Міністерство освіти і науки України
Луцький національний технічний університет

ПРОФЕСІЙНА ЕТИКА В ІТ-СФЕРІ

Методичні вказівки до лабораторних робіт
для здобувачів першого (бакалаврського) рівня вищої освіти
галузі знань F Інформаційні технології
всіх спеціальностей
денної та заочної форм навчання

Луцьк 2025

УДК 004:174
У П-73

Рекомендовано до видання вченою радою факультету КІТ ЛНТУ,
протокол № _____ від «__ » _____ 20 25 року.

Голова вченої ради факультету КІТ _____ Інна КОНДІУС

Електронна копія друкованого видання передана для внесення в репозитарій ЛНТУ
Директор бібліотеки _____ Наталія ПОЛІЩУК

Розглянуто і схвалено на засіданні кафедри комп'ютерної інженерії та безпеки ЛНТУ, протокол № _____ від « _____ » _____ 20 25 року.

Завідувач кафедри КІБ _____ Тарас ТЕРЛЕЦЬКИЙ

Укладачі: _____ Микола ПОЛІЩУК, кандидат технічних наук, доцент кафедри комп'ютерної інженерії та безпеки ЛНТУ

_____ Лілія ПОЛІЩУК, провідний фахівець навчально-меточного відділу ЛНТУ

Рецензент: _____ Олег КАЙДИК, кандидат технічних наук, доцент кафедри комп'ютерної інженерії та безпеки ЛНТУ

_____ Олег КУЛАКЕВИЧ директор ТОВ «РЕДВІНГ СТУДІО»

Відповідальний за випуск: _____ Тарас ТЕРЛЕЦЬКИЙ, кандидат технічних наук, доцент кафедри комп'ютерної інженерії та безпеки ЛНТУ

У П-73 Професійна етика в ІТ-сфері: методичні вказівки до лабораторних робіт для здобувачів першого (бакалаврського) рівня вищої освіти галузі знань F Інформаційні технології всіх спеціальностей денної та заочної форм навчання / уклад. М. М. Поліщук, Л. О. Поліщук: ЛНТУ, 2025. 44 с.

Методичні вказівки до лабораторних робіт «Професійна етика в ІТ-сфері»: складене відповідно до діючої програми курсу.

Призначене для здобувачів вищої освіти всіх спеціальностей галузі знань F Інформаційні технології

ЗМІСТ

ВСТУП

Сучасне інформаційне суспільство вимагає від фахівців IT-сфери не лише високого рівня технічної підготовки, а й дотримання етичних норм та стандартів. З огляду на це, навчальна дисципліна «Професійна етика в IT-сфері» покликана сформувати у майбутніх фахівців усвідомлення соціальної відповідальності, здатність до етичного прийняття рішень та забезпечення безпеки даних, конфіденційності, недоторканності приватного життя користувачів інформаційних систем.

Методичні вказівки призначені лабораторних робіт. Вони містять опис практичних завдань, тематику робіт, орієнтовні питання для обговорення, приклади етичних дилем і критерії оцінювання.

Мета дисципліни – формування в здобувачів освіти системи знань щодо етичних аспектів діяльності у сфері IT, розвиток критичного мислення, здатності до вирішення професійних конфліктів, усвідомлення соціальної відповідальності IT-спеціаліста в умовах цифрового суспільства.

Методичні вказівки є типовими, проте у разі необхідності за погодженням із викладачем або кафедрою комп’ютерної інженерії та безпеки можуть бути внесені зміни до окремих завдань або вимог.

Методичні вказівки до лабораторних робіт призначені для здобувачів першого (бакалаврського) рівня вищої освіти всіх спеціальностей галузі знань F Інформаційні технології

ЛАБОРАТОРНА РОБОТА 1
ВИНИКНЕННЯ ТА РОЗВИТОК ПРОФЕСІЙНОЇ ЕТИКИ В IT-СФЕРІ: ПРИЗНАЧЕННЯ В СУСПІЛЬСТВІ

Мета роботи – сформувати в здобувачів освіти уявлення про витоки, етапи становлення та значення професійної етики в інформаційно-комунікаційній сфері; показати її роль у забезпеченні довіри, відповідальності та безпеки в цифровому суспільстві.

Завдання 1.1 Історичний аналіз

Опрацюйте джерела (заздалегідь рекомендовані викладачем або знайдені самостійно) та побудуйте хронологічну шкалу (таймлайн) ключових етапів розвитку професійної етики в IT (від появи перших комп'ютерних кодексів до сучасних стандартів, як-от ACM Code of Ethics або ISO/IEC 27001).

Рекомендовані джерела для опрацювання:

1. Кодекс етики та професійної поведінки ACM. *ACM.* 2025. URL: https://www.acm.org/code-of-ethics

2. Кодекс етики IEEE. *IEEE.* 2025. URL: https://www.ieee.org/about/corporate/governance/p7-8

3. Кодекс етики та професійної практики програмної інженерії. *ACM.* 2025. URL: https://www.acm.org/code-of-ethics/software-engineering-code

Форма подачі: схематичне зображення і короткий коментар (до 200 слів).

Завдання 1.2 Аналітична дискусія

Розгляньте одне з наступних питань у мікрогрупі (3-4 особи), підготуйте коротку усну доповідь (до 3 хв):

1) Які соціальні наслідки неетичної поведінки IT-фахівців?

2) Чому в сучасному суспільстві етика в IT має не менше значення, ніж технічна компетентність?

Форма подачі: усна презентація або тези в письмовій формі.

Завдання 1.3 Есе / Рефлексія

Напишіть тези доповіді (300-400 слів) на одну з тем:

1) Чи може програміст бути морально відповідальним за наслідки використання його коду?

2) Як змінюється роль ІТ-спеціаліста в інформаційному суспільстві: технік чи етичний агент?

Форма подачі: тези, оформлені за вимогами (обсяг – 2-3 повних сторінок; формат аркуша А5; всі поля по 1,5 см; шрифт Times New Roman 11 пт; інтервал між рядками – 1, абзац – 1; перелік використаних джерел, на які є обов'язковими посилання в тексті, подається загальним списком у кінці рукопису згідно з вимогами ДСТУ 8302:2015).

Додаткові питання до захисту практичної роботи:

1) У чому полягає різниця між загальною етикою і професійною етикою ІТ-фахівця?

2) Чому поява етичних кодексів була зумовлена розвитком комп'ютерних технологій?

3) Які приклади можна навести як наслідки порушення професійної етики в історії ІТ?

4) Чи достатньо технічних стандартів безпеки без етичного мислення?

ЛАБОРАТОРНА РОБОТА 2
ЕТИЧНІ КОДЕКСИ ІТ-СПЕЦІАЛІСТІВ: СТАНДАРТИ ACM, IEEE, ISO/IEC 27001

Мета роботи – ознайомити здобувачів освіти зі змістом і структурою провідних етичних кодексів у сфері інформаційних технологій; навчити порівнювати їх та використовувати як орієнтири для прийняття етичних рішень у професійній діяльності.

