Міністерство освіти і науки України
Луцький національний технічний університет

ПРОФЕСІЙНА ЕТИКА В ІТ-СФЕРІ

Конспект лекцій
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: _____ Сергій ГРИНЮК, 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: конспект лекцій 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. 172 с.

Конспект лекцій «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.

Конспект лекцій є структурованим навчальним матеріалом, що охоплює ключові теоретичні положення, практичні аспекти, приклади застосування та етичні орієнтири, необхідні для формування фахових компетентностей у сфері інформаційних технологій.

Мета дисципліни – сформувати у здобувачів вищої освіти цілісне уявлення про професійну етику в галузі інформаційних технологій, розвинути здатність ідентифікувати та аналізувати етичні дилеми, приймати відповідальні рішення в умовах цифрового середовища, а також сприяти становленню фахової культури та особистої відповідальності IT-спеціаліста перед суспільством.

Конспект лекцій є типовим, проте у разі необхідності за погодженням із викладачем або кафедрою комп’ютерної інженерії та безпеки можуть бути внесені зміни до окремих тем.

Конспект лекцій призначений для здобувачів першого (бакалаврського) рівня вищої освіти галузі знань F Інформаційні технології денної та заочної форм навчання.

ЛЕКЦІЯ 1
ВИНИКНЕННЯ ТА РОЗВИТОК ПРОФЕСІЙНОЇ ЕТИКИ В ІТ-СФЕРІ: ПРИЗНАЧЕННЯ В СУСПІЛЬСТВІ

Мета – ознайомити здобувачів освіти з історичними етапами виникнення та еволюції професійної етики в ІТ-сфері, розкрити її суспільне призначення та обґрунтувати необхідність етичної відповідальності ІТ-фахівця в умовах цифрової трансформації. Лекція спрямована на формування усвідомлення ролі етики в регулюванні поведінки розробників, забезпеченні довіри до технологій і захисті інтересів користувачів.

1.1 Поняття професійної етики та її роль у сучасному світі

Професійна етика – це система моральних норм і принципів, що регламентують поведінку фахівців певної професійної галузі. Вона виникає на перетині етики загальнолюдської та специфіки професійної діяльності.

У сфері ІТ професійна етика виконує певні функції (рис. 1.1).

Рисунок 1.1 – Основні функції професійної етики в ІТ-сфері

Нормативна функція професійної етики в інформаційних технологіях полягає у встановленні чітких моральних орієнтирів і принципів поведінки фахівців у цій галузі. Вона виконує роль етичного регулятора, який визначає межі прийнятної професійної діяльності, виходячи з моральних засад, загальнолюдських цінностей та специфіки IT-середовища.

Ключові характеристики:

– формування професійних стандартів поведінки;

– визначення етично прийнятних практик у сфері розробки, аналізу, зберігання та передачі інформації;

– орієнтація на міжнародно визнані кодекси етики, зокрема ACM, IEEE та ISO/IEC 27001.

Ця функція забезпечує ідентифікацію належних способів професійної діяльності та сприяє запобіганню морально неприйнятних дій з боку IT-фахівців. Наприклад, розробник, який дотримується принципу «не завдавати шкоди», не створюватиме програми для стеження за користувачами без їхньої згоди.

Оціночна функція забезпечує фахівця інструментами морального аналізу та критичного осмислення професійних рішень. Вона дозволяє диференціювати дії, рішення або політики за критерієм етичності, спираючись на встановлені моральні стандарти та соціально прийнятні норми.

Ключові характеристики:

– можливість ідентифікувати етичні ризики;

– визначення рівня відповідності професійних дій принципам доброчесності;

– аналіз моральних наслідків застосування конкретних технологій або продуктів.

Ця функція дозволяє сформувати етично вмотивовану позицію у процесі прийняття рішень, що знижує імовірність професійних і моральних помилок. Наприклад, при розробці алгоритму рекомендацій IT-команда аналізує, чи не призводить він до дискримінації певних користувачів – це етична оцінка рішень.

Регулятивна функція забезпечує узгодженість та гармонійність взаємодії між усіма суб’єктами, залученими до IT-процесів. Вона визначає правила етичної

поведінки у професійній комунікації, розв'язанні конфліктів, розподілі відповідальності та забезпеченні відкритості й чесності у співпраці.

Ключові характеристики:

– створення моральних основ для взаємодії між розробниками, клієнтами, замовниками та користувачами.

– етичне регулювання діяльності ІТ-команд у межах корпоративного середовища.

– формування механізмів подолання етичних конфліктів.

Регулятивна функція сприяє підвищенню якості співпраці, зниженню внутрішньоорганізаційних ризиків та формуванню професійної відповідальності на всіх рівнях ІТ-проєктів. Наприклад, у компанії запроваджено правило – не розпочинати реалізацію проєкту без етичного аналізу потенційного впливу на кінцевих користувачів. Це приклад регулятивного механізму.

Інтегративна функція професійної етики в ІТ-сфері забезпечує формування єдиної етичної культури, яка об'єднує всіх учасників цифрового середовища навколо спільних цінностей, моральних орієнтирів та професійної доброчесності.

Ключові характеристики:

– уніфікація моральних стандартів у колективах та організаціях;

– створення єдиного простору професійної довіри та взаємоповаги;

– сприяння ціннісній ідентифікації працівників ІТ-галузі.

Інтегративна функція формує умови для підтримання моральної згуртованості в колективах, підвищення соціальної відповідальності ІТ-компаній та забезпечення стабільності етичного клімату в професійному середовищі. Наприклад, якщо всі члени ІТ-команди розуміють і поділяють цінність «прозорості у взаємодії з користувачами», це сприяє згуртованості та ефективності їхньої роботи.

У сучасному цифровому середовищі, де інформаційні технології проникають практично в усі сфери життя – від медицини до державного управління, – професійна етика ІТ-фахівців відіграє фундаментальну роль у забезпеченні безпеки, довіри та справедливості. Високий рівень автоматизації,

використання персональних даних та алгоритмічних рішень вимагає від спеціалістів глибокого усвідомлення етичних наслідків своєї діяльності. Етична відповідальність є необхідною умовою забезпечення сталого розвитку цифрового суспільства та збереження базових прав людини в умовах стрімкого технологічного прогресу.

Зважаючи на те, що ІТ-індустрія має глобальний характер і впливає на мільйони користувачів одночасно, професійна етика формує основу для прийняття відповідальних рішень у багатокультурному, багатонаціональному середовищі. Вона допомагає уникати технологічної дискримінації, інформаційної нерівності, зловживань даними та втручання у приватне життя. Таким чином, етична свідомість фахівців сприяє формуванню більш безпечного, інклюзивного та справедливого цифрового простору.

Крім того, професійна етика відіграє стратегічну роль у розвитку корпоративної культури, підтримці репутації організацій і формуванні довіри з боку клієнтів, партнерів та суспільства. В епоху інформаційної прозорості, коли кожне порушення етичних норм може швидко стати надбанням громадськості, дотримання етичних стандартів стає не лише моральним, а й практичним імперативом.

1.2 Історичні передумови виникнення професійної етики в ІТ

У процесі становлення інформаційних технологій як окремої професійної галузі виникла необхідність у формуванні етичних засад, які б регулювали поведінку фахівців. Рисунок 1.2, демонструє ключові історичні етапи розвитку комп’ютерної етики – від перших дискусій про відповідальність програмістів у середині XX століття до інституалізації етичних кодексів у 1990-х роках. Така історична ретроспектива дозволяє усвідомити глибинні причини появи професійної етики в ІТ-сфері та простежити її еволюцію як важливої складової технічної культури.

Рисунок 1.2 – Історичні передумови комп’ютерної етики

У 1950-60-х роках обчислювальні машини стрімко інтегруються у ключові сфери суспільства, насамперед – в оборону та науку. Саме в цей період відбувається становлення епохи комп’ютеризації, яка трансформує підходи до зберігання, обробки та аналізу даних.

У роки Холодної війни уряди, особливо США та СРСР, активно інвестували у розвиток комп’ютерної техніки для військових потреб. Приклади включають:

– ENIAC і наступні машини використовувалися для балістичних розрахунків, моделювання ядерних вибухів, криптографічної діяльності;

– проєкти NASA покладалися на комп’ютери для розрахунків орбіт космічних апаратів;

– у наукових лабораторіях розпочинається використання ЕОМ для чисельного аналізу, моделювання фізичних і хімічних процесів.

Цей технічний прорив посприяв зміщенню фокусу на обчислювальні системи як інструмент стратегічного значення.

Зі зростанням ролі ЕОМ у критичних системах виникають перші етичні дискусії:

– Хто відповідальний, якщо комп’ютерна система дала збій у військовій операції?

– Чи може програміст нести моральну відповідальність за наслідки використання його коду, наприклад у системах наведення зброї?

Піднімалася потреба розмежування ролей інженерів, програмістів та користувачів – де закінчується технічне завдання і починається відповідальність за прийняті рішення?

З’являються публікації й дебати в академічних та професійних спільнотах, які згодом стають підґрунтям для формування професійної етики в ІТ.

У 1970-х роках, на тлі стрімкого поширення комп’ютерів у бізнесі, науці, урядових структурах і освіті, починає формуватись нова дисципліна – комп’ютерна етика (англ. computer ethics). Саме в цей період виникає усвідомлення, що використання обчислювальної техніки ставить нові моральні виклики, які не можна повністю пояснити традиційною етикою.

1976 рік – американський філософ і дослідник Walter Maner вперше запропонував термін computer ethics для позначення галузі, яка вивчає «етичні проблеми, що є унікальними або суттєво посилюються використанням комп’ютерної техніки».

Він стверджував, що комп’ютери створюють ситуації морального вибору, які раніше не існували, наприклад, щодо доступу до особистих даних, автоматизованого прийняття рішень, збереження цифрової інформації.

У 1970-х починаються систематичні спроби осмислення етичної поведінки спеціалістів з ІТ:

– розробка професійних кодексів етики – Асоціації, як-от ACM (Association for Computing Machinery) та IEEE, починають працювати над кодексами етичної поведінки інженерів і програмістів;

– дослідження у галузі філософії техніки – в університетах з’являються перші курси з комп’ютерної етики, а науковці починають публікувати статті про моральну відповідальність у сфері ІТ;

– обговорення вразливостей – постають питання про етичність створення шкідливих програм, порушення авторських прав на програмне забезпечення, порушення приватності через доступ до комп'ютерних баз даних.

У 1980-х роках комп'ютери стають повсюдним інструментом в офісах, університетах, лабораторіях і навіть у домівках. Відповідно, зростає усвідомлення того, що традиційні етичні концепції недостатньо охоплюють нові виклики цифрової епохи. У цей період Джеймс Мур (James H. Moor), професор філософії з Дартмутського коледжу, формулює фундаментальні засади комп'ютерної етики як самостійної галузі прикладної етики.

У 1985 році Джеймс Мур публікує впливову статтю «What Is Computer Ethics?», яка стає ключовим теоретичним документом у цій сфері. У ній він стверджує: «Комп'ютерна етика – це вивчення того, як обчислювальні технології впливають на моральні цінності та прийняття етичних рішень».

Основні положення концепції Мура:

– комп'ютери – революційна сила, оскільки вони мають «логічну гнучкість»: їх можна запрограмувати на виконання безлічі нових і непередбачуваних функцій;

– через цю гнучкість комп'ютери створюють «політичні та соціальні вакууми» – ситуації, в яких відсутні чіткі закони, норми та етичні стандарти;

– у результаті виникає потреба у формулюванні нових правил поведінки, адаптованих до цифрового контексту – і цим має займатися комп'ютерна етика.

Ідеї Мура стали основою для викладання комп'ютерної етики в університетах. Його підхід стимулював розробку нових етичних кодексів у професійних організаціях (ACM, IEEE). У 1980-х роках комп'ютерна етика оформлюється як академічна дисципліна, з конференціями, публікаціями й дослідницькими програмами.

У 1990-х роках інформаційні технології стрімко поширюються: з'являється Всесвітня павутина (WWW), персональні комп'ютери стають звичними в офісах і домівках, а перші форми електронної комерції та онлайн-

комунікації відкривають нові можливості – і водночас нові етичні виклики. Це десятиліття стає переломним для інституціоналізації етики ІТ.

У відповідь на зростання впливу ІТ, провідні професійні об’єднання розробляють офіційні кодекси етики, які стають основою для професійної поведінки спеціалістів.

ACM Code of Ethics and Professional Conduct (1992). Американська асоціація обчислювальної техніки (ACM) опублікувала один із перших детальних етичних кодексів, що включав:

– повага до конфіденційності та приватності користувачів;
– заборона на навмисне створення шкідливого або ненадійного ПЗ;
– визнання суспільної відповідальності інженера;
– чесність, прозорість і відповідальність у професійній діяльності.

IEEE Code of Ethics (оновлено в 1990-х).

Інститут інженерів електрики та електроніки (IEEE) також актуалізував свій кодекс, підкреслюючи:

– публічну безпеку й добробут як найвищий пріоритет;
– відповідальне використання технологій;
– підзвітність за технічні рішення, що можуть вплинути на суспільство.

У 1990-х етика ІТ стає повноцінною складовою навчальних програм у багатьох університетах світу. З’являються самостійні курси з комп’ютерної етики в межах спеціальностей «інформатика», «інженерія» та «філософія технологій».

Відомі дослідники, як Deborah Johnson, Terrell Ward Bynum, James Moor, відіграють ключову роль у формуванні змісту та методики викладання.

1.3 Основні напрями розвитку етики в ІТ

Етика в ІТ розвивається у чотирьох взаємопов’язаних напрямах: кодекси етики, етичні комітети, освіта та соціальні ініціативи.

Кодекси професійної етики – це формалізовані документи, що містять перелік етичних принципів і норм поведінки, яких повинні дотримуватись фахівці у сфері інформаційних технологій. Мета – забезпечити відповідальне використання технологій та запобігти зловживанням.

1) ACM Code of Ethics and Professional Conduct (1992, оновлено 2018):

– чесність, прозорість, повага до конфіденційності;

– уникнення шкоди та відповідальність за наслідки програмного продукту.

2) IEEE Code of Ethics:

– забезпечення безпеки, добробуту та прав людини;

– професійна доброчесність і технічна компетентність.

3) IFIP (Міжнародна федерація з обробки інформації):

– стандарти глобального рівня для фахівців у галузі ІКТ.

Роль кодексів: виконують функцію етичного орієнтира, є підґрунтям для дисциплінарних дій у професійних спільнотах і використовуються у навчанні та при сертифікації спеціалістів.

Етичні комітети у компаніях – спеціальні підрозділи для оцінки спірних рішень.

Багато IT-компаній створюють внутрішні етичні комітети або наглядові ради, які аналізують:

– суперечливі технологічні рішення (напр., впровадження систем розпізнавання обличь).

– можливі ризики для суспільства або довкілля.

– етичність роботи алгоритмів, що приймають рішення замість людей.

Типові функції комітетів:

– оцінка ризиків перед запуском нових продуктів;

– розробка внутрішніх етичних політик;

– комунікація зі сторонніми експертами (філософами, правозахисниками, соціологами);

– розгляд скарг працівників на порушення етичних норм.

Наприклад, Google AI Ethics Board (спроба створення етичної ради з питань штучного інтелекту) та Microsoft Ethics & Society Committee – оцінка рішень, пов'язаних з використанням AI.

Викладання етики в IT у ЗВО – поширення етичної освіти серед студентів технічних спеціальностей.

У 2000-х роках етика IT стала необхідною складовою освітніх програм з комп'ютерних наук, кібербезпеки, інженерії, штучного інтелекту тощо.

Соціальні ініціативи – рухи за етику штучного інтелекту, захист цифрових прав тощо.

Громадські організації, активісти, науковці й IT-спільноти ініціюють рухи за етичне використання технологій, зокрема:

Напрями ініціатив:

– захист цифрових прав і свобод (аналог цифрових прав людини);

– етика штучного інтелекту: заклики до прозорості, підзвітності, запобігання дискримінації;

– справедливе використання алгоритмів – боротьба з упередженістю в AI;

– проти стеження й масового збору даних.

Приклади ініціатив:

– Electronic Frontier Foundation (EFF) – захист цифрової приватності;

– The Future of Life Institute – дослідження етичних меж розвитку AI;

– Partnership on AI – альянс компаній (Google, IBM, Microsoft тощо) і НУО для сприяння прозорому розвитку AI.

Результати:

– вплив на формування законів (наприклад, GDPR в ЄС);

– створення глобальних принципів етики (наприклад, рекомендації ЮНЕСКО з етики штучного інтелекту).

1.4 Необхідність етичного регулювання в ІТ-сфері

ІТ-сфера є однією з найдинамічніших галузей сучасності, і саме тому вона вимагає підвищеної уваги до етики.

Законодавство та регуляторні рамки не встигають за новими викликами, наприклад, масове застосування штучного інтелекту, біометричної ідентифікації чи нейромереж стало реальністю ще до того, як суспільство сформулювало чіткі правила їхнього етичного використання. Це породжує ситуації «нормативного вакууму», де етика є єдиним регулятором поведінки.

Окрему загрозу становить високий рівень доступу до конфіденційної інформації, яку обробляють ІТ-фахівці. Йдеться про персональні дані користувачів, медичні записи, банківські транзакції, історію браузера тощо. Неналежне поводження з такими даними може призвести до витоків, шантажу, дискримінації або навіть порушення основоположних прав людини. В умовах цифровізації суспільства етична поведінка фахівців стає запорукою довіри до технологій.

Ще одна особливість ІТ-сфери – можливість масштабного впливу. Один розроблений алгоритм або програма можуть використовуватися мільйонами людей, формувати поведінку користувачів, впливати на їхній вибір і навіть результати виборів. Цифрові системи дедалі частіше приймають рішення за людей – у медицині, правосудді, освіті. У такому середовищі помилка або навмисне зловживання можуть мати катастрофічні наслідки.

Крім того, анонімність у цифровому середовищі часто знижує поріг особистої відповідальності. Люди, які створюють чи використовують програмне забезпечення, можуть залишатися невідомими, ухиляючись від наслідків своїх дій. Це створює сприятливе середовище для неетичної поведінки – від кібербулінгу до розробки шкідливих програм. Етична культура в ІТ покликана підвищувати усвідомлену відповідальність за кожен рядок коду.

