.
9.Штучний інтелект на боці захисту та його межі.
10.Правові та етичні рамки.
11.Практичний мінімум адаптації захисту.

Тема 10. Заходи протидії соціальній інженерії

1.Місце теми в курсі: від розуміння до впровадження.
2.Каталог контрзаходів: структура й картка заходу.
3.Технічні контрзаходи.
4.Процедурні контрзаходи.
5.Людські та організаційні контрзаходи.
6.Пріоритизація: як обирати заходи.
7.Залежності та правильний порядок упровадження.
8.Сценарні плейбуки.
9.Масштабування за розміром організації.
10.Залишковий ризик і підтримання програми.

8. Опис ІЗ/КПІЗ

Не передбачено навчальним планом.

9. Загальні вимоги

Освітній процес регулюється академічними правилами ЛНТУ. Здобувачі освіти зобов'язані ознайомитися з вимогами, визначеними Кодексом академічної доброчесності ЛНТУ та Політикою етичного використання штучного інтелекту в ЛНТУ, і дотримуватися принципів академічної доброчесності та етичного використання штучного інтелекту в освітній діяльності.

Академічна доброчесність. Учасники освітнього процесу зобов'язані дотримуватися Закону України «Про академічну доброчесність» від 18.12.2025 № 4742-IX та внутрішніх нормативних документів ЛНТУ. Не допускаються академічний плагіат, фабрикація, фальсифікація, привласнення авторства, несамостійне виконання завдань, а також недоброчесне використання результатів, згенерованих штучним інтелектом.

Використання штучного інтелекту. Інструменти штучного інтелекту можуть використовуватися для пошуку ідей, пояснення методів, попереднього структурування, мовного редагування та допоміжного аналізу неконфіденційних даних, якщо конкретне завдання не передбачає повністю самостійного виконання. Здобувач освіти має зазначати використаний інструмент, мету та етап його застосування, перевіряти факти й розрахунки та самостійно обґрунтовувати висновки.

10. Література

І. Навчально-методичні матеріали та розробки

Праці автора силабуса:

1. Теорія інформації та кодування: метод. вказівки до лабораторних занять для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Інформаційні системи та технології охорони і безпеки» галузі знань F (12) Інформаційні технології спеціальності F6 (126) Інформаційні системи та технології денної та заоч. форм навч. / уклад. С. В. Гринюк, О. І. Міскевич. Луцьк: ЛНТУ, 2026. 74 с. URL: https://repository.lntu.edu.ua/handle/123456789/4409

2. Соціальна інженерія: метод. вказівки до практичних занять для здобувачів першого (бакалаврського) рівня вищої освіти галузь знань 12 (F) Інформаційні технології денної та заоч. форм навч. / уклад. О. І. Міскевич. Луцьк: ЛНТУ, 2026. 75 с. URL: https://repository.lntu.edu.ua/handle/123456789/2927

3. Соціальна інженерія: конспект лекцій для здобувачів першого (бакалаврського) рівня вищої освіти галузі знань 12 (F) Інформаційні технології денної та заоч. форм навч. / уклад. О. І. Міскевич. Луцьк: ЛНТУ, 2025. 76 с. URL: https://repository.lntu.edu.ua/handle/123456789/627

ІІ. Наукові праці

Праці автора силабуса:

4. Багнюк Н. В., Мельник К. В., Бортник К. Я., Міскевич О. І., Карасійчук Д. Я. Автоматизація керування конфігураціями комп'ютерних систем за допомогою Ansible та підходу «Infrastructure

as Code». Комп’ютерно-інтегровані технології: освіта, наука, виробництво. 2026. № 63. С. 145-153. URL: https://repository.lntu.edu.ua/handle/123456789/3569

5. Pekh P., Geledchak V., Miskevych O. Розробка та дослідження моделі оптимального управління освітленням розумного будинку засобами Matlab. Комп’ютерно-інтегровані технології: освіта, наука, виробництво. 2026. № 62. С. 77–82. URL: https://repository.lntu.edu.ua/handle/123456789/4457

6. Багнюк Н. В., Лавренчук С. В., Міскевич О. І., Свистун Б. В. Реалізація системи «Розумний будинок» з використанням Bluetooth, Arduino та Android: від датчиків до мобільного інтерфейсу. Комп’ютерно-інтегровані технології: освіта, наука, виробництво. 2024. № 56. С. 86–92. URL: https://repository.lntu.edu.ua/handle/123456789/4491

7. Multiprocessing as a Way to Optimize Queries / N. Khrystynets, K. Melnyk, S. Lavrenchuk, O. Miskevych, S. Kostiuchko // Artificial Intelligence, Medical Engineering and Education. - Guangzhou, China, 2024. - Vol. 48. - P. 455 - 464. URL: https://repository.lntu.edu.ua/handle/123456789/701

8. Міскевич О. І. Аналіз роботи мережевих утиліт в командному вікні Windows. Комп’ютерно-інтегровані технології: освіта, наука, виробництво. 2023. № 50. С. 84–89. URL: https://repository.lntu.edu.ua/handle/123456789/4449

III. Інформаційні ресурси

9. Онлайн-курс. «Learn Social Engineering From Scratch» URL: https://www.udemy.com/ (дата звернення: 10.05.2026).

10. Онлайн-курс. «The Complete Social Engineering, Phishing, OSINT». URL: https://www.udemy.com/ (дата звернення: 12.05.2026).