Завдання 2.1 Порівняльний аналіз кодексів

Ознайомтесь із наступними етичними стандартами:

–ACM Code of Ethics and Professional Conduct;

–IEEE Code of Ethics;

–ISO/IEC 27001:2022 (етичні принципи у контексті управління інформаційною безпекою).

Порівняйте їх за такими критеріями:

–структура документа;

–ключові принципи;

–орієнтація на відповідальність/безпеку/чесність;

–практична значущість.

Форма подачі: таблиця з порівнянням та короткі висновки (до 1 сторінки).

Таблиця 2.1 – Порівняльний аналіз етичних кодексів ІТ-спеціалістів

Критерій	ACM Code of Ethics (2018)	IEEE Code of Ethics (2020)	ISO/IEC 27001:2022
структура документа	4 розділи, 25 принципів; структурований за рівнями відповідальності		
ключові принципи	шанобливість, чесність, конфіденційність, соціальна відповідальність		
орієнтація	висока етична відповідальність + соціальні аспекти		
практична значущість	застосовується при розробці ПЗ, AI, взаємодії з користувачами		

Завдання 2.2 Практичний кейс: застосування кодексу

Оберіть один із наведених кейсів або придумайте власний:

–розробник виявив, що керівництво змінює алгоритм без відома користувача для збору даних.

–працівнику запропонували взяти участь у створенні програми для несанкціонованого доступу.

На основі одного з етичних кодексів поясніть:

1) Які принципи порушено?

2) Як правильно діяти згідно з кодексом?

Форма подачі: письмове пояснення (до 300 слів) з посиланнями на статті кодексу.

Завдання 2.3 Вибір та аргументація

Уявіть, що ваша компанія впроваджує новий етичний стандарт. Який з трьох (ACM, IEEE, ISO/IEC 27001) ви б обрали як базовий? Обґрунтуйте вибір.

Форма подачі: усна аргументація.

Додаткові питання до захисту лабораторної роботи:

1) Яка головна мета створення етичного кодексу в IT-сфері?

2) Чим відрізняються підходи ACM і IEEE до формування етичних норм?

3) Які пункти ISO/IEC 27001 можуть трактуватись як етичні, а не лише технічні?

4) Чи має компанія право формувати власний внутрішній кодекс етики замість існуючих стандартів?

ЛАБОРАТОРНА РОБОТА 3
ЕТИКА РОЗРОБНИКІВ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА СИСТЕМНИХ ІНЖЕНЕРІВ

Мета роботи – ознайомити студентів із професійно-етичними нормами, притаманними діяльності розробників ПЗ та системних інженерів; навчити ідентифікувати та аналізувати етичні дилеми, що виникають у процесі технічної реалізації рішень.

Завдання 3.1 Аналіз етичного кейсу

Проаналізуйте наведений приклад: розробник працює над програмою, яка передає дані користувача третім особам без явної згоди. Керівництво вимагає залишити цю функцію. Ваші дії як професійного розробника:

1) Які етичні принципи порушено?

2) Які документи (ACM/IEEE/внутрішні політики) можуть вас підтримати?

3) Як знайти компроміс між технічним завданням і етичними нормами?

Форма подачі: письмовий аналіз (до 1 сторінки), з посиланням на етичні стандарти.

Завдання 3.2 Модель поведінки в конфлікті ролей

Опишіть приклад ситуації, коли системний інженер чи розробник потрапляє в конфлікт ролей (наприклад, між інтересами компанії та користувача; між швидкістю розробки й безпечністю продукту).

Які варіанти дій? Який варіант ви б обрали і чому?

Форма подачі: усна доповідь або письмове обґрунтування.

Завдання 3.3 Кодекс етики розробника ПЗ

На основі міжнародних стандартів (ACM, IEEE, SECE, ISO) створіть власний міні-кодекс розробника програмного забезпечення, що містить 5 основних принципів поведінки та приклади, коли ці принципи можуть бути порушені.

Форма подачі: структурований документ до 1 сторінки.

Завдання 3.4 Системна етична дилема в архітектурі ПЗ

Уявіть, що ви – головний інженер великої IT-компанії, яка розробляє хмарну платформу для медичних установ. Підрядник пропонує прискорити реалізацію функціоналу, що обробляє персональні медичні записи, за рахунок спрощення процедур шифрування. Це дозволить вкластися в терміни, але потенційно знижує рівень захисту.

Ваші завдання:

1) визначте етичні ризики цього рішення (на рівні безпеки, відповідальності, законодавства, репутації тощо);

2) зіставте технічні аргументи з етичними – хто є всіма зацікавленими сторонами?

3) запропонуйте етично обґрунтовану стратегію дій: як пояснити своє рішення керівництву та які компромісні варіанти можливі (захист, тестування, попередження користувача)?

4) обґрунтуйте свою позицію з опорою на міжнародні етичні кодекси та стандарти (ACM, IEEE, ISO/IEC 27001, GDPR тощо).

Форма подачі: аналітичний звіт (1,5-2 сторінки), структурований за пунктами (можна додати діаграму зацікавлених сторін (stakeholder map) або схему впливу рішень).

Додаткові питання до захисту лабораторної роботи:

1) Які типові етичні конфлікти виникають у роботі розробника ПЗ?

2) У чому полягає відповідальність системного інженера за проєктні рішення?

3) Як відрізнити професійну помилку від етичного порушення?

4) Яке значення має відкритий код (open-source) у контексті етики розробки?

5) Чи несе розробник відповідальність за використання його ПЗ третіми сторонами?

ЛАБОРАТОРНА РОБОТА 4
ЕТИКА РОБОТИ СПЕЦІАЛІСТІВ З КІБЕРБЕЗПЕКИ: ВІДПОВІДАЛЬНІСТЬ, ПРАВОВІ ОБМЕЖЕННЯ, МОРАЛЬНІ ДИЛЕМИ

Мета роботи – сформувати у здобувачів освіти розуміння етичних засад діяльності в галузі кібербезпеки, розглянути моральні конфлікти та юридичні обмеження, з якими стикаються фахівці при доступі до інформації, тестуванні систем та захисті критичної інфраструктури.

Завдання 4.1 Аналіз етичної дилеми «етичного хакера»

Розгляньте ситуацію: фахівець із кібербезпеки під час тестування внутрішніх мереж виявляє критичну уразливість у програмному забезпеченні, яка дозволяє отримати доступ до персональних даних викладачів університету. Керівництво просить не документувати її, щоб не викликати «зайвих перевірок».

Завдання:

1) Які етичні та юридичні аспекти порушено?

2) Яка відповідальність лежить на спеціалісті?

3) Як діяти згідно з етичними нормами (посилання на ISO/IEC 27001, NIST, законодавство України, GDPR)?

✎ Форма подачі: письмова відповідь до 1 сторінки.

Завдання 4.2 Ситуаційне завдання «Запрошений фахівець або зловмисник?»