Глобальний характер ІТ-індустрії означає, що її учасники працюють у багатонаціональному середовищі з різними правовими та культурними традиціями. У таких умовах універсальні етичні принципи – чесність, прозорість,

справедливість – стають спільною основою для взаємодії. Вони дозволяють уникнути конфліктів інтересів, підтримувати глобальну довіру до технологій і забезпечувати відповідальний розвиток IT у різних країнах.

1.5 Призначення професійної етики IT-фахівця в суспільстві

Напрями, що визначають призначення професійної етики в IT (рис. 1.3), формують комплексний підхід до етичної відповідальності IT-фахівця в сучасному цифровому суспільстві. Вони охоплюють не лише технічні аспекти, а й соціальні, правові та гуманітарні виміри, спрямовані на забезпечення безпечного, справедливого та відповідального використання інформаційних технологій.

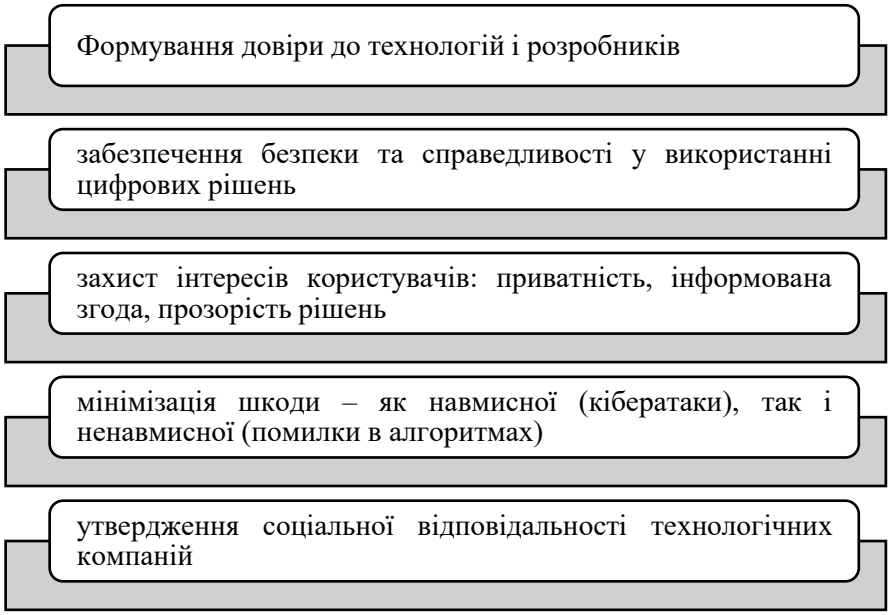

Рисунок 1.3 – Основні напрями реалізації професійної етики в IT-сфері

1) Формування довіри до технологій і розробників. У цифровому суспільстві, де значна частина рішень приймається автоматизовано або за допомогою алгоритмів, довіра до технологій має критичне значення.

Програмісти, інженери та компанії, які дотримуються етичних стандартів, демонструють готовність до відкритості, відповідальності та чесності. Це

дозволяє користувачам не лише користуватись продуктами, але й вірити в їхню безпечність, добросовісність і обґрунтованість.

Етична поведінка розробника включає:

– прозорість логіки алгоритмів і програм;

– чітке інформування про обмеження та ризики використання продукту;

– уникнення прихованих функцій, трекінгу без згоди або маніпулятивного дизайну (dark patterns*).*

Якщо етика ігнорується – довіра втрачається, що може призвести до репутаційних втрат, судових позовів і соціального спротиву (як це траплялося у випадках із Facebook/Cambridge Analytica).

2) Забезпечення безпеки та справедливості у використанні цифрових рішень. Етичні принципи допомагають гарантувати, що інформаційні системи не шкодять користувачам і функціонують справедливо. У практичному сенсі це означає:

– надійний захист від злому, втрати або крадіжки даних;

– відсутність дискримінаційних упереджень у штучному інтелекті або автоматизованих рішеннях (наприклад, при прийомі на роботу чи визначенні кредитоспроможності);

– недопущення технічної нерівності (наприклад, коли доступ до базових цифрових послуг мають лише жителі великих міст).

Етичний підхід вимагає оцінювати вплив цифрових рішень на різні соціальні групи та активно усувати ризики несправедливості, дискримінації або соціального виключення.

3) Захист інтересів користувачів: приватність, інформована згода, прозорість рішень. У центрі етичної парадигми ІТ має бути людина – її права, свободи та інтереси. Тому розробники зобов’язані:

– забезпечувати збір і обробку персональних даних лише з інформованої згоди;

– надавати користувачам можливість контролювати свої дані (видалення, перенесення, обмеження доступу);

– прозоро пояснювати, як працюють алгоритми, чому було прийнято те чи інше рішення (наприклад, у кредитному скорингу чи в медичних рекомендаціях).

Зневажання цих принципів ставить під загрозу приватність і автономію особи, і, зрештою, легітимність самих технологій.

4) Мінімізація шкоди – як навмисної (кібератаки), так і ненавмисної (помилки в алгоритмах). Етика в IT вимагає проактивного підходу до упередження шкоди, що може виникнути як результат злого умислу, так і випадкових помилок:

– навмисна шкода – це створення вірусів, троянів, бекдорів, фішингових сайтів, атак типу DoS, крадіжка даних.

– ненавмисна шкода – це баги у програмах, помилкові прогнози алгоритмів, «непередбачені» рішення ШІ-систем, що шкодять людям.

Етичний фахівець повинен:

– впроваджувати тестування, верифікацію, контроль якості на всіх етапах розробки.

– оцінювати потенційні ризики використання продукту та надавати інструменти для обмеження шкоди.

– повідомляти про виявлені уразливості, а не приховувати їх чи продавати на «темному ринку».

5) Утвердження соціальної відповідальності технологічних компаній. У сучасному світі великі технологічні корпорації (Google, Meta, Amazon тощо) мають величезний вплив на суспільство, іноді більший, ніж уряди. Це накладає на них моральне зобов’язання діяти відповідально перед суспільством.

Соціальна відповідальність включає:

– Розробку технологій на благо людства (наприклад, медичні системи підтримки рішень, освіта, доступність).

– Дотримання етичних принципів у корпоративній політиці (недискримінація, інклюзивність, екологічна свідомість).

– Активну позицію у формуванні етичних стандартів у галузі (участь у глобальних ініціативах, публікація принципів відповідального AI, співпраця з науковцями).

Етична поведінка компаній – це не лише PR, а довгострокова стратегія виживання і довіри у глобальному середовищі.

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

Мета – ознайомити здобувачів освіти з ключовими етичними кодексами та міжнародними стандартами, що регулюють професійну діяльність ІТ-фахівців, зокрема стандартами ACM, IEEE та ISO/IEC 27001. Лекція спрямована на формування розуміння етичних принципів у сфері інформаційних технологій, розвитку професійної відповідальності, дотримання норм інформаційної безпеки, а також вміння орієнтуватися в глобальних етичних стандартах ІТ-галузі.

2.1 Огляд Кодексу етики ACM (Association for Computing Machinery): принципи, структура, приклади застосування

Association for Computing Machinery (ACM) – одна з провідних міжнародних організацій у галузі комп'ютерних наук та ІТ. Її Кодекс етики та професійної поведінки спрямований на всіх, хто працює з обчислювальною технікою – від розробників і інженерів до викладачів та студентів. Кодекс ACM був істотно оновлений у 2018 році, врахувавши сучасні технологічні реалії і виклики (попередня версія створювалася ще 1992 року) [1].

Структура кодексу ACM чітко організована за розділами. У Преамбулі підкреслюється, що кодекс покликаний надихати на етичну поведінку та служити основою для вирішення конфліктних ситуацій, наголошуючи на приматі суспільного блага. Далі йдуть чотири розділи: Розділ 1 містить фундаментальні етичні принципи, що становлять базис кодексу; Розділ 2 описує додаткові професійні обов'язки для повсякденної роботи; Розділ 3 адресований особам у керівних ролях (лідерам команд, менеджерам) щодо їхньої особливої відповідальності; Розділ 4 присвячений забезпеченню дотримання кодексу. Загалом кодекс ACM включає декілька десятків конкретних імперативів (правил поведінки), кожен із яких сформульований як особиста відповідальність члена

професії. Кожен принцип супроводжується поясненнями (гайдлайнами), які допомагають зрозуміти його застосування на практиці.

Основні принципи кодексу ACM охоплюють широке коло етичних аспектів роботи IT-спеціаліста. Серед фундаментальних принципів (розділ 1) можна виділити такі:

– прагнути *суспільного блага та добробуту*, запобігаючи можливій шкоді;

– *уникати завдання шкоди* (не нашкодити користувачам, суспільству або довкіллю);

– *чесність та надійність* у професійній діяльності;

– *справедливе ставлення* до всіх і *недопущення дискримінації*;

– *повага до інтелектуальної власності* та результатів чужої праці;

– *забезпечення конфіденційності та приватності* інформації, довіреної професіоналу;

– *дотримання конфіденційності* (таємниці фірми, приватних даних клієнтів тощо).

Для прикладу, кодекс ACM вимагає мінімізувати негативні наслідки обчислень для суспільства, зокрема загрози для здоров'я, безпеки, приватності людей.

Принцип про недискримінацію прямо забороняє будь-які прояви упередженості чи харасменту: *«Домагання, включно з сексуальними домаганнями, булінгом та іншими зловживаннями владою – це форма дискримінації, що обмежує рівний доступ до робочого середовища…»* – зазначає кодекс, підкреслюючи неприпустимість таких дій. Так само наголошено на повазі до приватності: IT-фахівці мають особливий обов'язок захищати приватні дані користувачів і конфіденційну інформацію, яка їм довірена.

Кодекс ACM також прямо говорить про збереження таємниці інформації – якщо спеціаліст отримує доступ до комерційної таємниці, приватних бізнес-стратегій, персональних даних тощо, він зобов'язаний охороняти їхню конфіденційність (за винятком випадків, коли розголошення потрібне для виявлення протизаконної чи неетичної діяльності).

Кодекс ACM не лише декларує принципи, але й надає інструменти для їх застосування. При кодексі створено систему роз'яснень та навчальних матеріалів: опубліковано офіційні *кейси-студії* з детальним аналізом, які показують, як слід діяти в типових етичних дилемах в IT. Наприклад, ACM розробив сценарії, що ілюструють застосування принципів кодексу до таких ситуацій, як приватність користувачів, конфлікт інтересів, чесність при розробці, взаємини у команді тощо. Таким чином, кодекс ACM виконує як регулятивну, так і освітню функцію: він встановлює стандарти етичної поведінки для спеціалістів і навчає, як ці стандарти практично впроваджувати у професійній діяльності.

2.2 Огляд Кодексу етики IEEE: ключові положення, цінності, сфери відповідальності

Institute of Electrical and Electronics Engineers (IEEE) – найбільше у світі професійне об'єднання інженерів, що об'єднує фахівців з електротехніки, електроніки, комп'ютерних технологій та суміжних галузей. IEEE встановило власний Кодекс етики, який зобов'язані підтримувати всі його члени. Цей кодекс сформульований як набір із десяти принципових положень (комітментів), які інженери урочисто обіцяють виконувати, визнаючи важливість своїх технологій для якості життя в усьому світі [2]. У 2020 році Кодекс етики IEEE було оновлено і доповнено, щоб відобразити сучасні акценти – зокрема, додано чіткі зобов'язання щодо недопущення харасменту та захисту приватності.

Ключові цінності та положення кодексу IEEE можна згрупувати за кількома напрямами.

Перш за все – безпека, здоров'я та добробут суспільства. Члени IEEE зобов'язуються *«ставити на перше місце безпеку, здоров'я і добробут населення»*, враховувати екологічну сталість та негайно повідомляти про будь-які фактори, що можуть становити небезпеку для людей чи довкілля. Цей пункт означає, що інженер має брати до уваги вплив своїх рішень на громадськість і

ніколи свідомо не наражати людей на ризик – навіть якщо це суперечить комерційним інтересам проєкту.

По-друге, неухильна чесність, об'єктивність і професійна компетентність. Кодекс IEEE зобов'язує інженера бути *чесним і реалістичним при наданні оцінок та заяв, базованих на доступних даних*, визнавати свої помилки та виправляти їх, а також визнавати внесок інших фахівців. Інженери повинні *постійно підтримувати та підвищувати свій професійний рівень*, виконувати завдання тільки в межах своєї компетенції або за умови повного розкриття своїх обмежень. Важливим принципом є уникнення конфлікту інтересів – інженер має по можливості не допускати реальних чи потенційних конфліктів між особистими (або корпоративними) інтересами і обов'язком перед суспільством чи замовником, а якщо конфлікт не можна уникнути – відкрито повідомити про нього зацікавлених сторін. Так само категорично забороняється будь-яка неправомірна діяльність, зокрема всі форми хабарництва чи корупції: член IEEE погоджується *«уникати протиправної поведінки в професійній діяльності та відкидати хабарництво у всіх його формах»*. Цей пункт підкреслює, що професійна етика вимагає від інженера незаплямованої чесності та незалежності суджень, яких не можна купити за матеріальну вигоду.

По-третє, надзвичайно важливим блоком принципів IEEE є ставлення до інших людей та суспільна відповідальність інженера. Кодекс визначає, що інженер має *«ставитися справедливо та з повагою до всіх людей»*, не допускати будь-якої дискримінації за ознаками раси, релігії, статі, віку, національності, гендерної ідентичності, інвалідності чи за будь-якими іншими ознаками. У оновленій редакції прямо зафіксовано: *«не допускати жодних форм харасменту, включно з сексуальними домаганнями чи булінгом»*. Це свідчить про посилену увагу IEEE до етики взаємин у професійній спільноті та робочих колективах – нетерпимість до образ, цькування, несправедливого поводження. Кодекс також зобов'язує *«уникати завдання шкоди іншим – їхній власності, репутації чи кар'єрі – шляхом неправдивих або зловмисних дій»*. Таким чином, принцип «не нашкодь» втілений і на рівні взаємодії з колегами та суспільством: інженер не має права дискредитувати інших чи наносити їм шкоду навмисно.

Нарешті, кодекс IEEE містить зобов’язання щодо поширення етичної культури серед колег. Члени IEEE обіцяють *«сприяти дотриманню цього кодексу колегами та співробітниками»* і *«не чинити репресій проти тих, хто повідомляє про можливі порушення»*. Це положення закликає інженерів активно підтримувати один одного у дотриманні етики, створюючи атмосферу, де обговорення та дотримання етичних норм є невід’ємною частиною професійної діяльності.

Кодекс етики IEEE, порівняно з кодексом ACM, коротший і більш загальний за формою, проте охоплює аналогічні сфери відповідальності: пріоритет безпеки публіки, чесність та компетентність, справедливість і повага, відмова від незаконних дій і корупції тощо. У ньому підкреслюється *«дотримання найвищих стандартів доброчесності та відповідальної поведінки»* у всіх професійних справах.

Цей кодекс є обов’язковим для членів IEEE і виконує роль морального компаса для інженерів різних спеціальностей, спрямовуючи їхні рішення так, щоб технологічний прогрес узгоджувався з етичними цінностями і служив людству.

2.3 Стандарт ISO/IEC 27001 як інструмент етичного управління безпекою: структура, призначення, основні вимоги

Окрім професійних кодексів поведінки, важливим компонентом етичної складової діяльності IT-спеціалістів є відповідальне управління інформаційною безпекою. Міжнародний стандарт ISO/IEC 27001 відіграє ключову роль у цьому аспекті. ISO/IEC 27001 – це міжнародний стандарт, розроблений Міжнародною організацією зі стандартизації (ISO) спільно з Міжнародною електротехнічною комісією (IEC), який встановлює вимоги до створення, впровадження, підтримання та постійного поліпшення системи управління інформаційною безпекою (англ. Information Security Management System, ISMS) [3]. Головна мета впровадження цього стандарту – захистити конфіденційність, цілісність та

доступність інформації в організації шляхом системного підходу до управління ризиками у сфері інформаційної безпеки.

Іншими словами, стандарт ISO/IEC 27001 надає організаціям чітку рамкову структуру, яка дозволяє ідентифікувати потенційні загрози для інформації, оцінювати ризики і застосовувати адекватні заходи захисту. Цей процес є безперервним і циклічним, що гарантує постійне вдосконалення рівня безпеки у відповідь на нові виклики і вразливості. З точки зору етики, дотримання ISO 27001 демонструє, що організація усвідомлює свою відповідальність за захист даних клієнтів, партнерів та суспільства і прагне виконувати цю відповідальність на найвищому рівні. Наприклад, впровадження стандарту часто розглядають як ознаку зрілості й надійності компанії: сертифікація за ISO 27001 підвищує репутацію та довіру клієнтів, показуючи, що організація серйозно ставиться до захисту інформації і діє прозоро, згідно з визнаними практиками безпеки.

Стандарт ISO/IEC 27001 має власну структуру розділів і вимог, характерну для стандартів систем менеджменту. Спочатку в ньому визначено контекст організації: необхідно окреслити сферу застосування ISMS, врахувати потреби зацікавлених сторін та правові й регуляторні вимоги до безпеки. Далі йдуть вимоги до лідерства – керівництво організації повинне демонструвати залученість у процес забезпечення безпеки, призначити відповідальних осіб, затвердити політику безпеки і виділити необхідні ресурси. Блок планування включає оцінювання ризиків (виявлення інформаційних активів, загроз і вразливостей) та визначення цілей і заходів безпеки. На етапі впровадження (функціонування) організація реалізує політики й процедури, впроваджує засоби захисту інформації. Етап перевірки передбачає моніторинг, внутрішній аудит та менеджмент-огляд системи для оцінки її ефективності. Нарешті, етап поліпшення – на основі результатів перевірок і змін у зовнішньому середовищі вносяться корективи і удосконалення до ISMS. Ці етапи утворюють циклічну модель управління.

Три основні аспекти інформаційної безпеки (CIA-тріада): конфіденційність, цілісність та доступність даних [4] (рис. 2.1).

