МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Волинський національний університет імені Лесі Українки
Факультет інформаційних технологій і математики
Кафедра комп'ютерних наук та кібербезпеки

СИЛАБУС
вибіркового освітнього компонента
СОЦІАЛЬНА ІНЖЕНЕРІЯ
Підготовки першого (бакалаврського) рівня вищої освіти

Луцьк – 2026

Силабус нормативного освітнього компонента “Соціальна інженерія” підготовки бакалаврів

Розробники:
Чернящук Наталія Леонідівна, доктор педагогічних наук, професор, професор кафедри комп’ютерних наук та кібербезпеки

Погоджено
Гарант освітньо-професійної програми:  Чернящук Н.Л.

Силабус освітнього компонента затверджено на засіданні кафедри комп’ютерних наук та кібербезпеки

протокол № 6 від 15.01.2026 р.

Завідувач кафедри:  Гришанович Т. О.

І. Опис навчальної дисципліни

Найменування показників	Характеристика освітнього компонента
	Вибірковий
Денна форма навчання	Рік підготовки 2
150/5 кредитів	Семестр 3
	Лекції 10 год.
	Лабораторні 20 год.
	Самостійна робота 110 год.
ІНДЗ: немає	Консультації 10 год.
	Форма контролю: залік

ІІ Інформація про викладача

ПІП: Чернящук Наталія Леонідівна;
Науковий ступінь: доктор педагогічних наук;
Вчене звання: професор;
Посада: професор кафедри комп'ютерних наук та кібербезпеки;
Контактна інформація: Cherniashchuk.Nataliia@vnu.edu.ua
Дні занять: http://94.130.69.82/cgi-bin/timetable.cgi

ІІІ. Опис освітнього компонента

І. Анотація освітнього компонента. Освітній компонент «Соціальна інженерія» спрямований на формування у здобувачів освіти розуміння людського фактору в інформаційній безпеці, методів маніпулювання користувачами та способів протидії соціальним атакам. Курс охоплює теоретичні основи соціальної інженерії, аналіз типових сценаріїв атак, психологічні та технічні аспекти обману, а також практичні методи захисту організацій від несанкціонованого доступу та витоку інформації. У результаті навчання студенти набувають компетенцій для оцінки ризиків, розробки стратегій підвищення кіберстійкості персоналу та впровадження заходів протидії соціальним загрозам.

ІІ. Мета і завдання освітнього компонента: сформувати у здобувачів освіти системне розуміння принципів соціальної інженерії, людського фактору у інформаційній безпеці та методів захисту від маніпуляцій і шахрайських атак. Завдання освітнього компонента: ознайомити з теоретичними основами соціальної інженерії та психології маніпуляцій; проаналізувати типові сценарії соціальних атак і методи їх виявлення; розвинути навички оцінки ризиків, пов'язаних із людським фактором, та впровадження превентивних заходів; сформувати компетенції з розробки стратегій підвищення обізнаності персоналу та захисту організації від соціальних атак; підвищити критичне мислення та етичну відповідальність у контексті інформаційної безпеки.

ІІІ. Soft skills.

Комунікаційні навички – вміння ефективно взаємодіяти з людьми, слухати та доносити інформацію, що важливо для розуміння і протидії соціальним атакам.

Аналітичне та критичне мислення – здатність оцінювати поведінку користувачів, виявляти потенційні загрози та об'єктивно аналізувати ситуації.

Проблемне мислення та прийняття рішень – швидка реакція на інциденти, планування превентивних заходів.

Етична відповідальність – дотримання етичних стандартів та законодавства під час роботи з інформацією та людьми.

Навички командної роботи – здатність працювати у групі для підвищення кіберстійкості організації та проведення навчань для персоналу.

IV. Структура освітнього компонента

Програма навчальної дисципліни складається з таких **змістових модулів**:

1. Соціальна інженерія: концепції, методи та захист.