Вас, як фахівця з кібербезпеки, наймає невелика компанія для тестування її веб-сервісу на предмет уразливостей. У договорі вказано лише загальні межі тестування, без чітких обмежень щодо часу, методів та глибини перевірки. Під час тестування ви виявляєте бекенд-сервер із відкритим доступом до бази користувачів, що містить ПІБ, паролі, медичні дані та фінансову інформацію.

Ви експлуатуєте цю уразливість, щоб зібрати доказову базу, знімаючи копії частини БД для подальшого звіту. За кілька днів компанія звинувачує вас у несанкціонованому копіюванні персональних даних і звертається до поліції.

Проаналізуйте, чи мали ви право виконати такі дії:

1) Які етичні принципи ви потенційно порушили?

2) Яких правових меж не було дотримано (враховуючи GDPR, ISO/IEC 27001, закон України «Про захист персональних даних»)?

Як ви могли б діяти по-іншому, залишаючись у межах:

1) закону;

2) професійної етики;

3) договірних зобов'язань.

Сформулюйте рекомендації для себе як фахівця:

1) Як чітко оформити межі тестування з клієнтом?

2) Як захиститися юридично на випадок конфлікту?

3) Яку частину результатів і як можна документувати етично?

Форма подачі: розгорнуте письмове пояснення (1,5-2 сторінки) з посиланням на нормативні акти та етичні кодекси.

Завдання 4.3 Етична карта дій при Penetration Testing

Складіть етичну дорожню карту (checklist або flowchart) дій фахівця з безпеки при проведенні penetration testing:

Має включати:

–згоду клієнта;

–межі тестування;

–обробка та зберігання отриманих даних;

–повідомлення про уразливості;

–поведінка у випадку виявлення незаконного контенту.

Форма подачі: візуальна схема або таблиця з поясненнями.

Завдання 4.4 Дискусійні тези «Коли захист перетворюється на напад?»

Проаналізуйте дилему між активним захистом (наприклад, зворотні атаки, traceback-інструменти, honeypots) і правовими/етичними обмеженнями.

1) Чи має фахівець право діяти на випередження?

2) Яка межа між захистом і «кіберпомстою»?

Форма подачі: тези до 2 сторінок.

Таблиця 4.1 – Етичні дії фахівця з кібербезпеки при проведенні Penetration Testing

Етап / дія	Мета / суть дії	Етичні принципи	Потенційні ризики	Коментар / примітка
отримання письмової згоди клієнта	узгодження меж, методів і тривалості тестування	законність, прозорість, добровільність	несанкціоноване втручання, судові наслідки	має бути підписано уповноваженою особою
визначення меж тестування				
поводження з виявленими даними				
реакція на критичну вразливість				
виявлення нелегального контенту				
документування та звітність				

Додаткові питання до захисту лабораторної роботи:

1) У чому полягає етична відповідальність спеціаліста з кібербезпеки?

2) Які юридичні рамки обмежують дії фахівця під час тестування системи?

3) Чи можна «етичний хакінг» вважати безумовно легальним?

4) Яка роль принципу «мінімального втручання» в роботі з конфіденційною інформацією?

5) Як захистити себе юридично, виконуючи роль penetration tester-а або адміністратора безпеки?

ЛАБОРАТОРНА РОБОТА 5
КОНФІДЕНЦІЙНІСТЬ, ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ТА ЦИФРОВА ПРИВАТНІСТЬ

Мета роботи – сформувати у здобувачів освіти розуміння важливості захисту персональних даних як етичної та юридичної норми в ІТ-сфері. Розвивати навички розпізнавання загроз цифровій приватності та оцінки відповідності діяльності принципам конфіденційності.

Завдання 5.1 Аудит політики конфіденційності

Оберіть сайт або сервіс (Google, Instagram, мобільний додаток тощо) та проаналізуйте його політику конфіденційності:

1) Які саме персональні дані збираються?

2) Для чого вони використовуються?

3) Чи є користувачі поінформованими?

4) Чи є відповідність політики GDPR / закону України «Про захист персональних даних»?

Форма подачі: таблиця-аналіз або короткий аналітичний звіт (1 сторінка).

Завдання 5.2 Симуляція витоку даних

Уявіть, що в ІТ-компанії, де ви працюєте, відбувся витік даних користувачів: ПІБ, електронна пошта, IP-адреса, медичні записи, фото. Зловмисник вимагає викуп, інакше дані буде викладено в даркнеті. Ваше завдання:

1) Які етичні дії має вжити ІТ-відділ?

2) Які кроки передбачає законодавство (у т.ч. обов’язок повідомлення)?

3) Як комунікувати з користувачами, не втрачаючи довіру?

Форма подачі: опис сценарію дій (до 1,5 сторінки) з посиланням на ISO/IEC 27001, GDPR.

Завдання 5.3 Порушення приватності: аналіз кейсу

Проаналізуйте кейс (реальний або уявний).

Популярний мобільний застосунок збирає дані геолокації, мікрофона та камери, навіть коли не використовується. Компанія пояснює це «покращенням досвіду користувача», але не попереджає про це явно.

Завдання:

1) Які принципи цифрової етики та конфіденційності порушено?

2) Як має діяти компанія?

3) Які санкції можливі згідно з GDPR / українським законодавством?

Форма подачі: письмовий аналіз (1 сторінка).

Додаткові питання до захисту лабораторної роботи:

1) Що таке «принцип мінімізації даних» у GDPR?

2) У чому різниця між згодою користувача та публічною офертою?

3) Як балансувати між персоналізацією сервісу та захистом приватності?

4) Які права має користувач згідно з українським законом «Про захист персональних даних»?

5) Чи є використання кукісів втручанням у приватність?

6) Таблиця 5.1 – Аналіз політики конфіденційності цифрового сервісу

Параметр	Опис / інформація з політики конфіденційності	Висновок щодо відповідності (GDPR / закон України)
які дані збираються?	наприклад: ім’я, email, IP, геолокація, біометрія, банківські дані тощо	повнота розкриття, прозорість
з якою метою дані обробляються?	наприклад: покращення сервісу, аналітика, реклама, передача партнерам	чи відповідає мета принципу обмеженої мети
чи запитується згода користувача?	чи передбачено checkbox / активацію згоди	відповідність принципу добровільної згоди
хто має доступ до даних?	внутрішні працівники, сторонні сервіси, партнери тощо	наявність опису сторін передачі
термін зберігання персональних даних	як довго зберігаються дані, чи прописано це в політиці	дотримання принципу обмеженого зберігання
права користувача	доступ, виправлення, видалення, відкликання згоди, перенесення даних	відповідність GDPR ст. 12–23 або українському законодавству
захист даних / безпека	чи згадано про шифрування, обмеження доступу, технічні заходи	оцінка технічного захисту даних
контакти для звернення / запитів	чи вказано DPO або контактну особу з питань приватності	(обов’язковий елемент відповідності)

ЛАБОРАТОРНА РОБОТА 6
ЕТИЧНІ АСПЕКТИ ДЕРЖАВНОГО ТА КОРПОРАТИВНОГО КОНТРОЛЮ В ІТ-СФЕРІ

Мета роботи – формування критичного мислення щодо меж допустимого контролю в цифровому середовищі. Ознайомлення здобувачів освіти з етичними дилемами, що виникають у процесі державного нагляду, масового спостереження та корпоративного моніторингу ІТ-активності користувачів.