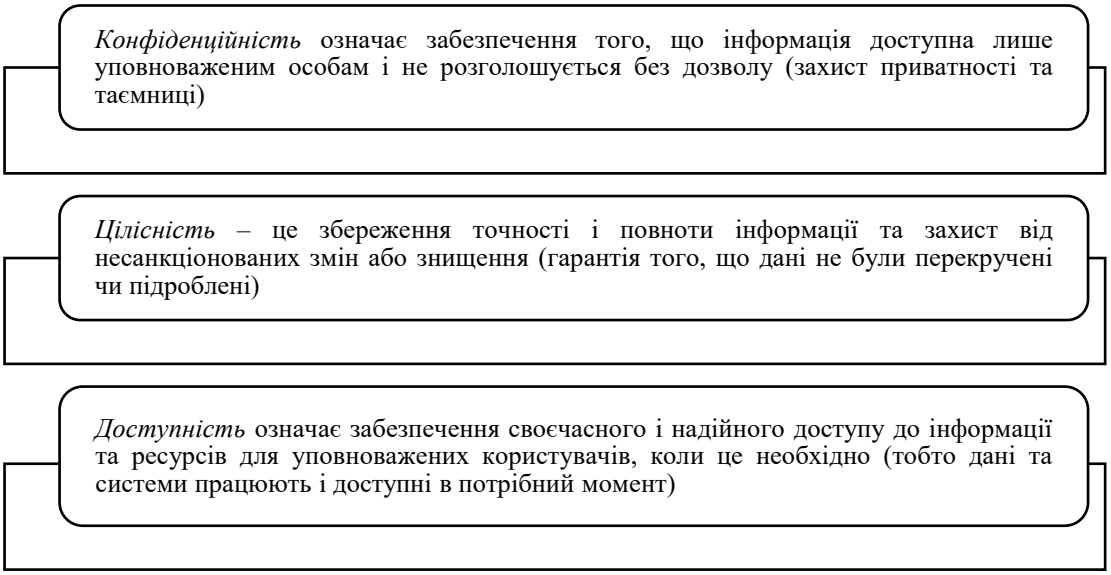

Рисунок 2.1 – Аспекти інформаційної безпеки (CIA-тріада)

Стандарт ISO 27001 приділяє увагу всім трьом цим аспектам: всі заходи безпеки спрямовані на те, щоб конфіденційна інформація залишалася захищеною від витоку, дані зберігали свою цілісність, а важливі системи були доступними для роботи навіть за умов інцидентів.

Цикл PDCA (рис. 2.2) лежить в основі стандарту ISO/IEC 27001 та інших систем менеджменту.

Стандарт ISO 27001 явно вимагає слідувати цьому циклу: організація повинна планувати заходи безпеки з урахуванням ризиків, виконувати їх, регулярно контролювати стан безпеки та працювати над помилками і поліпшеннями. Такий підхід дозволяє постійно підвищувати рівень захищеності інформації і оперативно реагувати на нові загрози.

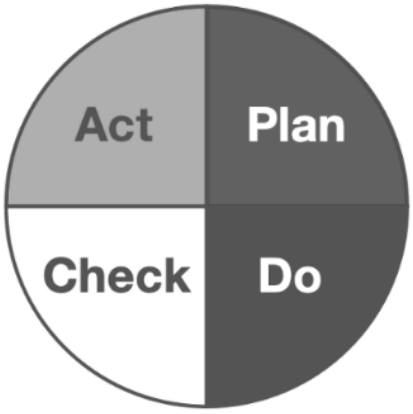

Рисунок 2.2 – Цикл PDCA (Plan – Do – Check – Act) [5]

Ця модель безперервного вдосконалення передбачає чотири етапи (рис. 2.3).

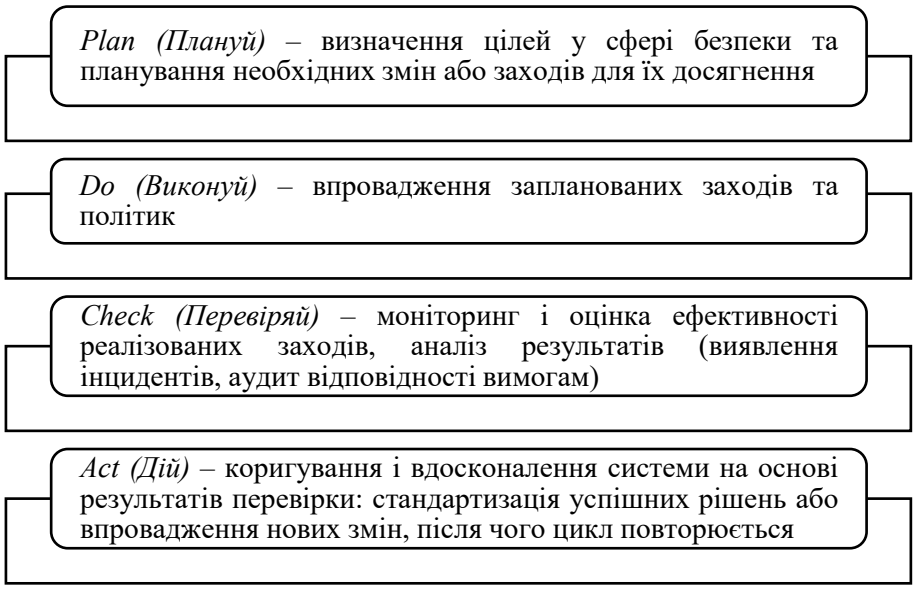

Рисунок 2.3 – Етапи циклу PDCA (Plan – Do – Check – Act)

Основні вимоги ISO/IEC 27001 конкретизовані в наборі заходів і політик, що їх організація має реалізувати. Значна частина стандарту міститься в додатку А (ISO/IEC 27002), де перелічено перелік *контролів* безпеки – тобто конкретних засобів і практик захисту. У новій версії 2022 року наводиться 93 контролі, згруповані у 4 категорії: організаційні, кадрові, фізичні та технологічні засоби безпеки. До прикладу, серед ключових контролів можна згадати такі:

- управління доступом – обмеження доступу до інформаційних ресурсів лише уповноваженим особам (впровадження систем автентифікації, розмежування прав користувачів тощо);
- класифікація інформації – визначення і класифікація важливих інформаційних активів (даних) за рівнями чутливості, аби застосувати до них відповідні заходи захисту;
- фізична безпека – захист фізичних носіїв інформації і інфраструктури (серверні кімнати, дата-центри) від несанкціонованого доступу чи стихійних лих (системи контролю доступу, відеонагляд, сигналізації);

– контроль пристроїв – заходи з управління та захисту пристроїв, які мають доступ до інформації (наприклад, політики безпеки для ноутбуків, смартфонів, шифрування дисків);

– криптографія – використання методів шифрування для захисту даних при зберіганні та передаванні, забезпечення цілісності і автентичності інформації;

– резервування і відновлення – регулярне резервне копіювання важливих даних та відпрацювання планів відновлення, щоб гарантувати доступність інформації у разі інцидентів чи збоїв;

– моніторинг та аудит – постійне відстеження подій безпеки, аналіз журналів та проведення аудитів, щоб вчасно виявляти вразливості або порушення та реагувати на них.

Ці та багато інших контролів створюють цілісну систему захисту, яка покликана закрити максимальне коло можливих шляхів реалізації загроз. Важливо підкреслити, що ISO 27001 є гнучким стандартом: організація сама визначає, які саме контролі з запропонованих є для неї актуальними, на основі оцінки ризиків. У підсумковому документі (*«Заява про застосовність»*) фіксується перелік прийнятих контролів. Таким чином, впровадження ISO 27001 стимулює компанію системно підійти до питань безпеки, приймаючи відповідальні рішення: де потрібно – посилити захист, а де ризики мінімальні – не витрачати зайвих ресурсів. Це теж етичний баланс між безпекою і ефективністю роботи.

Слід зазначити, що стандарт ISO/IEC 27001 має не стільки «моральний», скільки *управлінський* характер, тобто він не диктує особисту поведінку працівників, а встановлює організаційні процеси і політики. Проте його етичний вимір проявляється опосередковано: організація, яка дотримується ISO 27001, фактично реалізує свою етичну відповідальність перед клієнтами та суспільством за збереження довірених їй даних. В сучасних умовах приватність та інформаційна безпека стали суспільно значущими цінностями, тож компанії, що прагнуть діяти етично, добровільно імплементують ISO 27001 або аналогічні рамки, щоб гарантувати належний захист інформації. Багато підприємств

(особливо у сфері фінансів, IT-послуг, охорони здоров'я) сьогодні отримують *сертифікацію ISO 27001* – це означає, що незалежний аудит підтвердив відповідність їхньої системи безпеки вимогам стандарту. Сертифікація не є обов'язковою вимогою закону, але вона стала *де-факто* ознакою кращої практики: компанія демонструє, що впровадила належний рівень контролю і керує ризиками безпеки проактивно та відповідально. Це формує довіру з боку партнерів і користувачів, оскільки зменшує ймовірність витоків даних, кібератак та інших інцидентів, що можуть завдати шкоди людям.

2.4 Порівняльний аналіз ACM, IEEE і ISO/IEC 27001: спільні риси та відмінності

Спільні риси та цінності. Попри різну природу – перші два документи є *кодексами поведінки* для окремих професіоналів, а третій – *організаційним стандартом* – всі три запроваджені стандарти покликані гарантувати, що діяльність у сфері IT приносить користь суспільству і не завдає шкоди. І кодекси ACM та IEEE, і стандарт ISO 27001 виростають з єдиних базових цінностей: відповідальності, доброчесності, турботи про благо інших і запобігання шкоді. Наприклад, і ACM, і IEEE наголошують на пріоритеті суспільного блага та безпеки людей:

–ACM вимагає мінімізувати будь-які загрози для життя, здоров'я, безпеки і приватності, що можуть виникнути внаслідок впровадження комп'ютерних систем;

–аналогічно IEEE проголошує обов'язок ставити на перше місце безпеку, здоров'я і добробут публіки.

Обидва кодекси закликають фахівців поважати приватність особистої інформації: ACM підкреслює особливу відповідальність IT-спеціаліста за приватні дані користувачів, а IEEE прямо говорить про захист приватності інших як одну зі своїх засад. Так само обидва кодекси одностайні щодо недопустимості дискримінації та домагань: ACM засуджує будь-яку форму харасменту чи зловживання владою, що створює ворожу атмосферу, а IEEE зобов'язує

інженерів поводитися справедливо й з повагою та не допускати харасменту чи упередженості. Загалом, ACM та IEEE-етика мають багато спільних елементів: чесність і інтелектуальна чесність (не привласнювати чужі заслуги, не фальсифікувати дані), відкритість до конструктивної критики і виправлення помилок, обмін знаннями з суспільством про нові технології, постійне професійне зростання, виконання лише тієї роботи, на яку маєш компетенцію тощо. В усіх цих аспектах обидва кодекси збігаються, хоч і формулюють пункти дещо по-різному.

Стандарт ISO/IEC 27001, будучи іншого типу документом, також певною мірою поділяє згадані цінності. Звичайно, його основний фокус – інформаційна безпека, тобто конфіденційність, цілісність, доступність даних. Але і ACM, і IEEE-кодекси теж приділяють значну увагу безпечному поводженню з інформацією: наприклад, ACM вимагає захищати конфіденційну інформацію та приватність, а IEEE включає захист приватності та запобігання шкоді людям через інформаційні технології. Отже, у сфері захисту інформації та приватності стандарт ISO 27001 фактично забезпечує практичну реалізацію тих етичних принципів, які задекларовані в кодексах. Якщо кодекси кажуть: «не нашкодь користувачу, захисти його дані», то ISO 27001 дає інструментарій – як технічно та організаційно це зробити (через політики доступу, шифрування, моніторинг систем тощо). У цьому сенсі всі розглянуті стандарти прагнуть спільної мети: гарантувати, що IT-системи служать людям на благо і не становлять загроз – ні їхній безпеці, ні їхнім правам.

Відмінності в охопленні та підходах. Головна різниця між кодексами ACM/IEEE та стандартом ISO/IEC 27001 полягає в їхньому *предметі регулювання*. ACM і IEEE – це кодекси етики для особистої поведінки фахівців, натомість ISO 27001 – технічний стандарт для організаційного управління. Тобто перші адресовані безпосередньо індивідуумам (інженерам, розробникам, науковцям), регулюючи їхню поведінку в найрізноманітніших ситуаціях – від написання коду і спілкування в команді до публічних виступів чи конфліктів інтересів. Натомість ISO 27001 звернений до керівництва компаній та IT-служб – він встановлює, які процеси та практики повинні існувати в організації, щоб

забезпечити належний рівень інформаційної безпеки. Відповідно, зміст документів різниться: кодекси ACM/IEEE містять загальні моральні імперативи (типу «будь чесним», «уникай дискримінації», «поліпшуй компетентність»), тоді як ISO 27001 містить перелік конкретних вимог (наприклад, «мати реєстр активів», «проводити оцінку ризиків щорічно», «впровадити контроль фізичного доступу до серверної» тощо).

Ще одна відмінність – широта охоплення етичних питань. Кодекси ACM та IEEE мають дуже широкий діапазон: вони торкаються професійних чеснот (чесність, справедливість, повага), соціальної відповідальності, питань правового дотримання (виконання законів, повага до інтелектуальної власності), міжособистісних відносин у колективах, і навіть закликають служити суспільству (наприклад, брати участь в роз'ясненні технологій для громадськості, сприяти сталому розвитку). Наприклад, ACM прямо вимагає від членів професії *враховувати потреби менш захищених груп населення*, сприяти усуненню цифрової нерівності та забезпеченню доступності технологій для людей з інвалідністю (усе це випливає з принципів справедливості та недискримінації). Натомість стандарт ISO 27001 не охоплює такі соціально-етичні теми, як дискримінація чи конфлікти інтересів, – його сфера значно вужча і технічніша, обмежена питаннями інформаційної безпеки. Тобто ISO 27001 не скаже, як інженеру поводитися в соцмережах чи чи повинен він повідомити про небезпечний дефект продукту громадськості – це радше поле дії етичних кодексів.

Різняться і механізми впровадження та контролю. Кодекси етики (ACM, IEEE) за своєю природою *добровільні*: їх дотримання базується на особистій совісті та професійній гордості фахівців. Хоча професійні організації можуть мати процедури розгляду порушень (скажімо, ACM має Комітет з етики та процедури дисциплінарного впливу за порушення кодексу, на практиці застосування санкцій обмежене випадками серйозних проступків. Натомість ISO 27001 зазвичай впроваджується як частина *формальної системи менеджменту*: відповідність вимогам підтверджується зовнішніми аудиторами, видається офіційний сертифікат. Якщо організація не відповідає вимогам,

сертифікацію не видадуть або відкличуть. Таким чином, ISO 27001 – це ринковий механізм регуляції (компанія дотримується стандарту, щоб отримати конкурентну перевагу і довіру клієнтів), тоді як кодекси – морально-етичний механізм саморегуляції спільноти.

Різниця в акцентах ACM vs IEEE. Хоча кодекси ACM та IEEE багато в чому схожі, між ними є певні нюанси і різниця у тоні подачі. ACM детальніший і орієнтований на сферу IT: він має більше роз'яснень, особливу увагу приділяє таким питанням, як збереження конфіденційності даних, захист інтелектуальної власності (авторських прав, патентів, ліцензій) та дотримання конфіденційності інформації роботодавця чи клієнта. ACM навіть включає пункт: *«Не використовувати комп'ютерні ресурси та інформацію без дозволу або якщо до цього не змушує суспільне благо»*, наголошуючи на етиці у доступі до інформаційних систем. Кодекс IEEE, будучи ширшим за охопленням інженерних дисциплін, менш докладний щодо саме комп'ютерної специфіки – наприклад, він не згадує прямо про авторські права чи «несанкціонований доступ», але зате додає інші аспекти, важливі для інженерів (такі як екологічна стійкість, обов'язок дотримуватися законів і т. д.). Можна сказати, що ACM робить акцент на етиці обробки інформації, а IEEE – на етиці інженерної діяльності загалом, але обидва переслідують одну мету – утвердити стандарти чесної, відповідальної та шанобливої поведінки.

Що стосується зв'язку кодексів з ISO 27001, то їх не можна протиставляти, швидше – вони працюють на різних рівнях. *Кодекси ACM/IEEE формують етичний світогляд спеціаліста*, а *ISO 27001 дає інструменти для реалізації певної частини цього світогляду на рівні організації*. Наприклад, кодекси кажуть: «поважай приватність користувачів, захищай дані від неправомірного доступу» – ISO 27001 втілює це через систему контролів (управління паролями, шифрування тощо). Кодекси закликають «будь компетентним і постійно вчися» – ISO 27001 вимагає проводити тренінги персоналу з питань безпеки, підвищувати обізнаність. З іншого боку, ISO 27001 не охоплює багато етичних аспектів, тому повна етична картина вимальовується лише при використанні *обох* типів стандартів. Професіонал в IT має керуватися як нормами кодексу

етики (щоб не діяти аморально), так і стандартами належної практики (щоб діяти професійно й безпечно).

Отже, ACM, IEEE та ISO 27001 – не взаємозамінні, а взаємодоповнювальні елементи етичної інфраструктури в галузі IT. Вони поділяють фундаментальні цінності (принцип «не нашкодь», чесність, справедливість, захист інформації), але різняться сферою застосування і способом впровадження. Разом ці стандарти створюють багаторівневу систему: від особистих моральних принципів кожного IT-фахівця – до корпоративних політик і процедур, що забезпечують етичність і безпеку діяльності цілих організацій.

2.5 Приклади практичного застосування етичних кодексів у діяльності IT-спеціалістів

Теоретичні принципи етичних кодексів знаходять своє відображення у реальних ситуаціях, з якими стикаються IT-спеціалісти. Розглянемо декілька прикладів практичного застосування норм ACM та IEEE, а також роль стандарту ISO 27001 у повсякденній професійній діяльності.