Практика соціальної інженерії та захисні стратегії.

Назви змістових модулів і тем	Кількість годин					Форма контролю / бали
	Усього	у тому числі				
		Лек.	Лаб.	Сам. роб.	Конс.	
1. **Змістовий модуль 1.** Соціальна інженерія: концепції, методи та захист						Тестовий контроль знань / 15
Тема 1. Концепції та принципи соціальної інженерії.	11	1	2	10	1	Звіт по лаб. роботі /5
Тема 2. Психологія соціальної інженерії.	11	1	2	10	1	Звіт по лаб. роботі /5
Тема 3. Основні схеми впливу соціальної інженерії	11	1	2	10	1	Звіт по лаб. роботі /5
Тема 4. Методи та джерела для збору інформації	11	1	1	10	1	Звіт по лаб. роботі /5
Тема 5. Визначення цілі атаки соціального інженера	11	1	1	10	1	Звіт по лаб. роботі /5
Тема 6. Методи та інструменти соціальної інженерії	10	1	1	10	1	Звіт по лаб. роботі /5
Тема 7. Профілактика та пом'якшення наслідків атак соціальної інженерії	10	1	1	10	1	Звіт по лаб. роботі /5
Разом за змістовим модулем 1	75	7	10	70	7	50
Змістовий модуль 2. Практика соціальної інженерії та захисні стратегії**.**						Тестовий контроль знань / 15
Тема 5. Визначення цілі атаки соціального інженера	15	1	2	10	1	Звіт по лаб. роботі /7
Тема 6. Методи та інструменти соціальної інженерії	15	1	2	10	1	Звіт по лаб. роботі /7
Тема 7. Профілактика та пом'якшення наслідків атак соціальної інженерії	15	1	2	10	1	Звіт по лаб. роботі /7
Тема 8. Аудит соціальної інженерії	15		2	5		Звіт по лаб. роботі /7
Тема 9. Стратегія захисту від атак	15		2	5		Звіт по лаб. роботі /7
Разом за змістовим модулем 2	75	10	10	40	3	50
Всього годин/Балів	**150**	**24**	**20**	**110**	**10**	150 год. / 100 балів

Завдання для самостійного опрацювання

№ з/п	Тема	Кількість годин
1	Підготовка до лабораторних робіт	**25**
2	Опрацювання лекційного матеріалу	**25**
3	Оформлення результатів лабораторних робіт	**20**
4	Систематизація здобутих знань перед екзаменом	**20**
5	Робота з літературою в бібліотеці	**20**
	Разом	**110**

IV. Політика оцінювання

Політика викладача щодо здобувача освіти

Усі учасники освітнього процесу зобов'язані дотримуватись вимог чинного законодавства України, Статуту та Правил внутрішнього розпорядку Волинського національного університету імені Лесі Українки, а також загальноприйнятих норм академічної етики, корпоративної культури та взаємоповаги.
Під час занять з ОК «Соціальна інженерія» підтримується атмосфера співпраці, відкритості, відповідальності й толерантності. Очікується активна участь студентів у лекційних і лабораторних заняттях, своєчасне виконання індивідуальних та групових завдань, дотримання графіка навчання та вимог до оформлення робіт.
Недопустимими є запізнення, використання мобільних пристроїв не за навчальним призначенням, плагіат, списування, підміна особи та будь-які прояви порушення академічної доброчесності. Усі лабораторні, самостійні й підсумкові завдання виконуються із використанням засобів дистанційного курсу дисципліни в системі Moodle.
Викладач гарантує прозорість та об'єктивність оцінювання, надання зворотного зв'язку, створення комфортних умов для засвоєння матеріалу й розвитку професійних і комунікаційних компетентностей здобувачів освіти.

Політика щодо академічної доброчесності.