Завдання 6.1 Держава як спостерігач: аналіз етичної дилеми

Опрацюйте наступний приклад: уряд України впроваджує систему автоматичного аналізу всіх повідомлень у месенджерах на наявність забороненого контенту. Система працює без згоди користувачів, мотивуючи це «національною безпекою». Завдання:

1) Проаналізуйте, які етичні принципи порушено.

2) Чи виправдовує «суспільне благо» втручання в особисту комунікацію?

3) Яка роль етичної прозорості у державних ІТ-проєктах?

Форма подачі: письмовий аналіз (до 1 сторінки).

Завдання 6.2 Корпоративний контроль працівників: порівняльний кейс

Порівняйте дві ситуації:

–компанія № 1 веде повну історію дій працівників на комп’ютері, включаючи зняття скріншотів кожні 30 секунд;

–компанія № 2 контролює лише доступ до службових систем і реєструє IP-з’єднання.

Завдання:

1) Чи є обидва підходи етичними?

2) Які ризики, переваги й правові наслідки?

3) Який із варіантів контролю є етично прийнятним?

Форма подачі: порівняльна таблиця та короткі відповіді на питання.

Таблиця 6.1 – Порівняння етичних аспектів корпоративного контролю

Критерій	Компанія №1 (повна історія дій + скріншоти)	Компанія №2 (контроль доступу + логування IP)
Рівень втручання в приватність		
Прозорість дій керівництва		
Можливість зловживань		
Етична доцільність		
Відповідність принципу «необхідності» (GDPR, ISO 29100)		
Потенційна реакція працівників		
Правові ризики (Україна, ЄС)		
Рекомендація (етична оцінка)		

Примітка: таблиця може бути розширена пунктами: «вплив на ефективність», «приклади практик в українських IT-компаніях», «наявність згоди працівників» тощо.

Завдання 6.3 Межі допустимого контролю в IT-сфері

1) Який рівень контролю ви вважаєте допустимим у державних і корпоративних структурах?

2) Де межа між етичним наглядом і вторгненням у приватність?

3) Як балансувати безпеку, ефективність і гідність людини в цифровому середовищі?

Форма подачі: звіт (до 5 сторінок).

Додаткові питання до захисту лабораторної роботи:

1) У чому різниця між моніторингом і стеженням?

2) Які етичні норми повинні діяти під час використання систем відеоспостереження чи логування дій користувачів?

3) Чи є працівник зобов’язаним погоджуватись на корпоративний контроль?

4) Як реалізувати принцип інформованої згоди в державних цифрових ініціативах?

5) Чи можуть алгоритми нести етичну відповідальність за рішення, прийняті в межах контролю?

ЛАБОРАТОРНА РОБОТА 7
СОЦІАЛЬНА ВІДПОВІДАЛЬНІСТЬ ІТ-КОМПАНІЙ ТА ВПЛИВ ТЕХНОЛОГІЙ НА СУСПІЛЬСТВО

Мета роботи – сформувати у здобувачів освіти розуміння соціальної відповідальності ІТ-компаній у контексті сталого розвитку, впливу технологій на суспільні процеси та моральних обов'язків перед користувачами й спільнотами. Ознайомити з практиками етичного технологічного лідерства.

Завдання 7.1 Аналіз практик соціальної відповідальності

Оберіть одну з провідних ІТ-компаній (Google, Microsoft, Meta, SoftServe, EPAM тощо) і проаналізуйте її соціальні ініціативи за такими критеріями:

–освіта і цифрова грамотність;

–захист довкілля;

–інклюзивність (доступність технологій);

–етичні інновації / відкриті стандарти.

Форма подачі: аналітична таблиця 7.1 або короткий звіт (до 1 сторінки).

Завдання 7.2 Критичний аналіз: технології як загроза або благо?

1) Як ІТ-технології змінюють соціальні відносини, освіту, зайнятість?

2) У чому полягає відповідальність компанії за соціальні наслідки технологій (наприклад, автоматизація, deepfake, алгоритмічна дискримінація)?

3) Якими мають бути етичні межі використання ШІ?

Форма подачі: короткі письмові відповіді на питання.

Завдання 7.3 Симуляція: ІТ-компанія і громада

Уявіть, що ваша ІТ-компанія планує відкрити дата-центр у місті. Громада занепокоєна: викиди тепла, шум, споживання електроенергії, мало робочих місць. Ваше завдання:

–підготуйте етичну позицію компанії: як переконати громаду?

–які ініціативи ви запропонуєте (екологія, локальні гранти, освітні проєкти)?

–як це вплине на репутацію компанії?

Форма подачі: міні-презентація або письмовий план дій (до 1,5 сторінки).

Таблиця – Соціальна відповідальність IT-компанії

Напрям	Опис ініціативи / політики компанії	Приклади (назви проєктів / дій)	Оцінка ефективності / етичної цінності
Освіта та цифрова грамотність	які програми підтримки освіти реалізуються?	наприклад, Google for Education, EPAM University, IT-школи для молоді	висока / помірна / низька (з коментарем)
Екологічна відповідальність	як компанія знижує вплив на довкілля?	зелена енергія, компенсація CO_2, дата-центри з водяним охолодженням	висока / помірна / декларативна
Інклюзивність та доступність	чи враховується доступність для осіб з інвалідністю, гендерна рівність?	адаптивний інтерфейс, політика Diversity&Inclusion, доступні вакансії	✓ / ✕ або коментар
Етичні технології / ШІ	чи існують публічні принципи етики AI / технологій?	наприклад, Google AI Principles, Microsoft Responsible AI	✓ / ✕ або стислий аналіз
Співпраця з громадами / благодійність	як компанія взаємодіє з місцевими громадами / НГО?	волонтерство, гранти, підтримка шкіл, бібліотек, ветеранів	✓ / ✕ або приклад
Відкритість та звітність	чи публікує компанія відкриті звіти CSR / ESG / етичних кодексів?	звіт за 2023 рік, ESG-стратегія, політика прозорості, публічні аудитори	✓ / ✕ + рік останнього звіту

Примітка: у колонці «Оцінка ефективності» бажано додати коментар: «Програма має сталі результати, охоплено понад 10 000 учасників», або «Ініціатива анонсована, але не має звіту».

Додаткові питання до захисту лабораторної роботи:

1) Що таке CSR (Corporate Social Responsibility) в IT-сфері?

2) Які ризики і вигоди несе соціальна активність IT-компаній?

3) Чи повинні IT-компанії брати участь у вирішенні екологічних чи освітніх проблем?