Приклад 1: Протидія образливій поведінці в команді (кейс ACM). Уявімо ситуацію: технічний керівник проєкту (Team Lead) дозволяє собі грубу, принизливу поведінку щодо підлеглих – кричить при помилках, публічно їх висміює, а іноді навіть знімає авторівство з учасників команди, які йому не подобаються. Такий випадок розглянуто в одному з навчальних кейсів ACM, і аналіз показав, що кодекс етики ACM чітко кваліфікує подібну поведінку як неприйнятну. Вербальні образи та цькування порушують принцип «уникати шкоди», адже завдають психологічної шкоди і створюють небезпечне, токсичне середовище (порушення принципу 1.1 про благо і безпечне соціальне середовище). Позбавлення співробітників заслуженої авторської згадки – це не тільки несправедливо, але й суперечить вимозі «давати належну заслугу за результати праці» (принцип 1.5 про інтелектуальну власність). А вибіркове покарання тільки жінок у команді свідчить про гендерну упередженість, що грубо порушує принцип недискримінації 1.4. Більше того, керівник команди,

який потурає такій поведінці або відмахується від скарг, сам порушує свої обов'язки лідера за кодексом (у ACM є спеціальні принципи 3.3 і 3.4, що вимагають від керівників дбати про благополуччя команди і підтримувати етичну політику організації).

Цей приклад демонструє, як етичний кодекс надає чіткі критерії оцінки поведінки: і рядові співробітники, і менеджери можуть звернутися до нього, аби визначити, що є недопустимим, і обґрунтувати необхідність дисциплінарних заходів або змін у корпоративній культурі. Врешті-решт, дотримання кодексу захищає не тільки окремих працівників, але й якість роботи команди: у здоровій, поважній атмосфері колеги краще співпрацюють, вільно обмінюються ідеями, що позитивно впливає на результати проектів.

Приклад 2: Конфлікт інтересів та відмова від хабара (сценарій IEEE). Інженер-програміст працює консультантом і одночасно веде декілька проектів для різних замовників. Один із клієнтів пропонує йому додаткову фінансову «винагороду» (хабар) за те, щоб він прискорив роботу над їхнім проектом, навіть якщо доведеться менше уваги приділити іншим клієнтам. Така ситуація створює очевидний конфлікт інтересів – інженер має особисту вигоду, яка спонукає його знехтувати інтересами інших замовників і професійними зобов'язаннями рівного ставлення. Кодекс IEEE однозначно вимагає уникати реальних чи уявних конфліктів інтересів та відкрито заявляти про них. В даному випадку правильним кроком з точки зору етики було б відхилити таку «пропозицію» і, за необхідності, повідомити керівництву про неї. Адже прийняти її – означало б порушити одразу два пункти кодексу IEEE: про конфлікт інтересів і про недопустимість хабарництва (інженер «відкидає хабарництво у всіх формах» згідно з пунктом 4 кодексу). Практика показує, що професіонали, які дотримуються цих принципів, у довгостроковій перспективі здобувають більше довіри і репутацію доброчесних експертів. Натомість ті, хто погоджується на неетичні «вигоди», ризикують не тільки своєю репутацією, але й можуть понести юридичну відповідальність.

Отже, етичний кодекс IEEE слугує інженеру щитом від сумнівних компромісів: посилаючись на нього, спеціаліст може обґрунтовано відмовитися

від пропозицій, що суперечать професійній етиці, навіть якщо вони привабливі фінансово.

Приклад 3: Використання ISO 27001 у реагуванні на кіберінцидент. Розглянемо організацію-розробника програмного забезпечення, яка зберігає персональні дані користувачів. Однієї ночі компанія стикається з кіберінцидентом – виявлено ознаки несанкціонованого проникнення до бази даних. Як спрацьовує етичний підхід до безпеки в цьому випадку? Якщо компанія впровадила стандарт ISO 27001, у неї буде чіткий план реагування на інциденти: команда безпеки оперативно ізолює уражені системи, запускає процедури оповіщення, проводить розслідування. ISO 27001 вимагає реєструвати і аналізувати такі інциденти, а також повідомляти тих, кого це стосується (наприклад, клієнтів або регуляторів, якщо були скомпрометовані їхні дані). Етичний аспект тут проявляється у прозорості та відповідальності: замість замовчування проблеми, організація, що дотримується найкращих практик (у тому числі етичних), повідомить користувачів про витік даних і порадить їм змінити паролі чи вжити інших заходів захисту. Хоча закон (наприклад, GDPR) теж зобов'язує це зробити, саме етична культура компанії визначає, наскільки сумлінно і швидко вона виконає свій обов'язок перед клієнтами. Наявність сертифікованої системи за ISO 27001 зазвичай означає, що компанія проводила навчання персоналу, відпрацьовувала плани дій – тож у критичній ситуації люди знають, як діяти відповідально. У ширшому сенсі, стандарт ISO 27001 привносить етику в повсякденні процеси управління: наприклад, розробники вчаться принципу «privacy by design» (приватність за замовчуванням) – не збирати зайві персональні дані і шифрувати чутливу інформацію, адміністратори систем – принципу найменших привілеїв (давати доступ тільки тим, кому це потрібно). Все це відповідає етичним засадам захисту прав користувачів і мінімізації шкоди, проголошеним в кодексах.

Таким чином, у реальних бізнес-ситуаціях ISO 27001 слугує практичним втіленням етичних зобов'язань компанії забезпечити безпеку і конфіденційність інформації.

Приклад 4: Дилема випуску небезпечного продукту. Іноді IT-спеціалісти опиняються перед складним вибором: продукт (скажімо, нову версію програмного забезпечення або пристрій) потрібно випустити у визначений термін, але вони знають про серйозну невиправлену вразливість або дефект, що може зашкодити користувачам. Етичні кодекси дають однозначну підказку: безпека і благо користувача важливіші за комерційний інтерес. Інженер, який керується кодексом ACM чи IEEE, швидше за все наполягатиме на відтермінуванні релізу до усунення проблеми або принаймні на відкритому попередженні користувачів, навіть якщо керівництво чинитиме тиск. Принцип «не завдати шкоди» (ACM 1.2) та зобов'язання «ставити безпеку публіки на перше місце» (IEEE 1) створюють моральний імператив: не можна свідомо випускати в світ продукт, який може призвести до несправності, втрати даних чи травм. У ряді відомих історичних випадків (наприклад, провал запуску космічного апарату через баг в програмі або пригальмовування автомобіля через збій програмного забезпечення) розслідування згодом показували, що інженери відчували проблему, але не зупинили процес. Сьогодні все більше компаній заохочують етичну сміливість інженерів повідомляти про ризики без страху покарання – це якраз дух професійних кодексів. У поєднанні зі стандартами на кшталт ISO 27001 (який теж вимагає проводити оцінку ризиків і тестувати продукти на безпеку) кодекси етики створюють атмосферу, де питання безпеки та якості превалюють над поспішним прибутком, що зрештою вигідно і самій компанії, і споживачам.

Наведеними прикладами далеко не вичерпуються всі ситуації, де проявляється роль етичних норм. Проте вони ілюструють головне: етичні кодекси – це не абстрактні декларації, а дієві настанови для практичних дій. Коли спеціаліст добре знає принципи ACM/IEEE, він має певний «внутрішній компас», який допоможе йому прийняти правильне рішення у складній моральній дилемі. А стандарти на кшталт ISO 27001 надають йому інструменти і процеси, щоб таке рішення реалізувати в організаційному контексті. Компанії, що культивують повагу до етичних кодексів і впроваджують найкращі практики

безпеки, як правило, успішніше уникають скандалів, втримують довіру клієнтів і створюють здорове робоче середовище для своїх команд.

ЛЕКЦІЯ 3
ЕТИКА РОЗРОБНИКІВ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА СИСТЕМНИХ ІНЖЕНЕРІВ

Мета – розкрити основні етичні принципи та норми, що регулюють діяльність розробників програмного забезпечення та системних інженерів, визначити їхню відповідальність перед користувачами, суспільством і роботодавцями. Лекція має на меті сформувати розуміння професійної доброчесності, важливості етичного прийняття технічних рішень, а також ознайомити з типовими етичними викликами в процесі розробки, тестування й впровадження ІТ-систем.

3.1 Специфіка етичної відповідальності розробника ПЗ: вплив на користувача, складність рішень, етика коду

Розробник програмного забезпечення (ПЗ) безпосередньо впливає на кінцевого користувача своїми рішеннями. Продукти ІТ-сфери сьогодні охоплюють мільйони людей по всьому світу, тому дотримання етичних принципів є одним із ключових обов’язків розробника. Кожна функція або інтерфейс, написані програмістом, можуть покращити життя користувача або, навпаки, завдати шкоди – наприклад, якщо нехтувати приватністю чи безпекою даних [6]. Етична відповідальність розробника передбачає турботу про добробут і безпеку користувачів: програміст повинен створювати рішення, що не завдадуть шкоди, будуть надійними та захищеними від зловживань [7]. Важливим аспектом є також довіра користувачів – вона формується, коли розробник поважає приватність, прозоро поводиться з даними та відповідає очікуванням щодо якості продукту. Таким чином, вплив на користувача накладає на розробника моральний обов’язок пріоритетно ставити інтереси та безпеку людей вище за суто технічні або бізнесові вигоди.

В процесі розробки ПЗ інженер часто стикається зі складними етичними рішеннями, що не мають однозначної відповіді. Розробник повинен балансувати

між вимогами функціональності, швидкістю випуску продукту, продуктивністю системи та заходами безпеки. Наприклад, додаткова шифрація даних підвищує конфіденційність, але може сповільнити роботу програми; навпаки, спрощення захисту прискорить розробку, але ризикує безпекою користувачів. Нерідко важко визначити «золоту середину» – скільки саме захисту або тестування є достатньо. Як відзначає практика, не існує простої формули: підвищення безпеки є благом, допоки воно не завадить працездатності або не заблокує випуск продукту вчасно [7]. Такі дилеми вимагають від програміста професійного судження та критичного мислення з огляду на етичні наслідки. Рішення доводиться ухвалювати, зважуючи потенційний ризик для користувача та користь від функціоналу. Наприклад, при виявленні помилки (bug) розробник мусить визначити її пріоритет: чи негайно виправити, чи можна відкласти? Етичною є позиція, за якої виправлення критичних багів не відкладається, адже навіть незначна на перший погляд помилка може призвести до несподіваних наслідків для користувачів [7]. Складність рішень у ПЗ полягає ще й у тому, що наслідки технологічних рішень не завжди передбачувані: тому розробник має мислити на кілька кроків вперед, оцінюючи, як його код може бути використаний або навіть зловживаний у майбутньому.

Окремо варто виділити «етику коду» – моральні принципи, яких дотримується програміст безпосередньо при написанні та впровадженні програмного коду. Етичний розробник пише чесний та якісний код, уникаючи навмисного приховування недоліків або створення «бекдорів» (прихованих лазівок у систему).

По-перше, це означає відповідальність за продукт: програміст має правдиво інформувати колег, керівництво і користувачів про можливості та обмеження свого ПЗ, не давати неправдивих обіцянок щодо функціоналу.

По-друге, етика коду передбачає прагнення до надійності та відсутності дефектів: розробник зобов’язаний своєчасно виявляти, виправляти та повідомляти про помилки у програмному забезпеченні. Замовчування відомих проблем або свідоме залишення уразливостей у коді є неетичним кроком, що підриває довіру.

По-третє, повага до інтелектуальної власності та відкритого коду також є частиною етики: використовуючи чужий код чи бібліотеки, слід дотримуватися ліцензій та визнавати авторство, щоб не порушувати прав інших розробників.

Нарешті, етика коду включає уникнення упередженості та дискримінації в алгоритмах – програміст повинен стежити, щоб його код не містив несвідомих алгоритмічних упереджень, наприклад, під час розробки систем штучного інтелекту чи обробки даних про людей. Таким чином, етична відповідальність розробника ПЗ охоплює як глобальні аспекти (вплив на користувачів і суспільство), так і щоденні практики кодування (якість, чесність і професіоналізм у написанні коду).

3.2 Етика системного інженера: вплив архітектурних рішень, відповідальність за інтеграцію і надійність

Системний інженер відповідає за проектування комплексної архітектури системи та забезпечення узгодженої роботи всіх компонентів – програмних, апаратних, мережевих. Ця роль має ширший масштаб впливу, оскільки помилка або прорахунок на рівні системної архітектури може спричинити наслідки для великої кількості користувачів або навіть для суспільства в цілому. Архітектурні рішення системного інженера визначають фундаментальні характеристики системи – безпеку, надійність, масштабованість, відповідність зовнішнім вимогам (регуляторним, нормативним тощо). Тому етична відповідальність системного інженера є надзвичайно високою: він повинен зважувати не лише технічну доцільність, а й можливі моральні та суспільні наслідки своїх рішень. Наприклад, системні інженери проектують такі критичні системи, як безпілотні автомобілі, системи охорони здоров’я або фінансові платформи, і від їхніх рішень залежить життя та благополуччя людей [9]. У таких випадках недостатньо просто виконати технічне завдання – потрібно переконатися, що проект не наражає на небезпеку користувачів і враховує етичні принципи, як-от пріоритет безпеки людини, конфіденційність даних, справедливість алгоритмів прийняття рішень.

Вплив архітектурних рішень на етичність системи проявляється в багатьох аспектах. Одне з ключових завдань системного інженера – закласти в систему механізми, що запобігатимуть зловживанням і зменшать ризики. Наприклад, архітектура повинна передбачати захист від відмов (fail-safe): етично спроектована система має резервні копії або дублюючі сенсори там, де відмова одного компоненту може призвести до катастрофи (як у авіації чи автомобілях). Якщо ж інженер, з метою економії, свідомо виключає резервування або покладається на один датчик чи точку відмови, це може розглядатися як етичний компроміс з потенційно небезпечними наслідками. Етичний системний інженер, навпаки, обстоює рішення, що мінімізують ризики для життя і здоров'я користувачів та операторів системи. Зокрема, він зобов'язаний врахувати, які проблеми можуть виникнути при найгіршому сценарії роботи системи, і зробити все можливе, аби система залишалася безпечною навіть у випадку збоїв.

Системний інженер не тільки розробляє архітектуру, але й відповідає за інтеграцію компонентів і загальну надійність системи. Інтеграція означає з'єднання різних модулів (програмних і апаратних) у єдине ціле. Етично правильний підхід до інтеграції полягає в тому, щоб усі компоненти працювали узгоджено і прозоро, без прихованих несумісностей. Інженер повинен переконатися, що суміщення модулів не призводить до непередбачених уразливостей чи проблем. Наприклад, інтегруючи сторонній програмний компонент, слід оцінити його безпеку і ліцензійну чистоту, щоб не порушити прав користувачів або авторів цього компоненту. Надійність системи є одним з головних показників професійної етики системного інженера. Це передбачає, що система має працювати коректно у різних умовах, бути стійкою до збоїв і атак. З етичної точки зору, ненадійна система, яка часто падає або дає збої, є неприйнятною, особливо якщо від її роботи залежать люди (наприклад, системи медичного моніторингу, енергомережі тощо). Отже, інженер зобов'язаний докласти максимум зусиль для тестування, верифікації та валідації системи, щоб мінімізувати ймовірність критичних відмов. Він відповідає за створення процесів моніторингу та швидкого реагування на інциденти. Етична відповідальність тут полягає і в чесному інформуванні замовників та

користувачів про рівень надійності: приховувати відомі проблеми стабільності системи – значить ризикувати довірою і безпекою людей.

В цілому, етика системного інженера охоплює ті ж базові принципи, що й для інших інженерів: не нашкодь, забезпеч чесність і дотримання зобов'язань, поважай закон та права осіб. Але акценти дещо різні. Системний інженер діє на стику багатьох сфер, тому має враховувати багатосторонні наслідки: правові (відповідність стандартам і регуляціям), соціальні (довіра суспільства, відсутність дискримінації), екологічні (вплив системи на довкілля) тощо. Наприклад, при обробці даних користувачів системний інженер відповідає за дотримання принципів конфіденційності та захисту приватності у всій системі – від баз даних до каналів передачі інформації. Він також має стежити, щоб система не упереджувала або не дискримінувала окремі групи (особливо якщо це складні IT-системи з елементами AI). Крім того, системний інженер повинен дбати про відповідність правовим вимогам і стандартам індустрії: недотримання законів (наприклад, вимог безпеки чи стандартів надійності) не лише несе юридичні ризики, але й є етично безвідповідальним щодо суспільства.

Відповідальність за інтеграцію та надійність також означає бути чесним і прозорим із стейкхолдерами (замовниками, користувачами, регуляторами). Якщо проект має обмеження або потенційні ризики, системний інженер зобов'язаний чітко повідомити про них, запропонувати шляхи мінімізації та не замовчувати проблем. Це питання довіри: етичні практики – основа побудови довіри між інженером та суспільством. Наприклад, якщо система обробляє чутливі дані, етично вимагати впровадження суворих заходів безпеки (шифрування, контроль доступу) навіть якщо це збільшує бюджет чи строки. Компроміси, що підривають безпеку чи надійність системи заради економії, суперечать професійній етиці системних інженерів. Історія знає випадки, коли прорахунки в архітектурі чи свідоме спрощення системи призводили до трагедій – від аварій шатлів до авіакатастроф. Тому для системного інженера етична норма – ставити безпеку людей, надійність та суспільне благо вище комерційних інтересів. Як підсумок, етика системного інженера проявляється у тому, щоб

складні технічні рішення приймалися з урахуванням ризиків, довгострокових наслідків і інтересів суспільства, а не лише вимог технічного завдання.