Академічна доброчесність базується на засудженні практик списування (виконання письмових робіт із залученням зовнішніх джерел інформації, крім дозволених для використання), плагіату (відтворення опублікованих текстів інших авторів без зазначення авторства), фабрикації (вигадування даних чи фактів, що використовуються в освітньому процесі). У разі порушення здобувачем вищої освіти академічної доброчесності (списування, плагіат, фабрикація), робота оцінюється незадовільно та має бути виконана повторно, а результати раніше зданих робіт анулюються і виконуються повторно у порядку визначеному викладачем. При цьому викладач залишає за собою право змінити завдання.

Політика дедлайнів та перескладання.

Роботи, які здаються із порушенням термінів без поважних причин оцінюються на нижчу оцінку. Перескладання модулів відбувається із дозволу лектора за наявності поважних причин (наприклад, лікарняний).

Можливість визнання результатів навчання, отриманих у формальній, неформальній та інформальній освіті.

Під час вивчення освітнього компонента можливе визнання результатів навчання отриманих у формальній, неформальній та/або інформальній освіті. Порядок визнання результатів навчання для здобувачів вищої освіти, набутих у: формальній освіті (академічна мобільність студентів на території України чи поза її межами, для студентів, які переводяться, поновлюються з інших ЗВО (вітчизняних чи іноземних); неформальній та/або інформальній освіті здійснюється згідно «ПОЛОЖЕННЯ про визнання результатів навчання, отриманих у формальній, неформальній та/або інформальній освіті у Волинському національному університеті імені Лесі Українки».

Можливість отримати додаткові бали.

Здобувачі освіти можуть отримати додаткові бали за активну участь у навчальному процесі, своєчасне та якісне виконання практичних і самостійних завдань, ініціативність під час обговорень, а також за виконання завдань підвищеної складності. Додаткові бали можуть нараховуватися за: участь у науково-дослідній діяльності, конференціях, олімпіадах або конкурсах з питань інформаційної безпеки; розробку власних мініпроєктів або практичних рішень з кіберзахисту; створення навчальних матеріалів, презентацій чи довідників для одногрупників; відвідування всіх занять без пропусків та активну участь у лекціях і практичних заняттях. Нарахування додаткових балів здійснюється в межах, визначених критеріями оцінювання, і не може перевищувати граничне значення, передбачене системою оцінювання дисципліни.

V. Підсумковий контроль

Оцінювання здійснюється за 100-бальною шкалою і включає поточний контроль (активність на заняттях, лабораторні роботи) – до 70 балів, та підсумковий контроль (тести) – 30 балів. Для допуску до підсумкового контролю студент повинен набрати не менше 35 балів під час поточного оцінювання та виконати всі лабораторні роботи. Студенти, які набрали 75 і більше балів за семестр і виконали всі завдання, можуть отримати підсумкову оцінку без складання іспиту.

Питання, які виносяться на залік під час ліквідації академічної заборгованості.

1. Загальні поняття щодо інформаційної безпеки
2. Основні поняття та визначення дисципліни
3. Основні нормативно-правові документи України у сфері ІБ
4. Основні ненавмисні штучні загрози
5. Основные навмисні штучні загрози
6. Класифікація загроз безпеки
7. Опис моделі гіпотетичного порушника
8. Види інформації, що захищається у сфері управління
9. Контроль якості захисту інформації
10. Класифікаційна політика у сфері інформації
11. Джерела загроз інформаційної безпеки
12. Сертифікація: створення захищеної роботи
13. Відмінності мережі від обчислюваного центру
14. Характеристика ефективних стандартів щодо безпеки
15. Усна форма разповсюдження матеріалів із стандартів по ІБ
16. Визначення вразливих місць персонального комп’ютера
17. Мережевий захист ПК
18. Планування безпечної роботи на ПК
19. Принципи інженерно-технічного захисту інформації
20. Методи захисту інформації технічними засобами
21. Канали витоку інформації
22. Засоби забезпечення ІБ в комп’ютерних системах
23. Стратегії комплексного захисту інформації