4) Чи має ШІ, розроблений компанією, діяти за універсальними етичними нормами?

1. У чому полягає відповідальність за вплив на громадську думку через алгоритми?

ЛАБОРАТОРНА РОБОТА 8
ДЕЗІНФОРМАЦІЯ, ЕТИЧНІ ПИТАННЯ В АЛГОРИТМАХ ТА ШТУЧНОМУ ІНТЕЛЕКТІ

Мета роботи – ознайомити здобувачів освіти з основними проблемами етики штучного інтелекту, алгоритмічного упередження та впливу ІТ-систем на поширення дезінформації. Сприяти формуванню здатності до виявлення потенційних етичних ризиків при проєктуванні та використанні алгоритмічних рішень.

Завдання 8.1 Виявлення упередження в алгоритмах

Оберіть один із прикладів використання алгоритмів (рекомендації в YouTube, кредитний скоринг, автоматичне розпізнавання обличь, автоматичний відбір резюме тощо).

Проаналізуйте:

1) Які ризики упередженості (gender, race, geography)?

2) Які наслідки для користувачів та суспільства?

3) Чи були випадки публічного скандалу (наведіть приклад)?

Форма подачі: аналітична записка (до 1 сторінки).

Завдання 8.2 Аналіз фейкових новин і дезінформації

Оберіть приклад дезінформаційної кампанії (український контекст, Covid-19, війна, deepfake-відео тощо).

Проаналізуйте:

1) Які технології/платформи були використані?

2) Як алгоритми соцмереж сприяли поширенню?

3) Що можна вжити для протидії на рівні розробника?

Форма подачі: короткий звіт та 1 слайд з пропозиціями протидії.

Завдання 8.3 Кодекс етики для AI-проєкту

Створіть міні-кодекс етики для умовного проєкту зі ШІ (наприклад, чат-бот, аналітична система для освітнього закладу, автоматичний модератор контенту). У вашому кодексі мають бути:

–принципи прозорості, справедливості, відповідальності;

–як буде реалізовано захист персональних даних;

–як уникатиметься упередження.

Форма подачі: структурований документ (до 1,5 сторінки).

Завдання 8.4 Етична дилема для розробника контент-фільтра

Ви – інженер з машинного навчання в IT-компанії, що розробляє модуль автоматичного модератора для соціальної мережі. Модель ШІ повинна виявляти та блокувати дезінформацію, мову ворожнечі, спам тощо.

Після запуску система починає блокувати:

–пости, що містять слова «війна», «окупація», «ЗСУ» – навіть коли йдеться про офіційні джерела;

–частину україномовного контенту через помилки у розпізнаванні мови;

–аналітичні новини, які розходяться з популярною думкою.

Менеджмент наполягає не змінювати алгоритм до релізу, оскільки «він ефективно знижує ризики».

Визначте:

1) Які етичні принципи порушуються в роботі алгоритму?

2) Які групи користувачів страждають від алгоритмічної упередженості?

Як діяти в цій ситуації як відповідальний інженер:

1) Чи слід зупинити реліз?

2) Як аргументувати свою позицію перед менеджментом?

3) Які кроки можна запропонувати для виправлення?

4) На які міжнародні стандарти / принципи ви спираєтесь? (наприклад, UNESCO AI Ethics, ACM Code, Google AI Principles, EU AI Act).

Форма подачі: аналітична записка (до 1,5 сторінки) зі структурованими відповідями. Бажано вказати пропозиції вдосконалення алгоритму, наприклад, пояснюваність, ручна перевірка, багатомовність, відкриті скарги.

Додаткові питання до захисту лабораторної роботи:

1) Що таке алгоритмічна упередженість і як вона виникає?

2) Чому важлива пояснюваність (explainability) у ШІ-моделях?

3) У чому полягає небезпека deepfake-технологій?

4) Як ІТ-фахівець може діяти етично, працюючи з навчальними вибірками?

5) Чи можуть ШІ-системи нести моральну відповідальність?

ЛАБОРАТОРНА РОБОТА 9
ДОТРИМАННЯ ЕТИЧНИХ НОРМ ПРИ СТВОРЕННІ ТА ВИКОРИСТАННІ ЦИФРОВИХ ТЕХНОЛОГІЙ

Мета роботи – сформувати в здобувачів освіти усвідомлення важливості етичного підходу на всіх етапах життєвого циклу цифрових продуктів – від проєктування до використання. Розглянути типові ситуації порушення етичних норм з боку розробників, власників платформи та кінцевих користувачів.

Завдання 9.1 Аналіз етичних помилок у цифровому продукті

Оберіть реальний випадок (або використайте запропонований) цифрового продукту або IT-сервісу, де було зафіксовано порушення етичних норм (наприклад, збір даних без згоди, некоректна модерація, приховане стеження, вбудовані маніпуляції тощо). Проаналізуйте:

1) У чому полягає етичне порушення?
2) Хто відповідальний за нього?
3) Які були наслідки для компанії/користувачів?
4) Які заходи виправлення були або могли б бути вжиті?

Форма подачі: короткий звіт або аналітична довідка до 1 сторінки (див. додаток А).

Завдання 9.2 Рольова симуляція «етична рада проєкту»

Уявіть, що ви – члени внутрішньої етичної ради IT-компанії. Вам представили новий продукт – додаток для моніторингу поведінки працівників у дистанційній роботі. Система відстежує активність клавіатури, вебкамеру, геолокацію. Завдання:

1) сформуйте етичну оцінку продукту;
2) які функції слід виключити або обмежити;
3) як можна зберегти функціональність продукту, дотримуючись етичних норм.

Форма подачі: протокол (див. додаток Б) / список етичних рекомендацій.

Завдання 9.3 Етичний чеклист для стартапу

Складіть контрольний список (checklist) з 10 етичних запитань, які має пройти новий цифровий продукт перед запуском.

Обов’язково включити питання щодо:

1) приватності;
2) конфлікту інтересів;
3) штучного інтелекту / автоматизації;
4) маніпулятивних інтерфейсів;
5) соціального впливу.

Форма подачі: таблиця та список із коротким поясненням.

Таблиця 9.1 – Зразок етичного чеклиста (checklist)

Питання	Так / ні / частково	Коментар / рекомендація
Чи збирає продукт лише ті дані, які дійсно необхідні?		Які саме дані? Чи можна скоротити обсяг збору?
Чи передбачено явну і добровільну згоду користувача на обробку даних?		Чи реалізовано checkbox / інформування згідно з GDPR?
Чи можна користувачу видалити свої дані або профіль у будь-який момент?		описати механізм – через інтерфейс, за запитом тощо
Чи має продукт механізм запобігання дискримінації або упередженості (ШІ)?		наприклад, гендер, мова, регіон. Чи перевірялися навчальні вибірки?
Чи повідомляє продукт, коли рішення приймає алгоритм або ШІ?		Чи реалізована пояснюваність (Explainable AI)?
Чи не використовуються маніпулятивні UX-практики («темні патерни»)?		наприклад, приховані кнопки, примусова підписка
Чи відомо користувачу, хто несе відповідальність за продукт?		контактна особа, публічна інформація про компанію
Чи враховує продукт потреби людей з інвалідністю (доступність)?		наприклад, підтримка екранних читачів, кольоровий контраст
Чи передбачена система швидкого реагування на інциденти (витік, скарги)?		Хто відповідає за це? Чи описано це в політиці?
Чи оцінювався можливий соціальний вплив продукту на громаду / ринок?		Чи можуть бути негативні наслідки? Як їм запобігають?