3.3 Етичні дилеми у проєктуванні ПЗ і систем: приховані функції, збір даних, зворотна сумісність, lock-in, утримання помилок

Процес розробки програмних та системних рішень сповнений різноманітних етичних дилем, коли інженери мають обирати між зручністю/вигодою і моральними принципами. Розгляньмо декілька типових ситуацій, зокрема:

–приховані функції (прихований функціонал). Часом в програмне забезпечення свідомо закладають можливості, про які не повідомляють користувачам відкрито. Це можуть бути так звані *«Easter eggs»* (невинні «пасхальні яйця» – приховані жарти) або ж серйозніші речі – наприклад, прихований збір даних чи бекдор для віддаленого доступу. З етичної точки зору, будь-яка суттєва функція, яка впливає на права чи досвід користувача, не має бути прихованою. Якщо розробник впроваджує функціонал, що збирає інформацію або змінює поведінку програми без відома користувача, це підриває довіру. Особливо неприпустимо приховувати функції моніторингу або стеження. Наприклад, випадки, коли мобільний застосунок таємно записує розмови або надсилає дані на сервер, розцінюються як грубе порушення приватності. Етична норма тут – прозорість: користувач має право знати, що робить програма. Прихований функціонал часто тісно пов’язаний з наступним пунктом (збором даних). Важливо підкреслити, що прихованою може бути не тільки технічна функція, а й прихований намір програміста або компанії. Якщо справжня мета програми відрізняється від декларованої, це етично проблемно. Як зазначають фахівці, «ховати» збір даних у, здавалося б, безневинному додатку (наприклад, грі чи фоторедакторі) з наміром продати цю інформацію – це порушення довіри та етичних норм приватності й конфіденційності даних. Розробник, який свідомо додає подібну приховану функцію, стоїть перед дилемою: виконати наказ керівництва чи зберегти професійну етику. Правильним рішенням було б

відмовитися від обману користувача, натомість реалізувати ці функції відкрито (наприклад, запитавши згоду на збір даних або надавши вибір відключити функцію);

– збір даних та приватність. У цифрову епоху дані користувачів стали цінним ресурсом, і розробники часто інтегрують у продукти засоби збору інформації: від файлів логів і трекерів до модулів аналітики. Етична дилема: де межа між корисним збором даних для покращення сервісу та надмірним стеженням, що порушує приватність? З одного боку, збирати деякі дані необхідно (для роботи функцій чи виправлення багів). З іншого – кожен зайвий біт персональної інформації, зібраний без явної потреби та згоди, ставить під питання етичність продукту. Наприклад, програма може зберігати детальні журнали дій користувача. Розробники часто роблять це за замовчуванням для налагодження. Але слід спитати: чи захищені такі логи належним чином, хто має до них доступ і скільки часу вони зберігаються?. Якщо журналюються конфіденційні дії (скажімо, медичні запити чи фінансові транзакції), то утримання таких даних – велика відповідальність. Етично розробник має застосовувати принцип мінімізації даних: збирати лише те, що дійсно потрібно, і тільки за згодою користувача. Крім того, інформацію слід зберігати безпечним чином та знищувати, коли в ній більше немає потреби. На жаль, бізнес-моделі багатьох безкоштовних сервісів будуються за принципом: "якщо ви не платите за продукт – продуктом є ви самі". Персональні дані перетворюються на товар для реклами чи продажу третім сторонам. Це породжує конфлікт інтересів: розробник може бути під тиском перетворити користувача на «джерело прибутку» шляхом максимально можливого збору інформації. Етичний підхід полягає в тому, щоб бути чесним із користувачами щодо монетизації даних: чітко повідомляти, які дані збираються і з якою метою, надавати можливість відмовитися. Таким чином, дилема збору даних вирішується на користь прозорості та вибору користувача. Розробник, що дотримується етики, радше обмежить себе у потенційному заробітку, ніж зрадить довіру аудиторії шляхом прихованого стеження;

– зворотна сумісність та ефект «lock-in». Зворотна сумісність означає здатність нових версій програмного забезпечення або систем працювати з даними чи компонентами від попередніх версій. Vendor lock-in (ефект блокування постачальником) виникає, коли користувач або клієнт стає залежним від закритих форматів чи пропрієтарних технологій певної компанії настільки, що перехід до альтернатив стає надто складним. Етична дилема для розробників і компаній: *чи повинні ми підтримувати відкритість і сумісність, навіть якщо це спрощує користувачу перехід до конкурентів?* З комерційного погляду, lock-in вигідний – він «прив'язує» клієнтів. Але з позиції етики технологій, навмисне створення несумісностей або штучне ускладнення експорту даних – це дія всупереч інтересам користувача. Наприклад, компанія може припинити підтримку старого формату файлів, щоби примусити всіх купити нову версію ПЗ – хоча технічно можна було б зберегти сумісність. Або виробник гаджетів може використовувати нестандартні роз'єми/протоколи, щоб користувач не міг підключити сторонні пристрої. Етично, інженери мають прагнути до максимальної інтероперабельності своїх систем. Використання відкритих стандартів і підтримка зворотної сумісності розглядається як благо для галузі: це стимулює інновації, чесну конкуренцію і дає користувачам свободу вибору. Як зазначається в рекомендаціях, підтримуючи стандарти та розумну зворотну сумісність, розробники заохочують інновації та зменшують антиконкурентні практики, водночас підвищуючи довіру користувачів до технологій [10]. З іншого боку, замкнуті екосистеми часто критикуються за неетичність: вони можуть навмисно ускладнювати життя користувачу (скажімо, неможливість перенести свої дані у разі зміни платформи) задля утримання його в межах платних сервісів. Отже, перед інженером стоїть вибір – слідувати короткостроковій бізнес-логіці чи довгостроковим етичним принципам. В більшості випадків етичний імператив – на боці відкритості: краще втратити частку контролю над користувачем, але натомість здобути репутацію чесного ринку гравця та забезпечити користувачам справедливі умови;

– утримання помилок (bugs) у системі. У процесі розробки практично неминуче виникають баги – помилки в коді чи проектуванні. Питання, яке

виникає: як наполегливо слід виправляти помилки, особливо якщо їх виправлення вимагає значних ресурсів або впливає на графік випуску продукту? Чи етично випустити продукт раніше, знаючи про певні недоліки, сподіваючись «доопрацювати на льоту»? В ідеалі, звісно, кожну знайдену помилку треба виправляти оперативно. Але реальні умови (дедлайни, бюджет) диктують пріоритети: незначні баги можуть відкласти на потім. Етична дилема проявляється тоді, коли програміст або компанія знають про серйозну проблему, яка може зашкодити користувачам, але вирішують не усувати її негайно – наприклад, щоб встигнути до релізу або уникнути витрат. Така ситуація прямо пов'язана з поняттям бездіяльності. Ще Айзек Азімов у «Законах робототехніки» писав, що робот не має права бездіяти, якщо бездіяльність призведе до шкоди людині. Аналогічно, для розробника бездіяльність щодо відомого багу, який може нашкодити, – неетична. Однак на практиці інженери часто стикаються з тим, що багато помилок лишаються ігнорованими та невиправленими, бо ніхто не хоче навіть думати про них, особливо якщо вони здаються рідкісними чи малоймовірними. Наприклад, уявімо, що в програмі знайдено уразливість безпеки, але реалізувати виправлення складно і дорого. Якщо випуск оновлення відкладають, користувачі залишаються під загрозою – це неетично. Правильний крок – поставити безпеку вище комерційного комфорту, негайно працювати над патчем і, бажано, попередити користувачів про ризик (що рідко робиться, але було б чесно). Інший приклад – приховування помилок. Деякі компанії замовчують баги, сподіваючись, що ніхто не помітить, або аби уникнути поганої слави. З етичного погляду, така практика є хибною. Натомість принцип професійної етики вимагає прозорості та відповідальності: визнайте помилку, виправте її, винесіть уроки. У програмуванні існує поняття «технічного боргу» – накопичених невиправлених проблем. Етично допустимо мати технічний борг, якщо він не шкодить користувачу безпосередньо і планомірно зменшується з часом. Але створювати «етичний борг» – тобто відкладати виправлення критичних помилок на невизначений час – непрофесійно. Підсумовуючи, утримання помилок може бути виправдане лише у випадку, коли їх вплив мінімальний і прозоро комунікується. В усіх інших ситуаціях етика вимагає

активної позиції: виявив проблему – вирішу або пом’якши її якомога швидше, навіть якщо це невигідно в короткостроковому плані.

3.4 Відмінність етичної відповідальності розробника ПЗ і системного інженера

Розробник фокусується на користувачах, коді та функціях, тоді як системний інженер – на загальній архітектурі, інтеграції та надійності системи (рис. 3.1).

Рисунок 3.1 – Етичні акценти ролей розробника ПЗ та системного інженера

Хоча базові етичні принципи (такі як «не нашкодь», чесність, повага до прав та приватності) є спільними для обох ролей, між етичною відповідальністю розробника програмного забезпечення і системного інженера є суттєві відмінності, зумовлені різним характером їхньої роботи. Розробник ПЗ (software developer) здебільшого працює над створенням і вдосконаленням конкретних програм та функціоналу, занурений у написання коду. Натомість системний

інженер (systems engineer) займається інтегрованою системою загалом, слідкуючи, щоб усі частини системи працювали злагоджено і відповідали визначеним вимогам. Іншими словами, *«роль системного інженера – гарантувати, що всі елементи системи узгоджуються між собою, тоді як програмісти відповідають за побудову самих технологічних компонентів та коду»* [11].

З огляду на це, масштаб впливу та пріоритети етичних питань різняться. Розробник ПЗ приймає рішення на мікро-рівні продукту: які алгоритми реалізувати, як обробити дані користувача, як реагувати на помилки. Його етичні дилеми часто стосуються конкретного функціоналу: чи впроваджувати потенційно корисну, але сумнівну з погляду приватності опцію? як балансувати між зручністю інтерфейсу і чесністю (наприклад, не маніпулювати користувачем через дизайн)? чи писати код швидко, пожертвувавши якістю, чи навпаки? Тобто, відповідальність розробника локалізована, ближча до безпосереднього досвіду користувача та якості програмного продукту. Поганий код, залишений розробником, може спричинити баги або витік даних, що вдарить по окремих користувачах чи репутації компанії. Відповідно, етичний розробник концентрується на тому, щоб продукт був безпечним, зручним та не порушував прав людей – він як би виступає адвокатом користувача на етапі реалізації. Нерідко саме розробники підіймають питання етики, коли їм доручають реалізувати потенційно шкідливу функцію, адже вони ближче бачать практичні наслідки таких рішень.

Системний інженер, працюючи на макро-рівні, опікується ширшою картиною: загальною інфраструктурою та архітектурою. Його рішення менш помітні пересічному користувачу, але саме вони визначають фундаментальні властивості системи, від яких залежить благополуччя багатьох. Етичні виклики системного інженера – це питання стратегічних компромісів: чи достатньо система безпечна, щоб випустити її на ринок (наприклад, новий авіаційний софт або авто-пілот)? скільки рівнів резервування закласти (безпека vs. вартість)? які стандарти і регуляції врахувати і чи можна собі дозволити їх спростити?

Системний інженер мусить координувати роботу різних команд, тому його етична роль – часто арбітр між різними вимогами: комерційними, технічними, правовими. Наприклад, менеджмент може тиснути скоротити час на тестування, але інженер розуміє, що недостатньо протестована система – це ризик для людей; його етичний обов'язок – наполягти на необхідних перевірках, навіть якщо це непопулярно. Інший приклад: у дизайні системи інженер має врахувати екологічні наслідки (скажімо, енергоефективність дата-центрів) або питання довготривалої підтримки (щоб система через кілька років не стала небезпечно застарілою). Отже, відповідальність системного інженера більш пов'язана з гарантією загальної цілісності та надійності великого продукту. Якщо розробник дбає про окремий додаток, то системний інженер – про екосистему в цілому.

Ще одна відмінність – часова та процесна перспектива. Розробник ПЗ часто працює в рамках ітеративних циклів розробки, зосереджений на поточних задачах і швидких релізах. Етичні рішення приймаються тут і зараз (наприклад, як реалізувати фічу у цьому спринті). Натомість системний інженер відповідає за повний життєвий цикл системи: від концепції до виводу з експлуатації. Він мусить думати на роки вперед. Відповідно, етика системного інженера включає довгострокову відповідальність: не тільки запустити систему, а й гарантувати можливість її безпечного супроводу, оновлення, а також етичного зняття з експлуатації (наприклад, збереження або знищення даних після закриття проекту).

Незважаючи на ці відмінності, обидві ролі мають працювати в тандемі задля створення етично стійких технологій. Розробник і системний інженер доповнюють один одного: перший глибоко розуміє деталі реалізації і може вчасно сигналізувати про етичні проблеми на рівні функцій, другий – бачить загальну картину і встановлює етичні «рамки» проекту (політики, стандарти). У найкращому випадку в команді панує культура етичного обговорення, коли будь-хто – від рядового девелопера до головного інженера – може підняти питання моральності того чи іншого технічного рішення, і це буде почуто. Так, розробник може звернути увагу, що нова фіча порушує приватність, а системний інженер – підтримати його, змінивши вимоги до системи відповідно до етичних

принципів. Обидві ролі пов’язані спільною метою – створювати технології, що служать людям, а не шкодять їм. Етика в IT – це командна гра, де кожен відповідає за свій спектр питань, але успіх визначається узгодженістю дій.

3.5 Кейс-аналіз 2 практичних ситуацій: етичне рішення у команді та проєкті

Розглянемо два реальні або уявні сценарії, що демонструють етичні виклики на практиці:

– випадок 1 стосується морального вибору всередині команди розробки, коли інженери стикаються з неетичним завданням від керівництва;

– випадок 2 показує ситуацію на рівні великого інженерного проєкту, де рішення (або їх відсутність) призвели до серйозних наслідків, висвітлюючи важливість етики системної інженерії.

Випадок 1. Прихований збір даних у продукті та реакція команди.

Ситуація. Команда розробників працює над мобільним застосунком-фільтром для обробки фотографій. Продукт безкоштовний, і керівництво компанії шукає способи монетизації. Маркетинговий директор ставить завдання: вбудувати в застосунок прихований модуль, який збиратиме персональні дані користувачів (контакти, геолокацію, уподобання) без явного повідомлення, щоб потім ця інформація використовувалась для реклами або продавалася партнерам. Іншими словами, пропонується приховано перетворити користувачів на «продукт» для третьої сторони. Офіційно про цю функцію не буде згадки в політиці конфіденційності (сподіваються, що користувачі не помітять), або ж її замаскують під збір анонімної статистики. Один із розробників, отримавши таке технічне завдання, стурбований: це суперечить його особистим принципам та професійній етиці. Він пам’ятає, що прихований збір персональної інформації без дозволу користувача – пряме порушення етичних норм. В команді починається обговорення: частина інженерів теж не згодна з таким підходом, інші ж пропонують «не втручатися», бо рішення приймає керівництво, та й компанія так робить не вперше.

Етична проблема. Даний сценарій порушує принцип прозорості та приватності. Користувачі довіряють застосунку обробку своїх фото, а натомість «за їхньою спиною» буде зібрано інші дані, які їх ніяк не стосуються. Це обман і зловживання довірою. З точки зору професійних етичних кодексів, розробник зобов'язаний захищати конфіденційність даних користувача і не використовувати їх не за призначенням без згоди. Прихований модуль, по суті, є прихованою функцією (з попереднього розділу) і є неетичним. Більше того, такий збір може бути незаконним (порушення політики конфіденційності, законів на кшталт GDPR), тобто розробникам пропонують долучитися і до потенційно протиправної дії. Також постає питання особистої моральної відповідальності: чи можуть інженери прикриватися тим, що «це рішення бізнесу, ми лише код пишемо»? Згідно з принципами етики, особистісний моральний вибір розробника нікуди не зникає, навіть якщо наказ надійшов зверху – кожен професіонал відповідальний за свій внесок. Таким чином, команда стикається з дилемою лояльності: лояльність до працедавця vs. лояльність до етичних норм і користувача.

Рішення і наслідки. Оптимальний етичний крок для команди – відкрита дискусія з керівництвом, наведення аргументів проти прихованого збору даних. Розробники можуть спробувати переконати бізнес-сторону у ризиках: по-перше, репутаційних (якщо обман випливе, застосунок втратить користувачів, а компанія – добро ім'я), по-друге, юридичних (штрафи та санкції), і найголовніше – моральних (так робити просто недобре по відношенню до людей). Альтернативою може бути пошук прозорих моделей монетизації: наприклад, зробити платну преміум-версію або показувати рекламу, але чесно, з відома користувача. Якщо керівництво йти назустріч відмовляється і наполягає, перед розробниками постає складний вибір: або підкоритися і реалізувати сумнівний модуль, або відмовитися брати участь (аж до звільнення чи переведення на інший проект). У випадках, коли йдеться про кричуще порушення етики чи закону, найбільш морально виправдано відмовитися від виконання такого завдання. В історії ІТ є приклади, коли інженери звільнялися на знак протесту проти неетичних проектів (наприклад, працівники Google відмовлялися працювати над

військовими технологіями, що вважали неетичними). Тут кожен член команди має зважити особисті цінності. Наш герой-розробник може спробувати заручитися підтримкою колег: якщо вся команда одностайно скаже «ні», керівництво, ймовірно, змушене буде переглянути план. І навіть якщо ні – то масова відмова або звільнення теж подасть сигнал, що такі методи неприйнятні.

Кінцівка сценарію (припустимо). Розробник висловлює свої заперечення на внутрішньому обговоренні. Його підтримують кілька ключових колег, які теж не хочуть втрачати репутацію. Разом вони готують звернення до менеджменту, наводячи аргументи. На щастя, СТО компанії дослухається: прихований трекер скасовують. Натомість вирішують впровадити опційний збір даних: при встановленні нової версії додатку користувачам буде показано діалог із проханням дозволити збирати анонімні дані для поліпшення сервісу. Хоч, можливо, відгукнеться менше користувачів, зате це прозора згода. Таким чином, команда досягає компромісу, що узгоджується з етикою. Цей випадок демонструє, що етичне лідерство може йти «знизу» – від самих інженерів. Відмова реалізувати неетичну функцію – нелегкий крок, але він абсолютно виправданий з моральної точки зору і в довгостроковій перспективі вигідний і користувачам, і самій компанії, яка уникне скандалу.

Випадок 2. Наслідки етичних прорахунків у проектуванні авіаційної системи (уроки Boeing 737 MAX).