VI. Шкала оцінювання

Шкала оцінювання (національна та ECTS)

Оцінка в балах	**Лінгвістична оцінка**	**Оцінка за шкалою ECTS**	
		оцінка	**пояснення**
90–100	Відмінно	A	відмінне виконання
82–89	Дуже добре	B	вище середнього рівня
75–81	Добре	C	загалом хороша робота
67–74	Задовільно	D	непогано
60–66	Достатньо	E	виконання відповідає мінімальним критеріям

0–59	Незадовільно	Fx	Необхідне перескладання

VII. Рекомендована література та інтернет-ресурси

1. Bravo, C., & Toska, D. (2023). *The Art of Social Engineering: Uncover the Secrets Behind the Human Dynamics in Cybersecurity*. Packt Publishing.
   Комплексне дослідження психологічних аспектів соціальної інженерії та методів захисту від атак.
2. HL, V., & V, V. (2024). *Social Engineering in Cybersecurity: Threats and Defenses*. CRC Press.
   Глибокий аналіз різноманітних атак соціальної інженерії та стратегій їх запобігання.
3. Shapiro, S. J. (2023). *Fancy Bear Goes Phishing: The Dark History of the Information Age, in Five Extraordinary Hacks*. Farrar, Straus and Giroux.
   Історичний огляд п’яти значущих випадків хакерських атак, що ілюструють розвиток кіберзагроз.
4. Rathod, T. (2025). *A Comprehensive Survey on Social Engineering-Based Attacks*. Elsevier.
   Систематичний огляд досліджень, присвячених методам, моделям та фреймворкам соціальної інженерії.
5. Akeiber, H. J. (2025). *The Evolution of Social Engineering Attacks: A Cybersecurity Engineering Perspective*. Rafidain Journal of Engineering Sciences.
   Аналіз еволюції атак соціальної інженерії з акцентом на використання штучного інтелекту та технологій deepfake.
6. Waelchli, S. (2025). *Reducing the Risk of Social Engineering Attacks Using SOAR Technology*. ScienceDirect.
   Вивчення використання технологій SOAR для зменшення вразливості до атак соціальної інженерії.
7. Veitaitė, I. (2024). *The Impact of Social Engineering*. SCSA Journal.
   Оцінка впливу атак соціальної інженерії на організації та стратегії їх мінімізації.
8. Prajapati, P. (2024). *Social Engineering*. SSRN.
   Дослідження механізмів соціальної інженерії, включаючи фішинг, преекстинг та імперсонацію.
9. Wibowo, B. (2024). *Social Engineering as a Major Cybersecurity Threat*. Sultan Publisher.
   Аналіз викликів, з якими стикаються організації при захисті від атак соціальної інженерії.
10. Chetioui, K., Bah, B., Alami, A. O., & Bahnasse, A. (2021). *Overview of Social Engineering Attacks on Social Networks*. ResearchGate.
    Огляд атак соціальної інженерії в контексті соціальних мереж.
11. Palo Alto Networks. (2025). *2025 Unit 42 Global Incident Response Report: Social Engineering Edition*.
    Аналіз тенденцій атак соціальної інженерії та їх вплив на кібербезпеку.
12. Proofpoint. (2025). *The Human Factor 2025: Vol. 1 Social Engineering*.
    Дослідження поєднання технологій та психології в атаках соціальної інженерії.
13. CrowdStrike. (2025). *2025 Global Threat Report*.
    Огляд нових загроз у кіберпросторі, зокрема атак соціальної інженерії.
14. IBM. (2025). *IBM X-Force 2025 Threat Intelligence Index*.
    Інсайти щодо змінюваного ландшафту загроз та стратегії кіберзахисту.
15. World Economic Forum. (2025). *Global Cybersecurity Outlook 2025*.
    Прогнозування тенденцій у сфері кібербезпеки та викликів, зокрема у контексті соціальної інженерії.