Примітка: для повної оцінки продукту необхідно обґрунтовувати відповіді в колонці «Коментар».

Додаткові питання до захисту лабораторної роботи:

1) У чому різниця між юридично допустимим і етично допустимим?

2) Яку відповідальність має нести розробник, якщо його продукт використовується в шкодочинних цілях?

3) Як побудувати довіру користувача до цифрового сервісу?

4) Чи можна виправдати етичні компроміси «для зручності» користувача?

5) Хто має перевіряти цифрові продукти на відповідність етичним стандартам?

ЛАБОРАТОРНА РОБОТА 10
КОНФЛІКТИ ІНТЕРЕСІВ ТА НЕЕТИЧНА ПОВЕДІНКА В IT-КОМАНДАХ

Мета роботи – сформувати в здобувачів освіти уявлення про типові форми конфліктів інтересів у професійному IT-середовищі, навчити виявляти та аналізувати неетичну поведінку в командах, а також виробити стратегії етичного реагування.

Завдання 10.1 Ідентифікація конфлікту інтересів

Ознайомтесь з кейсом: розробник працює над внутрішнім проєктом компанії, але паралельно створює схожий функціонал для власного фриланс-проєкту. Він використовує частину коду, написаного на роботі, та не повідомляє про це менеджеру.

Ваші дії як колеги / етичного офіцера:

1) Визначте, чи має місце конфлікт інтересів.

2) Які етичні й юридичні ризики виникають?

3) Як правильно реагувати в межах команди?

Форма подачі: письмова оцінка (до 1 сторінки).

Завдання 10.2 Симуляція: внутрішнє розслідування в команді

Уявіть, що менеджер отримав анонімну скаргу на неетичну поведінку: один з розробників редагує чужі коміти у Git без погодження, а також використовує службовий час для побічних проєктів.

Завдання:

1) Як має діяти керівник команди?

2) Як провести етичне розслідування?

3) Як зберегти атмосферу довіри й справедливості?

Форма подачі: письмовий план реагування або командне обговорення (протокол).

Завдання 10.3 Визначення форм неетичної поведінки в IT-командах

Створіть перелік з 5 форм неетичної поведінки в IT-командах (наприклад, плагіат коду, приховування багів, маніпуляція звітами, фаворитизм тощо). Для кожної форми:

1) дайте короткий опис;
2) вкажіть можливі наслідки;
3) запропонуйте спосіб реагування.

Форма подачі: таблиця 10.1.

Таблиця 10.1 – Форми неетичної поведінки в IT-командах

Форма неетичної поведінки	Короткий опис	Можливі наслідки для команди / проєкту	Рекомендований спосіб реагування
Плагіат коду	присвоєння або копіювання коду без належного зазначення авторства	втрата довіри, порушення авторських прав, юридичні ризики	повідомити керівника, перевірка історії комітів, створення правил
Приховування критичних багів	…	…	…
Маніпуляція звітністю	…	…	…
Використання службових ресурсів у власних цілях	…	…	…
Фаворитизм або токсичне лідерство	…	…	…
…			

Додаткові питання до захисту лабораторної роботи:

1) Що таке конфлікт інтересів і як його виявити?
2) Яка різниця між помилкою та неетичною дією в командній роботі?
3) Як діяти, якщо колега порушує етичні норми, але ви боїтесь повідомляти?
4) Як компанії запобігають неетичній поведінці (кодекс, канали для скарг тощо)?
5) Чи завжди конфлікт інтересів – це порушення?

ЛАБОРАТОРНА РОБОТА 11
ВІДПОВІДАЛЬНІСТЬ ЗА КІБЕРЗЛОЧИНИ ТА ПОРУШЕННЯ БЕЗПЕКИ ІНФОРМАЦІЇ

Мета роботи – ознайомити здобувачів освіти з поняттям кіберзлочину, типами відповідальності (кримінальної, адміністративної, професійної), механізмами реагування на порушення безпеки інформації. Сформувати усвідомлення меж законної діяльності в ІТ.

Завдання 11.1 Класифікація кіберзлочинів

Підготуйте таблицю з 5 прикладами кіберзлочинів із коротким описом та вказівкою на:

1) статтю Кримінального кодексу України або міжнародного законодавства;

2) тип відповідальності (кримінальна / адміністративна);

3) потенційні етичні наслідки для спеціаліста.

Форма подачі: таблиця 11.1.

Таблиця 11.1 – Кіберзлочини, їх правова та етична оцінка

Тип кіберзлочину	Опис ситуації	Стаття КК України / міжнародна норма	Тип відповідальності	Етична оцінка / наслідки
несанкціонований доступ до системи	хакер отримав доступ до бази даних через вразливість	ст. 361 КК України	кримінальна	порушення принципу конфіденційності, загроза довірі до систем
встановлення шкідливого ПЗ	…	…	…	…
порушення авторських прав (плагіат ПЗ)	…	…	…	…
фішинг / крадіжка персональних даних	…	…	…	…
зловживання службовими правами доступу	…	…	…	…

Завдання 11.2 Профілактика інцидентів: чеклист дій

Складіть короткий чеклист дій ІТ-фахівця, який дізнався про порушення безпеки в організації (наприклад, витік паролів, фішинг, зараження мережі):

1) Як зафіксувати факт?

2) Кому повідомити?

3) Як зберегти доказову базу?

4) Як уникнути відповідальності в разі непомітної помилки?

Форма подачі: чеклист (до 10 пунктів) у формі таблиці або списку.

Таблиця – Чеклист реагування на інцидент інформаційної безпеки

Крок	Опис дії / що слід зробити	Примітки / обґрунтування
Виявити та зафіксувати інцидент	зафіксувати дату, час, тип інциденту (витік, злом, вірус, фішинг)	важливо для доказової бази, внутрішнього звіту
Не панікувати та не видаляти сліди	…	…
Повідомити відповідальну особу / відділ безпеки	…	…
Обмежити поширення інциденту	…	…
Оформити попередній звіт про інцидент	…	…
Співпрацювати з фахівцями з кібербезпеки	…	…
Проінформувати користувачів (за потреби)	…	…
Зберегти копії логів / доказів	…	…
Проаналізувати причини та наслідки	…	…
Участь у вдосконаленні політик безпеки	…	…

Завдання 11.3 Аналіз кейсу: несанкціонований доступ

Молодий ІТ-спеціаліст отримує дані доступу до внутрішньої CRM-системи колишнього місця роботи. Він вирішує «пожартувати» та змінює контактну інформацію клієнтів, не завдаючи прямої шкоди. Ваше завдання:

1) Які правові та етичні норми порушено?