Ситуація. Велика інженерна команда працювала над модернізацією пасажирського літака Boeing 737 MAX. Це був масштабний проект системної інженерії, що охоплював і апаратні зміни (нові двигуни), і програмне забезпечення керування польотом. Через конструктивні особливості оновлених двигунів літак мав тенденцію задирати ніс вгору під час зльоту, що могло призвести до зриву потоку (звалювання). Рішенням було розробити програмну систему MCAS (Maneuvering Characteristics Augmentation System), яка автоматично опускала ніс літака, якщо датчики (кутові сенсори атаки, AOA) фіксували небезпечний підйом носа. На етапі проектування було прийнято кілька спірних рішень. По-перше, систему MCAS зробили залежною лише від одного датчика AOA замість двох, хоча літак мав два сенсори (один ліворуч, інший

праворуч). Це означало, що якщо єдиний активний датчик помилиться, MCAS може спрацьовувати хибно. По-друге, аби новий літак сертифікувався як варіант попередньої моделі (737 NG) і пілотам не довелося проходити дорогий тривалий тренінг, інженери не проінформували належним чином пілотів про наявність MCAS та її особливості [12]. Система працювала приховано, без індикації в кабіні (сигналізація про розбіжність даних двох AOA була лише опцією, якої не було в літаках, що розбилися). Ці рішення приймалися під тиском конкурентної гонки (Boeing поспішав випустити нову модель раніше за конкурента Airbus) і з метою зниження витрат на сертифікацію. Протягом експлуатації 737 MAX сталося дві катастрофи (рейси Lion Air 610 та Ethiopian Airlines 302 у 2018-2019 рр.), в яких загинуло 346 людей. Розслідування показали, що некоректна робота MCAS (через збій єдиного датчика) стала ключовим фактором аварій – система настійливо спрямовувала носи літаків донизу через помилкові дані, а пілоти не були підготовлені швидко розпізнати і нейтралізувати цю автоматичну функцію.

Етичні проблеми. Цей випадок являє собою комплексний провал етики системного проектування і інженерного менеджменту. Перша проблема – пріоритет швидкості та вигоди над безпекою. Рішення використовувати один сенсор замість двох суперечить фундаментальному принципу безпечних систем: відмовостійкість через резервування. В авіації зазвичай критичні датчики дублюються або навіть будуються з потрійним резервом, щоб одна несправність не спричинила катастрофу. Тут же інженери (або керівники, що тиснули на інженерів) знехтували цим принципом. Можливо, вони розраховували, що ймовірність збою мала, або хотіли здешевити систему – але з етичної точки зору, кожна зайва частка ризику для життя пасажирів мусила бути виправдана дуже вагомими причинами, яких не було. Друга проблема – бракувала прозорість і повнота інформації. Приховування від пілотів деталей про нову автоматичну систему заради простішої сертифікації є неетичним обманом як щодо пілотів, так і регуляторів. Пілоти мають право знати, з якими алгоритмами вони взаємодіють, адже в критичний момент це знання – питання життя і смерті. Boeing позбавив їх цієї можливості, вважаючи, що «літак достатньо схожий на попередній». Це схоже на приховану функцію на системному рівні: MCAS працювала фоново, і

екіпажі були не готові до її агресивного втручання. Третя етична проблема – відповідальність та культура всередині організації. Після першої аварії компанія схильна була звинуватити «помилки пілотів» та не визнала одразу недоліки дизайну [12]. Така реакція свідчить про небажання брати відповідальність, що теж етично хибно. Натомість етичним було б одразу приземлити парк 737 MAX, детально розібрати проблеми, інформувати спільноту і виправити систему – можливо, тоді друга трагедія не сталася б.

Аналіз рішень та уроки. З позиції етики системної інженерії, кожне критичне інженерне рішення повинно проходити «етичну перевірку»: чи не створює воно неприпустимий ризик? чи не ставить комерційний інтерес вище безпеки людей? У випадку з MCAS, інженери мали настояти на використанні двох (або більше) сенсорів для алгоритму – навіть якщо це складніше. Якщо ж рішення приймали не вони, а менеджмент, то технічні фахівці повинні були підняти червоний прапорець і чітко попередити про можливі наслідки. Відомо, що окремі інженери Boeing висловлювали занепокоєння, але, здається, їхня думка не отримала достатньої ваги у компанії [13]. Це вказує на проблему корпоративної культури: етичний голос інженерів був приглушений бізнес-пріоритетами. Щоб уникнути такого в майбутньому, у великих організаціях впроваджують незалежні інженерні ради з безпеки, механізми анонімного повідомлення про проблеми, заохочують атмосферу, де інженер може заперечити керівнику, якщо бачить загрозу. Другий урок – прозорість і навчання. Безпека авіації побудована на довірі та співпраці між виробником, пілотами і регуляторами. Приховання інформації руйнує цю довіру. Після цих катастроф Boeing довелося докорінно переглянути свої підходи: оновлений MCAS тепер отримує дані з двох датчиків, в кабіні додали індикатор несправності сенсорів, а для пілотів ввели обов’язковий тренаж щодо нової системи. Ці дії – запізніле, але необхідне відновлення етичних норм: повернення до пріоритету безпеки та інформованості.

Висновок кейсу. Трагедія 737 MAX яскраво продемонструвала, що етичні рішення в інженерії – не абстракція, а питання життя. Ціна помилки або свідомого компромісу може бути катастрофічною. Системні інженери повинні

мати сміливість і підтримку ставити незручні питання: «А що якщо цей датчик вийде з ладу? Чи безпечно залишати це на розсуд алгоритму? Чи знають користувачі (пілоти) достатньо про нову функцію?» Якщо відповідь негативна, етика диктує *не приймати* такий дизайн. Кейс Boeing 737 MAX увійшов у підручники з інженерної етики як приклад того, як технічна досконалість без етичної зрілості може призвести до провалу. Він спонукав до реформ: посилення регуляторів, перегляд процесів сертифікації, а головне – до усвідомлення, що інженери несуть особисту відповідальність перед суспільством і мусять відстоювати безпеку навіть під тиском корпорацій. Для кожного системного інженера цей випадок – нагадування про його професійний обов'язок: *«краще затримати випуск або збільшити витрати, ніж запустити систему, яка може нашкодити людям»*.

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

Мета – сформувати у здобувачів освіти цілісне уявлення про етичні засади професійної діяльності фахівців з кібербезпеки, розкрити особливості їхньої відповідальності в умовах роботи з критичною інформацією, ознайомити з правовими обмеженнями та типовими моральними дилемами, що виникають у сфері цифрової безпеки. Лекція спрямована на розвиток етичної свідомості, здатності до прийняття зважених рішень та дотримання високих стандартів професійної поведінки в умовах ризиків, пов’язаних із кіберзагрозами.

4.1 Професійна відповідальність фахівця з кібербезпеки

У сфері цифрової безпеки фахівець з кібербезпеки відіграє критично важливу роль, адже саме від нього залежить стабільність інформаційних систем, збереження конфіденційних даних і запобігання порушенням цифрових прав людини. Професійна відповідальність у цій галузі має багатовимірний характер – вона охоплює як технічні, так і правові, етичні та соціальні аспекти.

Насамперед, фахівець з кібербезпеки має високий рівень доступу до систем – часто це root-доступи, адміністративні облікові записи, доступ до внутрішніх журналів, логів, поштових серверів, баз даних із персональними або фінансовими записами. Такий рівень контролю вимагає особливої обережності, відповідальності та доброчесності. Будь-яка дія фахівця, навіть на перший погляд технічно нейтральна, може мати серйозні етичні або юридичні наслідки.

Особливо важливим є дотримання принципу «діяти лише в межах необхідного». У міжнародній практиці це правило фіксується як *principle of least privilege* або *need-to-know*. Це означає, що фахівець має право використовувати лише ті ресурси, до яких йому надали доступ для виконання конкретного завдання, і не більше. Самостійна ініціатива перевірити сторонню систему,

протестувати чутливий вузол або переглянути несанкціоновані дані (навіть «заради безпеки») є порушенням професійної етики.

Ще один важливий аспект – відповідальність за наслідки технічних рішень. Спеціаліст з кібербезпеки повинен усвідомлювати, що його помилки чи недбалість можуть призвести до витоку даних, блокування критичних процесів, фінансових втрат, а в окремих випадках – навіть до порушення життєво важливих сервісів (наприклад, у лікарнях чи транспортних системах). Відповідальність охоплює не лише навмисні дії, а й бездіяльність: якщо фахівець не реагує на виявлену вразливість або відмовляється інформувати керівництво про ризики, він також порушує етичні стандарти.

Професійна відповідальність також включає збереження конфіденційності. Це стосується не лише особистих даних користувачів, а й внутрішньої інформації про інфраструктуру, протоколи, конфігурації безпеки тощо. Витік такої інформації, навіть ненавмисний (наприклад, через розміщення скриншоту в соціальних мережах), може призвести до серйозних наслідків. Фахівець має усвідомлювати, що кожна дія, пов’язана з інформаційними системами, має проходити через призму ризику та наслідків.

Особливим елементом професійної відповідальності є зобов’язання не шкодити. Це означає не лише уникнення зловживань, а й активне сприяння безпеці – своєчасне оновлення систем, перевірка логів, участь у створенні політик безпеки, консультування працівників щодо цифрової гігієни. Також важливо пам’ятати про відповідальність перед суспільством: фахівець із кібербезпеки має діяти не лише в інтересах своєї організації, а й із урахуванням загальнолюдських етичних цінностей, прав людини та цифрової свободи.

4.2 Етичні ризики, пов’язані з доступом до критичної інформації

Професійна діяльність спеціалістів з кібербезпеки передбачає роботу з критично важливими інформаційними ресурсами, які зазвичай недоступні іншим категоріям працівників. Йдеться про адміністраторські облікові записи, конфігурації мережевого захисту, шифрувальні ключі, лог-файли, журнали

автентифікації, а також великі масиви персональних даних. Цей рівень доступу робить фахівця не лише технічно спроможним впливати на цілі системи, але й морально вразливим – адже саме в його руках зосереджено потенціал як для захисту, так і для зловживання.

Одним із головних етичних викликів у таких умовах є тонка межа між необхідною дією та надмірною ініціативою. Наприклад, виявлення спірного вмісту в корпоративній переписці або аномального трафіку користувача не завжди потребує негайної реакції – без санкції відповідальної особи це може порушити принцип законності та етичної виваженості. Навіть короткочасне ознайомлення з особистими файлами або службовими документами, які не мають прямого стосунку до поставленого завдання, є прикладом неетичної поведінки, що хоч і не завжди є злочином, проте підриває довіру до фахівця.

Етичні ризики в діяльності фахівця з кібербезпеки значною мірою залежать від рівня і типу доступу, який він має до інформаційних систем. Різні категорії доступу – адміністративний, мережевий та до даних – передбачають різну ступінь відповідальності та потенційну загрозу зловживання. Матриця, на рисунку 4.1, демонструє ключові типи доступу та пов’язані з ними етичні ризики. Такий підхід дозволяє структурувати уявлення про професійні загрози з точки зору моральної відповідальності та сформувати внутрішні обмеження у роботі з критичними системами.

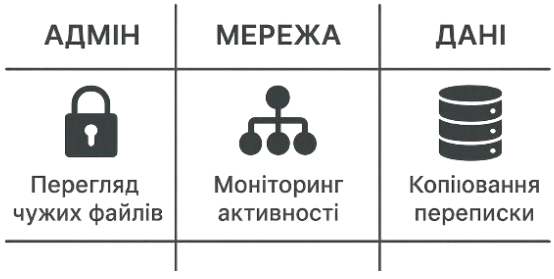

Рисунок 4.1 – Матриця етичних ризиків залежно від типу доступу

В етиці кібербезпеки одним із базових є принцип «need to know» – знати лише те, що необхідно для виконання своїх обов’язків. Порушення цього принципу – навіть із «цікавості» – розцінюється як порушення професійної

доброчесності. Особливо ризикованими є ситуації, коли спеціаліст має повний доступ до:

– адміністративних облікових записів, які дозволяють змінювати системні параметри, видаляти або копіювати дані;

– механізмів автентифікації, включаючи бази паролів, токенів або біометричних шаблонів;

– особистих даних користувачів, зокрема фінансових звітів, електронної пошти, історії дій у системі.

Наявність такого доступу сама по собі є джерелом постійної етичної напруги. Неетичне поводження в цій сфері проявляється не лише у випадках навмисного злому або витоку інформації, а й у дрібних, але системних порушеннях: наприклад, перегляд пошти колеги без дозволу, створення обхідних акаунтів, використання робочого ресурсу для несанкціонованого моніторингу активності інших користувачів.

Також слід враховувати, що не всі зловживання одразу є кримінально караними. Наприклад, перегляд внутрішньої переписки чи копіювання логів з цікавості – це не завжди правопорушення згідно з законом, але така поведінка може призвести до втрати довіри з боку роботодавця, юридичних санкцій згідно з внутрішніми політиками, а також шкоди репутації фахівця. У цьому контексті етика відіграє роль першого запобіжника – вона випереджає юридичну реакцію, формуючи культуру саморегуляції.

Крім того, фахівець із кібербезпеки мусить постійно перебувати у стані професійного самоконтролю, навіть за умов слабкого зовнішнього нагляду. Саме тому внутрішня етична зрілість вважається не менш важливою за технічні навички. Добропорядність, стриманість, відмова від непотрібного доступу або «цікавості» – це не прояви обмеження, а ознаки професійної етики в умовах високих ризиків.

4.3 Правові обмеження в діяльності фахівця з кібербезпеки

Професійна діяльність спеціалістів з кібербезпеки регламентується як внутрішнім національним законодавством, так і нормами міжнародного права. Це зумовлено високими ризиками несанкціонованого доступу, обробки персональних даних, вторгнення в системи та порушення конфіденційності. Водночас етична складова безпосередньо взаємодіє з правовою: дотримання букви закону не завжди гарантує відповідальну поведінку, і навпаки – етичні наміри не звільняють фахівця від юридичної відповідальності.

В Україні основними нормативно-правовими актами, що регламентують діяльність у сфері кібербезпеки, є:

– Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» №80/94-ВР – встановлює вимоги до захисту інформації та відповідальність за порушення режиму доступу [14].

– Закон України «Про інформацію», а також «Про захист персональних даних» – визначають правовий режим обробки даних та умови доступу до них [15; 16].

– Кримінальний кодекс України – містить статті 361-363¹:

1) ст. 361: «Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів)»;

2) ст. 362: «Несанкціоновані дії з інформацією»;

3) ст. 363: «Порушення правил експлуатації ЕОМ»;

4) ст. 363¹: «Створення з метою використання, розповсюдження або збуту шкідливого ПЗ» [17].

На практиці це означає, що фахівець з кібербезпеки не має права самостійно здійснювати тестування системи або виявляти її вразливості без чіткого погодження з власником ІТ-інфраструктури. Навіть якщо дії мали «доброзичливий» характер, вони можуть бути кваліфіковані як несанкціоноване втручання, що тягне за собою кримінальну відповідальність.

Фахівці, що працюють із закордонними сервісами або в транснаціональних компаніях, повинні враховувати вимоги міжнародного регулювання, зокрема:

– Будапештська конвенція про кіберзлочинність (2001) – перший міжнародний договір, який визначає злочини в кіберпросторі та процедури розслідування. Україна ратифікувала конвенцію у 2005 році. Вона передбачає обов'язковість санкцій для доступу до інформаційних систем, а також передбачає можливість кримінальної відповідальності навіть за намір отримати несанкціонований доступ [18].

– Загальний регламент захисту даних (GDPR) Європейського Союзу – один із найжорсткіших регуляторів у світі щодо обробки персональних даних. Стаття 32 регламенту вимагає від організацій здійснювати технічні і організаційні заходи для забезпечення безпеки обробки даних, однак усі дії мають бути належним чином документовані та погоджені [19].

– ISO/IEC 27001:2022 – міжнародний стандарт управління інформаційною безпекою, який, хоча і не є юридично обов'язковим, часто вимагається в рамках контрактів або сертифікації. Він вимагає запровадження політик контролю доступу, реєстрації подій, перевірки правомірності дій адміністраторів та кіберфахівців [3].

У таблиці 4.1 систематизовано найпоширеніші дії кіберфахівців, відповідні їм правові обмеження та етичну оцінку. Такий підхід дозволяє краще зрозуміти межі допустимого, розвивати етичну чутливість і приймати зважені рішення в умовах професійної відповідальності.

Особливу етично-правову складність становлять так звані «сірі» тестування, коли фахівцю доручають здійснити тест без відома співробітників або навіть системних адміністраторів. Такі тести (Red Team або Black Box) дозволяють оцінити ефективність реального захисту, але повинні бути чітко обґрунтовані документально, з визначенням:

- чітких меж тестування;
- осіб, відповідальних за результати;
- способів зберігання та захисту зібраних даних;
- протоколів інформування після завершення.

Таблиця 4.1 – Аналіз дій фахівця з кібербезпеки: правові межі та етична оцінка

Дії фахівця з кібербезпеки	Правова межа	Етична оцінка
доступ до пошти користувача без згоди	порушення ст. 32 Конституції України та законів про персональні дані	недопустимо – втручання у приватне життя
передача звіту з уразливістю третій стороні без згоди замовника	порушення NDA або GDPR (якщо персональні/комерційні дані)	недопустимо – навіть з благих намірів, порушує конфіденційність
збір відкритих даних про співробітників компанії (OSINT)	допустимо за умови, що джерела дійсно публічні та не порушують інші права	допустимо, якщо не переходить межу втручання або дискредитації

Відсутність цих умов робить таке тестування неетичним і вразливим до юридичних наслідків. Більше того, колізія з законодавством країни, на території якої розміщені сервери, може поставити фахівця під загрозу кримінального переслідування (наприклад, у Франції, Німеччині, Сингапурі діють суворі режими доступу до обчислювальних систем, навіть у навчальних цілях).

4.4 Моральні дилеми: етичне хакерство, атаки для тестування, перевірка співробітників

У сфері кібербезпеки фахівці щодня стикаються з ситуаціями, що не мають однозначної відповіді з погляду моралі. Ці ситуації, які отримали назву моральних дилем, часто виникають на перетині добрих намірів, технічних можливостей і правових обмежень. На відміну від чітко врегульованих норм, дилеми – це випадки, коли дія є або законною, але потенційно неетичною, або навпаки – етично виправданою, але суперечить формальним процедурам чи інтересам сторін. У таких випадках фахівець повинен керуватися внутрішнім професійним етичним компасом, нормами корпоративної культури та принципами прозорості.

Етичне хакерство (white hat)

Однією з найпоширеніших дилем є етичне хакерство, коли фахівець (внутрішній або зовнішній) виявляє вразливість в інформаційній системі без попереднього дозволу. Постає питання: чи повідомляти про вразливість власника системи, якщо вона несанкціоновано виявлена? Що робити, якщо власником є держава або організація з сумнівною репутацією щодо прав людини?

Міжнародна практика пропонує принцип Responsible Disclosure (відповідальне розкриття), згідно з яким етичний хакер повинен конфіденційно повідомити власника системи, надати час на усунення проблеми, а лише потім – за згодою – оприлюднити інформацію. Однак така практика не є універсальною. У деяких юрисдикціях навіть доброзичливе хакерство прирівнюється до злочину (якщо не було формального дозволу), що ставить фахівця в етичний глухий кут: замовчування – небезпека для користувачів, розкриття – можливі санкції або кримінальне переслідування.

Атаки з дозволу (red teaming)

Red teaming – це метод тестування, що імітує дії зловмисника для виявлення вразливостей до реальних атак. Формально такі дії дозволені й навіть рекомендовані стандартами (зокрема, ISO/IEC 27002), однак з етичної точки зору виникає ряд запитань.

Чи повинні бути повідомлені інші працівники (зокрема служба безпеки, технічна підтримка), що атака є симуляцією? Чи допустимі фішингові листи до співробітників із метою перевірки їхньої обачності? А якщо внаслідок такої симуляції працівник помиляється і його карають – чи справедливо це? Відповідь полягає в етичному дизайні симуляції: атака повинна мати чіткі межі, відповідального за наслідки, а також правила аналізу результатів без дискредитації окремих працівників.

Інсайдерське тестування та перевірка співробітників

Ще одна складна ситуація – навмисна перевірка працівників на “стійкість” до маніпуляцій чи помилок. Наприклад, фахівець з безпеки імітує фішинговий лист або просить колегу передати логін/пароль під виглядом адміністратора.

Навіть якщо така дія попередньо погоджена керівництвом, вона створює етичну напругу – між потребою перевірки та збереженням довіри в колективі.

Особливо критичними є ситуації, коли такі перевірки не супроводжуються інформованою згодою, або коли результати використовуються для публічного осуду, а не навчання. Це може зруйнувати психологічну безпеку в команді та спричинити професійне вигорання. Вихід – впровадження етичних політик тестування, де чітко регламентується мета, масштаб, обробка результатів та права працівників.

Збір відкритих (але чутливих) даних

Поширеною практикою є OSINT – збирання даних з відкритих джерел (форумів, соцмереж, публічних баз). У сфері кіберзахисту це використовується для оцінки ризиків (наприклад, чи публікує співробітник конфіденційні фото з офісу). Проте постає запитання: чи етично аналізувати особисте життя працівника або клієнта на підставі відкритої інформації?

З формальної точки зору – це дозволено. Але з етичної – має значення мета збору, форма зберігання, обсяг даних і спосіб повідомлення. Якщо дані збираються з прицілом на дисциплінарний вплив або контроль, це може вважатися втручанням у приватність. Більш етичним є використання OSINT у рамках навчання, прогнозування загроз або консультування, але з дотриманням принципу пропорційності.

Ключовими критеріями для етичних засад оцінки таких ситуацій є:

- інформована згода (explicit or implicit);
- прозорість дій та цілей (transparency);
- повага до гідності та приватності;
- відсутність завдання шкоди особі чи організації.

Етична поведінка фахівця з кібербезпеки вимагає не лише уникнення порушень, а й активного аналізу наслідків своїх дій. Добрі наміри не звільняють від відповідальності за морально сумнівні рішення. В умовах зростаючої цифрової взаємозалежності саме етична зрілість визначає, чи зможе спеціаліст діяти на користь суспільства, не виходячи за межі дозволеного.

4.5 Case-study: етичні аспекти тестових атак, використання вразливостей

Практичні кейси в сфері кібербезпеки демонструють, що навіть добре підготовлені фахівці можуть опинитися в ситуаціях, коли юридично правильне рішення не завжди збігається з етично прийнятним, і навпаки. Нижче розглянуто два реальні сценарії, що ілюструють моральну напругу під час роботи з вразливостями – як у межах санкціонованих тестів, так і поза ними.

Випадок 1. PenTest в межах компанії, публікація вразливості у Twitter.

Ситуація: під час внутрішнього тестування безпеки CRM-системи компанії фахівець з кібербезпеки виявляє вразливість, що дозволяє отримати доступ до платіжних реквізитів клієнтів. Він формує звіт із детальним описом проблеми, однак керівництво компанії реагує критично: відкидає серйозність ризику та просить обмежити опис проблеми в офіційній документації. Обурений байдужістю, фахівець вирішує оприлюднити деталі вразливості у Twitter.

Етична оцінка: попри щирі наміри захистити користувачів, самовільне публічне розкриття вразливості без згоди власника системи є грубим порушенням професійної етики. Така дія:

- компрометує систему без належного виправлення;
- може завдати шкоди клієнтам (витік даних, шахрайство);
- підриває довіру до спеціаліста як до конфіденційного партнера.

Правильна стратегія передбачає використання процедур Responsible Disclosure – конфіденційного повідомлення вразливості з фіксацією дати, способу інформування, і лише після спливу розумного терміну (30-90 днів) – публікація в обмеженій формі (якщо проблему не усунули). У багатьох компаніях існують спеціальні політики Bug Bounty або приватні канали розслідувань, якими слід користуватись.

Висновок: добрі наміри не звільняють від відповідальності. Професійна етика вимагає збереження конфіденційності, захисту користувача та дотримання узгоджених каналів комунікації.

Випадок 2: Виявлення вразливості під час навчального хакатону

Ситуація: учасник студентського хакатону, що проходить у відкритому середовищі, під час дослідження виявляє відкритий порт (наприклад, 8080), який веде до адміністративної панелі веб-сайту партнера заходу. Жодних обмежень у мережі немає, і доступ не захищений паролем. Виникає спокуса перевірити, наскільки глибоким є рівень вразливості – можливо, навіть увійти в систему.

Етична оцінка: навіть якщо ресурси доступні публічно, етично неприпустимо виконувати будь-які дії в межах сторонньої системи без дозволу. Навіть базове сканування, якщо воно не передбачене умовами заходу, може вважатися несанкціонованим втручанням. У цьому випадку учасник має:

- зупинитися після виявлення відкритого порту;
- зафіксувати технічну інформацію (IP, сервіс, порт);
- повідомити відповідальних осіб (організаторів або представників компанії).

Такі ситуації також демонструють межу між навчальною допитливістю і відповідальністю. Організатори заходів мають пояснювати учасникам межі дозволеного, а учасники – розвивати самоконтроль.

Висновок: навіть у неформальних умовах кіберетика вимагає поваги до цифрової власності та принципу недоторканості систем. Виявлення – допустиме, втручання – неприпустиме без офіційного дозволу.

ЛЕКЦІЯ 5
КОНФІДЕНЦІЙНІСТЬ, ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ТА ЦИФРОВА ПРИВАТНІСТЬ

Мета – сформувати у здобувачів освіти комплексне розуміння сучасних концепцій конфіденційності, цифрової приватності та захисту персональних даних в умовах цифрової трансформації суспільства; ознайомити з ключовими правовими актами (GDPR, Закон України №2297-VI), технологіями приватності (шифрування, VPN, ZKP, PIMS), проблемами інформованої згоди та викликами для конфіденційності у середовищі Big Data, IoT і соціальних мереж; розвинути етичну чутливість до балансу між безпекою, зручністю та правами людини у цифровому просторі.

5.1 Значення приватності в цифрову епоху

Збір, обробка та поширення персональної інформації відбувається постійно – у соціальних мережах, банківських системах, електронній комерції, охороні здоров'я, в освітньому та державному секторах. У цьому контексті цифрова приватність (англ. *digital privacy*) перетворилася з особистої потреби на один із ключових принципів цифрової демократії, довіри до технологій та кібербезпеки.

Водночас розвиток великих даних (*Big Data*), штучного інтелекту, Інтернету речей (IoT) та хмарних сервісів створює нові виклики, адже збір даних став невидимим, масовим та потенційно неконтрольованим. Багато користувачів не усвідомлюють обсяг інформації, яку вони залишають у цифровому просторі, а також не мають реального контролю над її використанням. Саме тому конфіденційність в умовах цифровізації вимагає не лише технологічних рішень, а й етичних норм, правового регулювання та просвітницької роботи.

Цифрова приватність – це не просто технічне питання контролю над даними, а базова умова особистої автономії, гідності, інформаційної безпеки та цифрового суверенітету особистості.

На відміну від традиційного уявлення про конфіденційність як про обмежений доступ до приватного листування або медичних даних, сьогодні мова йде про всеохопний цифровий слід, який залишає кожен користувач: історія пошуку, геолокація, уподобання, реакції в соціальних мережах, біометричні дані, поведінкові патерни. У багатьох випадках збір цих даних відбувається без активної згоди або навіть усвідомлення з боку користувача, що створює асиметрію між провайдерами цифрових послуг і тими, хто ними користується.

Ключовим викликом цифрової епохи є те, що приватність стає технічно вразливою і юридично розмито регульованою, а отже – часто нехтуваною. Багато цифрових платформ будують бізнес-моделі на монетизації персональних даних, що створює конфлікт між економічною вигодою та етичними стандартами.

Цифрова приватність також має критичне значення в політичному контексті. Доказом цього є численні скандали з витоками даних, як-от справа Cambridge Analytica, яка продемонструвала, що неетичне використання особистої інформації може впливати на демократичні процеси [20]. Таким чином, захист цифрової приватності – це не лише гарантія недоторканості особистого життя, а й елемент національної безпеки, соціальної стабільності та верховенства права.

У науковому та правовому дискурсі приватність дедалі частіше розглядається як цифрове право людини, співвідносне з правом на свободу вираження поглядів, вільне пересування, недоторканність житла. Зокрема, Європейський Суд з прав людини (ЄСПЛ) неодноразово підтверджував, що цифрове життя входить до сфери захисту ст. 8 Конвенції про права людини [21].

Таким чином, значення приватності у XXI столітті виходить далеко за межі технічної категорії або юридичної вимоги. Це – системоутворюючий принцип, що формує довіру до технологій, стабільність цифрового громадянства та можливість людини залишатися суб’єктом, а не об’єктом інформаційної екосистеми.

5.2 Концепція конфіденційності: філософія, еволюція, принципи

У цифрову епоху поняття конфіденційності набуло особливого значення як фундаментальне право особи на контроль над власною інформацією. Це право охоплює не лише захист персональних даних від несанкціонованого доступу, а й можливість самостійно визначати, яка інформація про себе буде зібрана, ким, коли та з якою метою. Конфіденційність тісно пов'язана з такими філософськими категоріями, як автономія, людська гідність, право на приватність та інформаційний самовизначення.

Вперше правове формулювання конфіденційності з'явилося ще в кінці XIX століття. У США 1890 року відома юридична публікація Воррена і Брендайса визначила право на приватність як «the right to be let alone» [22]. Це було реакцією на розвиток фотожурналістики та масової преси, які порушували межі особистого життя. Згодом ця ідея була розширена до права на контроль над особистою інформацією.

У європейському контексті після Другої світової війни конфіденційність увійшла до системи фундаментальних прав людини. Вона була закріплена у ст. 8 Конвенції про захист прав людини і основоположних свобод Ради Європи, яка гарантує право кожної особи на повагу до приватного і сімейного життя, житла та кореспонденції [23]. Цей підхід пізніше ліг в основу рішень Європейського суду з прав людини щодо цифрової приватності.

Також право на конфіденційність закріплено в статті 17 Загальної декларації прав людини (1948), що визнає право кожного на захист від свавільного втручання в особисте життя, сім'ю, житло або кореспонденцію, а також від посягання на честь і репутацію [24].

З розвитком інформаційних технологій конфіденційність набула нового функціонального значення. У цифровому середовищі особистість представлена не лише як біологічна або соціальна сутність, а як інформаційна структура – сукупність даних, записів, цифрового сліду, поведінкових моделей. Це призвело до появи концепції «інформаційної приватності» (*informational privacy*), яка

визнає право особи на інформаційний контроль – тобто здатність вирішувати, хто і як буде використовувати її персональні дані.

У відповідь на ці виклики в міжнародному праві та національних законодавствах сформувався звід принципів обробки персональних даних, який уніфікує практики роботи з інформацією. Найвідомішим є перелік із 10 принципів, що лежить в основі таких документів, як GDPR [25] та стандартів OECP щодо захисту приватності та транскордонних потоків персональних даних [26]:

–законність, справедливість і прозорість – дані мають оброблятися на законній підставі, відкрито для суб'єкта;

–цільова обмеженість (*purpose limitation*) – збір даних дозволений лише для конкретних, чітко визначених цілей;

–мінімізація обсягу – збираються лише ті дані, які дійсно необхідні;

–точність – дані повинні бути актуальними та точними;

–обмеження зберігання – дані не повинні зберігатися довше, ніж потрібно;

–цілісність і конфіденційність – дані повинні бути захищені від несанкціонованого доступу або втрати;

–підзвітність (accountability) – організації зобов'язані документувати свою відповідність принципам захисту;

–права суб'єкта даних – включно з правом на доступ, виправлення, обмеження, забуття;

–інформована згода – збір і обробка даних потребує добровільної, конкретної та свідомої згоди;

–оцінка ризиків – впровадження процедур оцінювання впливу на конфіденційність (*Privacy Impact Assessment*).

Ці принципи не лише визначають юридичні вимоги, а й формують етичні межі поводження з даними, закладаючи фундамент для цифрової приватності в межах інформаційного суспільства. Їх застосування є критично важливим не лише у сфері державного управління або банківських послуг, а й у проєктуванні програмного забезпечення, мобільних застосунків, платформ електронної комерції, охорони здоров'я та освіти.

Таким чином, конфіденційність у цифрову епоху є не лише технічним або юридичним поняттям, а комплексною багаторівневою цінністю, що вимагає міждисциплінарного підходу, балансу між доступом до інформації та свободою особи, а також постійного оновлення практик захисту даних у відповідь на технологічний прогрес.

5.3 Основи захисту персональних даних: GDPR, українське законодавство

5.3.1 Загальний регламент про захист даних (GDPR)

Загальний регламент про захист даних (General Data Protection Regulation, GDPR) – це нормативно-правовий акт Європейського Союзу, що набув чинності 25 травня 2018 року та має пряме застосування в усіх державах-членах ЄС. Регламент 2016/679 Європейського парламенту та Ради ЄС було прийнято з метою уніфікації правил обробки персональних даних, посилення прав фізичних осіб та підвищення рівня прозорості в цифровому середовищі [27].

Однією з ключових особливостей GDPR є його екстериторіальність: дія поширюється не лише на організації, зареєстровані в ЄС, але й на будь-які компанії чи структури, які обробляють персональні дані резидентів ЄС – незалежно від географічного розташування серверів чи юридичної особи. Це означає, що навіть українська компанія, яка надає послуги громадянам ЄС, зобов’язана дотримуватись вимог GDPR.

GDPR базується на семи основоположних принципах обробки персональних даних (ст. 5), які визначають етичні та правові межі поводження з інформацією:

- законність, справедливість і прозорість обробки;
- обмеження мети – збір даних лише для чітко визначених цілей;
- мінімізація обсягу даних;
- точність і актуальність;
- обмеження строків зберігання;
- цілісність і конфіденційність;

– підзвітність (accountability).

Ці принципи конкретизуються в нормах, які мають пряму дію і обов'язковість виконання для всіх суб'єктів, що обробляють персональні дані.

GDPR значно розширює та деталізує права громадян як суб'єктів даних. До основних прав належать:

– Право на згоду (ст. 6) – обробка даних допускається лише після надання чіткої, інформованої та добровільної згоди. Заборонено попередньо встановлені «галочки» або неявне погодження.

– Право на доступ (ст. 15) – особа має право знати, які саме її дані зберігає організація, з якою метою та кому вони передаються.

– Право на виправлення та обмеження обробки (ст. 16–18) – користувач може вимагати оновлення або часткове обмеження обробки своїх даних.

– Право на переносимість (ст. 20) – дані мають бути надані у структурованому, машиночитаному форматі.

– Право бути забутим (ст. 17) – суб'єкт може вимагати повного видалення своїх персональних даних, якщо вони більше не потрібні або обробка порушує закон.

– Право на заперечення (ст. 21) – особа має право відмовитись від обробки в цілях прямого маркетингу.

Однією з інновацій GDPR є обов'язок компаній повідомляти про витік персональних даних протягом 72 годин з моменту виявлення (ст. 33). У разі серйозної загрози для прав і свобод суб'єктів даних, організація також повинна проінформувати постраждалих осіб (ст. 34).

Організаціям, які обробляють великі обсяги персональних даних, зокрема у сфері медицини, фінансів, освіти чи телекомунікацій, необхідно призначити уповноважену особу з захисту даних (Data Protection Officer, DPO) – фахівця, що відповідає за дотримання стандартів приватності (ст. 37-39).

GDPR вимагає реалізації принципу Privacy by Design and by Default (ст. 25), що означає вбудовування захисту даних ще на етапі архітектури та проєктування IT-систем. Наприклад, системи повинні за замовчуванням використовувати шифрування, обмеження доступу, мінімізацію даних.

У разі порушення регламенту передбачено значні штрафи:

– до 10 млн євро або 2% від загального обороту – за порушення технічного або адміністративного характеру (ст. 83, ч. 4);

– до 20 млн євро або 4% обороту – за серйозні порушення прав суб'єктів даних або умисне нехтування згодою.

Ці санкції були застосовані до таких компаній, як Google, Meta (Facebook), British Airways та H&M. Приклади – у реєстрі санкцій на сайті EDPB [28].

Станом на 2025 рік GDPR визнано глобальним стандартом, за зразком якого ухвалюються аналогічні нормативні акти в інших країнах – Бразилія (LGPD), Індія (Digital Personal Data Protection Act), Канада (PIPEDA), Каліфорнія (CCPA). У рамках Глобальної декларації щодо цифрових прав [29] ЄС просуває GDPR як модель прав людини в цифровому середовищі.

5.3.2 Законодавство України у сфері захисту персональних даних

В Україні правове регулювання обробки персональних даних ґрунтується на Законі України «Про захист персональних даних» №2297-VI від 1 червня 2010 року, який набув чинності 1 січня 2011 року [16]. Цей документ закріплює основні принципи обробки персональної інформації, права суб'єктів даних, а також обов'язки володільців та розпорядників персональних баз.