2) Чи вважатиметься це кіберзлочином?

3) Яка відповідальність настає? Як уникнути подібних ситуацій?

Форма подачі: письмовий аналіз (1 сторінка).

Додаткові питання до захисту лабораторної роботи:

1) Яка різниця між етичним хакером і злочинцем?

2) У яких випадках може настати кримінальна відповідальність за дії в мережі?

3) Як впливає недотримання етичних норм на репутацію ІТ-фахівця?

4) Які документи регламентують кібербезпеку в Україні та ЄС?

5) Що робити ІТ-фахівцю, якщо він випадково знайшов уразливість?

ЛАБОРАТОРНА РОБОТА 12
РЕАЛЬНІ КЕЙСИ ПОРУШЕННЯ ПРОФЕСІЙНОЇ ЕТИКИ В ІТ: АНАЛІЗ ТА ВИСНОВКИ

Мета роботи – навчити здобувачів освіти проводити критичний аналіз резонансних етичних інцидентів у сфері ІТ. Показати вплив неетичних рішень на бізнес, суспільство та репутацію розробників. Розвивати навички формулювання висновків і пропозицій щодо запобігання аналогічним ситуаціям.

Завдання 12.1 Аналіз кейсу за шаблоном

Оберіть один із відомих етичних скандалів в ІТ-сфері (на вибір):

–Facebook / Cambridge Analytica;

–Uber: система стеження за конкурентами («Greyball»);

–Google: звільнення дослідниці етики ШІ Тімніт Ґебру;

–TikTok: цензура контенту за політичними критеріями;

–GitHub Copilot і порушення авторських прав.

Завдання:

–проведіть аналіз за шаблоном (таблиця):

Таблиця – Шаблон аналізу кейсу

Розділ	Зміст
Назва кейсу	наприклад, Cambridge Analytica і Facebook
Короткий опис подій	що сталося, коли, хто був учасником
Порушені етичні принципи	наприклад, приватність, прозорість, чесність
Вплив на користувачів	чим загрожувало, як постраждали
Наслідки для компанії	штрафи, публічна критика, втрати
Оцінка дій компанії	чи були дії виправданими / як реагувала компанія
Ваші висновки та поради	що треба було зробити і як цього уникнути

–сформулюйте висновки й пропозиції.

Форма подачі: письмова аналітична довідка з таблицею (1-1,5 сторінки).

Завдання 12.2 Створення етичного плану дій

Уявіть, що ви – керівник ІТ-компанії, яка потрапила в подібний скандал. Складіть план дій, щоб:

1) відновити довіру користувачів;

2) посилити внутрішню етику / прозорість;

3) запобігти повторенню.

Форма подачі: покроковий план (таблиця).

Таблиця 12.1 – Етичний план дій для ІТ-компанії

Напрям реагування	Конкретні дії	Очікуваний ефект	Коментар / чому це важливо
Відкрита комунікація	провести пресконференцію, опублікувати офіційне вибачення	зниження напруги, часткове відновлення довіри	прозорість – перший крок до відновлення репутації
Внутрішнє розслідування	…	…	….
Посилення політик етики	…	…	….
Освітня ініціатива	…	…	….
Технічна перевірка систем	…	…	….
Діалог з громадськістю / НГО	…	…	….
Моніторинг і звітність	…	…	….

Примітка. Здобувачі освіти можуть адаптувати дії під обраний кейс (Google, Uber, TikTok тощо). У стовпці «Коментар» слід пояснити, чому саме ця дія доречна.

Завдання 12.3 Дискусія / міні-дебати

Поділіться на малі групи. Кожна група отримує кейс та готує:

–позицію компанії (захисну аргументацію);

–позицію етичного контролера / громадськості (критика рішень);

–пропозицію компромісного вирішення.

Форма подачі: презентація + письмові тези (1-2 сторінки).

Додаткові питання до захисту лабораторної роботи:

1. Який наслідок має публічний етичний скандал для IT-компанії?

2. Як розрізнити етичну помилку і системну етичну політику?

3. Чи достатньо внутрішнього кодексу, щоб уникнути порушень?

4. Хто має нести відповідальність: окремі працівники чи компанія в цілому?

5. Як впливає громадська думка на дії IT-корпорацій?

Додаток А

Аналітична довідка

Назва кейсу: Facebook і Cambridge Analytica.

Тип порушення: несанкціонований доступ до персональних даних користувачів соціальної мережі.

У 2018 році стало відомо, що компанія Cambridge Analytica отримала доступ до особистих даних понад 87 мільйонів користувачів Facebook через додаток-психологічний тест. Попри те, що лише кілька сотень тисяч користувачів дали згоду на використання даних, були зібрані також дані їхніх друзів без жодного повідомлення чи дозволу.

Етичні порушення:

– порушення принципу інформованої згоди: користувачі не знали, що їхні дані передаються третім особам;

– надмірний збір даних (data overcollection): дані збирались у значно ширшому обсязі, ніж це було необхідно;

– використання для політичного маніпулювання: дані застосовувались для таргетованої політичної реклами під час виборів.

Відповідальні сторони:

– Facebook як платформа, що не проконтролювала використання API додатку;

– розробники застосунку, які порушили правила користування;

– Cambridge Analytica – як компанія, що використала дані з етичним і правовим порушенням.

Наслідки:

– розслідування Сенату США, штраф Facebook на $5 млрд від Федеральної торгової комісії США;

– падіння рівня довіри користувачів до Facebook;

– глобальна дискусія про цифрову приватність і необхідність регулювання великих IT-компаній.

Етична оцінка та рекомендації:

– компанії повинні дотримуватись принципу прозорості щодо обробки даних;

– необхідне запровадження етичного аудиту додатків і API;

– потрібна більш чітка комунікація з користувачами щодо їхніх прав.

Висновок. Цей кейс демонструє, що юридична відповідність не завжди гарантує етичну поведінку. У цифровому середовищі розробник і платформа несуть спільну відповідальність за прозорість, захист приватності та соціальні наслідки використання технологій.

Додаток Б

Протокол засідання етичної ради ІТ-компанії

Проєкт: Система моніторингу працівників для дистанційної роботи

Дата засідання: 08.05.2025

Учасники: Іваненко М., Шевчук А., Олійник Д., Яремчук С. (етична рада)

1. Опис цифрового продукту

Система призначена для моніторингу працівників на віддаленій роботі. Передбачає:

1) відстеження натискань клавіш (кейлогер);
2) фото з вебкамери кожні 5 хв;
3) геолокацію пристрою;
4) скріншоти екрана.

2. Етична оцінка функціоналу

Функція	Оцінка етичності	Коментар / проблеми
відстеження натискань клавіш	порушення приватності	може виявляти паролі, особисту інформацію, потребує суттєвого обмеження
фото з вебкамери	надмірне вторгнення	без чіткої згоди це порушення особистого простору
геолокація	умовно допустимо	лише за згодою і в службовий час, пропонується деактивація у вихідні
скріншоти екрана	за умови обмеження	допустимо для службових додатків з повідомленням працівника

3. Рішення етичної ради:

1) заборонити вбудований кейлогер;
2) припинити використання фото з вебкамери – високий рівень ризику вторгнення в особисте життя;
3) геолокацію дозволити лише при підписанні інформованої згоди;
4) скріншоти обмежити до службового ПЗ та обов’язкове сповіщення користувача.

Рекомендовано:

1) створити політику конфіденційності для працівників;

2) впровадити добровільну участь у пілотному тестуванні;

3) додати механізм подання скарг на використання системи.

4. Підсумок: продукт може бути запущений лише після внесення етичних правок, публічного обговорення з працівниками та чіткого документування умов використання.

/Підписи членів етичної ради/

СПИСОК ВИКОРИСТВНИХ ДЖЕРЕЛ

1. ACM Code of Ethics and Professional Conduct (Кодекс етики та професійної поведінки ACM). *ACM.* 2025. URL: https://www.acm.org/code-of-ethics (дата звернення: 09.07.2025).

2. Board of Directors Approves Revisions to the IEEE / Code of Ethics Changes reflect commitment to ethical and professional conduct. *IEEE Spectrum.* URL: https://spectrum.ieee.org/board-of-directors-approves-revisions-to-the-ieee-code-of-ethics (дата звернення: 09.07.2025).

3. ISO/IEC 27001. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. *Online Browsing Platform (OBP).* URL: https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27001:ed-3:v1:en (дата звернення: 09.07.2025).

4. Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events. (Цілісність даних: Виявлення програм-вимагачів та інших руйнівних подій і реагування на них). *NIST SPECIAL PUBLICATION 1800-26A.* URL: https://www.nccoe.nist.gov/publication/1800-26/VolA/ (дата звернення: 09.07.2025).

5. Plan, Do, Check, Act (PDCA). Lean Enterprise Institute. URL: https://www.lean.org/lexicon-terms/pdca/ (дата звернення: 09.07.2025).

6. Професійна етика в IT: розуміння та приклади. *Computools.* URL: https://careers.computools.ua/professional-ethics-in-it/ (дата звернення: 10.07.2025)

7. Етична відповідальність розробників програмного забезпечення: збереження доброчесності в технологічній галузі. *MoldStud.* URL: https://moldstud.com/articles/p-the-ethical-responsibilities-of-software-developers-maintaining-integrity-in-the-tech-industry (дата звернення: 10.07.2025).

8. 12 етичних дилем, які гризуть розробники сьогодні. *IDG Communications.* URL: https://www.infoworld.com/article/2172450/12-ethical-dilemmas-gnawing-at-developers-today-2.html (дата звернення: 10.07.2025).

9. Етичні міркування в практиці системної інженерії. *MoldStud.* URL: https://moldstud.com/articles/p-ethical-considerations-in-systems-engineering-practices (дата звернення: 10.07.2025).

10. Етичні питання при розробці програмного забезпечення. *X-Team.* URL: https://x-team.com/magazine/ethical-issues-in-software-development (дата звернення: 10.07.2025).

11. Системний інженер проти інженера-програміста: відмінності та подібності. *Fellow.* URL: https://fellow.app/blog/system-engineer-vs-software-engineer/ (дата звернення: 10.07.2025).

12. Joseph Herkert, Jason Borenstein, Keith Miller. The Boeing 737 MAX: Lessons for Engineering Ethics. *Science and Engineering Ethics.* Vol. 26(6). 2020. Pp. 2957-2974. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC7351545/pdf/11948_2020_Article_252.pdf (дата звернення: 10.07.2025).

13. Engineering Ethics and the Boeing Scandal. *Ethics Unwrapped.* URL: https://ethicsunwrapped.utexas.edu/engineering-ethics-and-the-boeing-scandal (дата звернення: 10.07.2025).

14. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 5 липня 1994 року № 80/94-ВР. *Законодавство України.* URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення: 10.07.2025).

15. Про інформацію: Закон України від 2 жовтня 1992 року № 2657-XII. *Законодавство України.* URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 10.07.2025).

16. Про захист персональних даних: Закон України від 1 червня 2010 року № 2297-VI. *Законодавство України.* URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 10.07.2025)

17. Кримінальний кодекс України від 5 квітня 2001 року № 2341-III. *Законодавство України.* URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 10.07.2025).

18. The Convention on Cybercrime (Budapest Convention, ETS No. 185) and its Protocols. *Council of Europe.* URL: https://www.coe.int/en/web/cybercrime/the-budapest-convention (дата звернення: 10.07.2025).

19. Complete guide to GDPR compliance. *Proton.* URL: https://gdpr.eu/ (дата звернення: 10.07.2025).

20. Cambridge Analytica: The story so far. *BBC.* URL: https://www.bbc.com/news/technology-43465968 (дата звернення: 11.07.2025).

21. Конвенція про захист прав людини і основоположних свобод (з протоколами) (Європейська конвенція з прав людини). *Законодавство України.* URL: https://zakon.rada.gov.ua/laws/show/995_004#Text (дата звернення: 11.07.2025).

22. Warren & Brandeis. The Right to Privacy. *Harvard Law Review.* Vol. IV. № 5. 1890. URL: https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html (дата звернення: 11.07.2025).

23. European Convention on Human Rights. *Council of Europe.* URL: https://www.echr.coe.int/documents/d/echr/convention_eng (дата звернення: 11.07.2025).

24. Universal Declaration of Human Rights. *United Nations.* URL: https://www.un.org/en/about-us/universal-declaration-of-human-rights (дата звернення: 11.07.2025).

25. Що таке GDPR, новий закон ЄС про захист даних? *Proton.* URL: https://gdpr.eu/what-is-gdpr/ (дата звернення: 11.07.2025).

ДЛЯ НОТАТОК

У П-73 Професійна етика в ІТ-сфері: методичні вказівки до лабораторних робіт для здобувачів першого (бакалаврського) рівня вищої освіти галузі знань F Інформаційні технології всіх спеціальностей денної та заочної форм навчання / уклад. М. М. Поліщук, Л. О. Поліщук: ЛНТУ, 2025. 44 с.

Комп’ютерний набір: М. М. Поліщук
Л. О. Поліщук

Редактор: М. М. Поліщук
Л. О. Поліщук

Підп. до друку «___» _____ 2025р.
Формат 60х84/16. Папір офс. Гарнітура Таймс.
Ум. друк. арк. ____. Тираж 10 прим. Зам. ____

Відділ іміджу та промоції
Луцького національного технічного університету
43018, м. Луцьк, вул. Львівська, 75
Друк – ВІП ЛНТУ