Закон передбачає такі ключові компоненти:

1) категорії персональних даних:

– загальні дані (ПІБ, дата народження, адреса, номер телефону тощо);

– чутливі (спеціальні) дані – що стосуються расової чи етнічної приналежності, політичних поглядів, релігійних переконань, стану здоров'я, статевого життя, біометричних і генетичних даних (ст. 7);

– дані про судимість – підпадають під окремий режим захисту.

2) Підстави для обробки персональних даних (ст. 11):

– згода суб'єкта даних (в письмовій або електронній формі);

– необхідність виконання договірних зобов'язань;

– вимоги законодавства;

– життєво важливі інтереси особи;

– легітимний інтерес володільця, якщо він не суперечить правам суб'єкта.

3) Права суб’єкта персональних даних (ст. 8):

– право на інформацію про мету і склад зібраних даних;

– доступ до своїх даних;

– право вимагати виправлення або знищення неточних чи незаконно оброблених даних;

– право відкликати згоду на обробку;

– право на оскарження неправомірних дій у судовому порядку або через Уповноваженого ВРУ з прав людини.

4) Обов’язки володільців даних:

– повідомити суб’єкта про збір і мету обробки;

– забезпечити захист даних від несанкціонованого доступу;

– реєструвати бази даних у відповідних реєстрах (до 2014 р.);

– відповідати за збереження і точність інформації.

Хоча Закон №2297 був актуальним на момент його ухвалення, сьогодні його положення потребують істотного оновлення з урахуванням викликів цифрової трансформації, розвитку хмарних технологій, big data та впровадження електронного урядування.

Ключові недоліки чинного закону:

– відсутність незалежного органу контролю (на відміну від європейських Data Protection Authorities);

– неповне відображення сучасних принципів захисту даних, таких як мінімізація, обмеження строків зберігання, прозорість;

– слабкий механізм згоди – не деталізовано вимоги до добровільності, поінформованості, можливості відкликання;

– відсутність ефективної процедури повідомлення про витоки даних.

У 2023 році було зареєстровано законопроєкт № 8153 «Про персональні дані», який передбачає суттєве оновлення підходів до захисту приватності та наближення українського законодавства до стандартів ЄС у контексті євроінтеграції [30].

Основні новації проєкту:

– створення Національного органу з питань захисту персональних даних – незалежного регулятора, що діятиме на кшталт європейських Data Protection Authorities;

– запровадження прав: на переносимість даних, право бути забутим, право на обмеження обробки;

– обов'язок повідомляти про витік даних протягом 72 годин;

– чітке визначення обов'язків Data Protection Officer (DPO);

– санкції до 5% річного обороту або 30 тис. неоподатковуваних мінімумів доходів громадян за грубі порушення;

– вимоги до згоди – її має бути надано в чіткій, зрозумілій формі, із зазначенням мети та обсягу обробки;

– впровадження принципу «Privacy by Design» – обов'язкове врахування вимог конфіденційності на етапі розробки програмних рішень.

Законодавство України у сфері захисту персональних даних продовжує розвиватись у напрямі європейської інтеграції, однак існує розрив між формальними нормами та реальним станом практики. Актуалізація закону № 2297 [16] та ухвалення сучасного проєкту на основі GDPR – критично важливий крок для забезпечення цифрових прав громадян, розвитку національної цифрової економіки та залучення міжнародних інвесторів.

5.4 Технології цифрової приватності: шифрування, VPN, zero-knowledge, PIMS

У відповідь на виклики цифрової епохи та масовий збір персональних даних активно розвиваються технології цифрової приватності (*privacy-enhancing technologies, PETs*). Їх метою є технічне забезпечення контролю над даними, зменшення ризику втрат конфіденційної інформації та надання користувачам засобів захисту своєї цифрової ідентичності. Найбільш поширеними серед таких технологій є: шифрування, віртуальні приватні мережі (VPN), zero-knowledge протоколи та персональні інформаційні менеджери (PIMS).

Шифрування (encryption) – це процес перетворення даних у форму, недоступну для сторонніх осіб без відповідного ключа розшифрування. Сучасні криптографічні системи поділяються на:

- симетричні (AES, ChaCha20) – використовують один ключ для шифрування і дешифрування;
- асиметричні (RSA, ECC) – застосовують пару ключів: публічний і приватний.

Шифрування відіграє критичну роль у:

- захисті файлів і документів;
- забезпеченні безпеки електронної пошти (наприклад, через PGP) [31];
- шифруванні інтернет-трафіку (TLS/SSL);
- захисті баз даних і хмарних сховищ.

Згідно з ст. 32 GDPR [32], шифрування розглядається як обов'язковий або рекомендований захід захисту під час обробки персональних даних. Шифрування є не лише технологічним елементом, а й етичною практикою мінімізації шкоди у випадку витоку.

Віртуальна приватна мережа (VPN) створює захищене з'єднання між пристроєм користувача та сервером, тунелюючи весь трафік через зашифрований канал. Це забезпечує:

- приховування IP-адреси користувача;
- захист у відкритих мережах Wi-Fi;
- обхід цензури або геоблокування;
- анонімізацію дій у мережі.

VPN важливий для журналістів, правозахисників, IT-спеціалістів, які працюють із конфіденційними даними. Разом із тим, не всі VPN однаково безпечні: безкоштовні сервіси часто порушують принципи приватності, зберігаючи журнали активності користувачів. Рекомендовано використовувати відкриті протоколи (OpenVPN, WireGuard) та політики «no-logs».

Протоколи з нульовим розголошенням (zero-knowledge proof, ZKP) дозволяють підтвердити істинність твердження без розкриття самої інформації.

Ця концепція активно використовується в криптовалютних системах (Zcash), у цифровій ідентифікації та у сфері біометрії.

Наприклад, ZKP може підтвердити, що користувач має певний атрибут (вік, право доступу), не розкриваючи сам документ. Такий підхід:

- зменшує обсяг зібраних даних;
- мінімізує ризики витоку;
- відповідає принципу data minimization у GDPR.

У 2020-2023 роках протоколи ZKP стали основою технологій декларативної автентифікації, де користувач не передає дані, а лише доводить їх наявність [33].

Personal Information Management Systems (PIMS) – це цифрові інструменти, які дозволяють користувачам самостійно управляти обробкою своїх даних. PIMS реалізують концепцію:

- інформованої згоди;
- гнучкого відкликання дозволів;
- централізованого перегляду, хто і як обробляє персональні дані.

Відомі приклади:

- Solid – проєкт під егідою Тіма Бернерса-Лі [34];
- Databox – британський дослідницький проєкт [35];
- MyData – міжнародна ініціатива з цифрової етики [36].

У 2022-2024 роках PIMS активно розглядаються в ЄС як інструмент реалізації цифрових прав користувачів в рамках Європейського закону про управління даними [37] та Закону про дані [38].

Технології цифрової приватності не є просто технічними засобами захисту – вони формують нову етичну та правову парадигму взаємодії між людиною, даними і цифровими системами. Впровадження PETs (Privacy-Enhancing Technologies) є ключовою умовою реалізації принципу «конфіденційність за замовчуванням» та дотримання стандартів цифрових прав. Однак для їх ефективності потрібна синергія: технології + правова база + цифрова грамотність користувача.

5.5 Проблеми згоди та цифрової прозорості

Одним із ключових елементів захисту персональних даних є згода суб'єкта на їх обробку. Проте у цифрову епоху, коли обробка даних стала масовою, автоматизованою та часто непрозорою, традиційна модель згоди виявляється неефективною, маніпулятивною або формальною. Це створює серйозні етичні та юридичні виклики, пов'язані з обсягом, якістю та контекстом отриманої згоди, а також із рівнем цифрової прозорості.

Згідно зі ст. 6 «Законність обробки» та ст. 7 «Умови отримання згоди» GDPR [39], згода є однією з шести законних підстав обробки даних і повинна відповідати чітким критеріям:

- бути вільно наданою, конкретною, інформованою та однозначною;
- передбачати реальну можливість відкликання без негативних наслідків;
- надаватися окремо для кожної мети, а не «пакетно»;
- бути зрозумілою для нефахівця – без складної юридичної мови.

Ці самі критерії закріплено і в українському законодавстві (Закон №2297-VI, ст. 2, 6) [16], однак у практиці часто спостерігається формалізація згоди, коли користувач «приймає» умови без належного ознайомлення або можливості відмови.

5.5.1 Проблема «псевдозгоди» (consent fatigue)

Згода в сучасному цифровому середовищі часто набуває характеру псевдозгоди, коли користувач:

- натискає «Погоджуюсь», не читаючи умов;
- не має реального вибору (наприклад, без згоди сервіс не працює);
- не розуміє, хто саме обробляє дані і для чого;
- не отримує чіткої інформації про третіх осіб, які отримують доступ.

Це явище називають «втомою від згоди» (*consent fatigue*), за якої багато користувачів механічно підтверджують згоду без осмислення наслідків. За дослідженням MIT Technology Review, понад 90% користувачів погоджуються з

політиками конфіденційності, не читаючи їх, а 70% не знають, що можуть відкликати згоду.

5.5.2 Маніпуляції через темні патерни (dark patterns)

У дизайні вебсайтів та застосунків широко застосовуються темні патерни – UX-техніки, що навмисно вводять користувача в оману або стимулюють до «зручного» для сервісу рішення. Найпоширеніші приклади:

– візуальний тиск: кнопка «Прийняти всі» яскрава, а «Налаштувати» – малопомітна;

– емоційні формулювання: «Ви ж не хочете втратити знижку?»;

– непрозорість вибору: десятки чекбоксів у складній формі без пояснення наслідків.

Згідно з аналізом Mozilla у 2022 році, 94% популярних сайтів в ЄС порушували принципи чесної згоди, використовуючи маніпулятивний дизайн. Такі практики є неетичними та можуть порушувати ст. 5 GDPR (принцип прозорості та добросовісності).

5.5.3 Непрозорість даних і ланцюги обробки

Навіть якщо користувач дає формальну згоду, проблемою залишається відсутність прозорості щодо того, хто фактично обробляє дані, де вони зберігаються і з ким передаються. Зокрема:

– компанії залучають третіх осіб і підрядників, не повідомляючи про це явно;

– політики конфіденційності подаються у нечитабельному вигляді (юридична мова, обсяг 20+ сторінок);

– користувач не має засобів перевірки або відкликання згоди постфактум.

Це суперечить концепції Data Transparency – прозорості ланцюга обробки даних, яка передбачає лог документування, інтерфейси доступу до інформації про те, хто, коли і як використовує персональні дані [26].

5.5.4 Етичні альтернативи: етичний дизайн і PIMS

У відповідь на кризу згоди виникає напрям етичного дизайну цифрових сервісів, що пропонує:

– дизайн за замовчуванням з максимальним захистом (privacy by default);

– просту мову та візуалізацію згоди (інфографіка, анімація);

– контекстуальні підказки замість універсальних повідомлень;

– відмову від темних патернів.

Крім того, впроваджуються персональні менеджери приватності (PIMS), які дають користувачу змогу централізовано переглядати, змінювати або відкликати згоди [34; 36].

Згода в цифрову добу – це більше, ніж галочка в політики конфіденційності. Вона має бути інформованою, реалістичною і зворотною. Водночас, справжня приватність можлива лише за умови прозорості технологій, відповідального дизайну інтерфейсів і цифрової етики в основі бізнес-процесів.

5.6 Конфіденційність у Big Data, IoT та соціальних мережах

У контексті цифрової трансформації конфіденційність стає дедалі складнішою для забезпечення через стрімке зростання обсягів даних, розвиток мережевих пристроїв та інтенсивне використання соціальних платформ. Big Data, Інтернет речей (IoT) та соціальні мережі суттєво змінюють природу збору, обробки та поширення персональної інформації. Усі три сфери створюють нові виклики для реалізації принципів конфіденційності, оскільки дані генеруються постійно, пасивно і часто – без відома користувача.

5.6.1 Конфіденційність у Big Data: обсяг, кореляція, непрозорість

Big Data – це масиви даних, які характеризуються «3V»: обсягом (Volume), швидкістю (Velocity) та різноманітністю (Variety). Вони використовуються для аналітики, прогнозування поведінки, автоматизованого прийняття рішень.

Проблеми конфіденційності тут полягають у:

– додатковому виведенні інформації (inference) – з окремих анонімізованих даних можна встановити особу шляхом кореляції;

– непрозорості алгоритмів обробки – користувач не знає, які дані обробляються, в якій формі та з якою метою;

– вторинному використанні даних – зібрані для однієї мети, дані застосовуються для іншої (наприклад, рекламні цілі, скоринг, дискримінація);

– профілюванні – формування цифрових профілів, які впливають на рішення банків, роботодавців, держави.

Як зауважує Організація економічного співробітництва та розвитку (OECP), Big Data створює загрозу переходу до «персоналізованої дискримінації», де людина не знає, що її обробляють і за якими критеріями.

Підходи до пом'якшення ризиків:

– анонімізація та псевдонімізація;

– обмеження вторинної обробки;

– «інформаційна гігієна» – скорочення обсягу даних до необхідного мінімуму.

5.6.2 Конфіденційність у IoT: постійний моніторинг і технічна вразливість

Інтернет речей (IoT) – це екосистема взаємопов'язаних пристроїв (сенсори, камери, побутова техніка, носимі пристрої), які постійно збирають і передають дані в реальному часі. Вони створюють перманентне цифрове спостереження, часто без чіткої індикації або згоди.

Основні ризики:

– відсутність інтерфейсу згоди – більшість IoT-пристроїв не мають екрану, де можна було б прийняти або відкликати дозвіл;

– низький рівень безпеки – паролі за замовчуванням, відсутність оновлень, відкриті API;

– комбінований ефект – кілька пристроїв можуть у сукупності відтворити повну картину приватного життя (патерни сну, харчування, переміщення);

– вразливість до зловживання – компанії або треті сторони можуть збирати дані з пристроїв у маркетингових або інших цілях.

ENISA (Агентство з кліматичної нейтральності) рекомендує впроваджувати Privacy-by-Design у розробці IoT-систем, включаючи:

– локальне зберігання;

– шифрування трафіку;

– контроль користувача за періодом зберігання даних;

– фізичні індикатори збору (лампочки, дисплеї).

5.6.3 Конфіденційність у соціальних мережах: публічність проти контролю

Соціальні мережі (Facebook, Instagram, TikTok, X/Twitter тощо) поєднують елементи приватної комунікації, публічного самовираження та соціального обміну. Водночас, вони є одними з найбільших загроз конфіденційності з таких причин:

- прозора за формою, не прозора за суттю – користувач «контролює» видимість поста, але не знає, хто ще і як обробляє його дані;
- збір метаданих – навіть без публікацій сервіс збирає інформацію про кліки, скролінг, тривалість перегляду;
- алгоритмічна обробка – персоналізований контент створюється за допомогою алгоритмів, які формують «інформаційну бульбашку»;
- обмін з третіми особами – дані продаються рекламним агентствам або інтегруються з іншими сервісами (наприклад, додатки Facebook Login);
- розпливчаста згода – користувач часто не усвідомлює, що саме дозволяє платформі при реєстрації або інсталяції.

Згідно рекомендацій Європейської ради із захисту даних, соціальні мережі зобов'язані:

- надавати повну інформацію про типи та обсяг обробки;
- забезпечити «прості» налаштування конфіденційності;
- мінімізувати необов'язковий збір даних;
- дозволяти відключення таргетованої реклами.

5.6.4 Етичні наслідки та цифрова асиметрія

Big Data, IoT та соцмережі створюють нову інформаційну асиметрію – користувач практично не знає, що саме про нього знають, і не має реального впливу на обробку. Це призводить до таких етичних проблем:

- втрата автономії – рішення приймаються на основі непрозорих алгоритмів;
- цифрова дискримінація – соціальні, медичні або фінансові послуги формуються з урахуванням профілів;
- відсутність «забуття» – цифровий слід важко стерти навіть після видалення акаунту;

– економіка уваги – приватність стає ресурсом, який обмінюється на зручність або доступ до контенту.

Конфіденційність у середовищі Big Data, IoT і соціальних мереж вимагає переосмислення підходів до контролю за даними, впровадження принципу приватності за замовчуванням, посилення ролі цифрової етики та цифрової освіти користувачів. Технології повинні не лише слугувати джерелом зручності й комунікації, а й поважати гідність, автономію та право на інформаційне самовизначення.

ЛЕКЦІЯ 6
ЕТИЧНІ АСПЕКТИ ДЕРЖАВНОГО ТА КОРПОРАТИВНОГО КОНТРОЛЮ В ІТ-СФЕРІ

Мета – сформувати у здобувачів освіти критичне розуміння етичних засад, меж і ризиків державного та корпоративного контролю в ІТ-сфері; проаналізувати приклади сучасних практик цифрового нагляду, алгоритмічного моніторингу, стеження за працівниками та автоматизованого ухвалення рішень; ознайомити з міжнародними стандартами, правами людини в цифровому середовищі та концепціями прозорості й підзвітності контролю; розвинути здатність оцінювати конфлікти між безпекою, приватністю та автономією особи в умовах цифрового управління.

6.1 Контроль у цифрову епоху: між ефективністю, безпекою та етикою

Контроль у сфері інформаційних технологій перетворився з допоміжного інструменту адміністративного управління на системоутворюючий механізм функціонування цифрового суспільства. Його здійснюють як державні інституції (для забезпечення національної безпеки, законності та кіберзахисту), так і корпоративні суб’єкти (у межах моніторингу внутрішніх процесів, управління персоналом, дотримання нормативних вимог і захисту активів). Така багаторівнева присутність контролю в цифровому середовищі не лише відображає потребу в управлінні інформаційними потоками, але й формує нові етичні дилеми, що стосуються приватності, цифрової гідності та довіри до технологій.

Особливість цифрового контролю полягає в тому, що він має невидимий, алгоритмічний і всепроникний характер. На відміну від традиційних форм спостереження, де присутність контролера була відчутною й локалізованою (наприклад, фізичне відеоспостереження), сьогодні контроль реалізується через автоматичні системи, що збирають, аналізують та зберігають величезні обсяги

поведінкових, технічних та біометричних даних – часто без усвідомлення цього самим суб'єктом спостереження.

Алгоритми приймають рішення швидше за людину, але без контексту, емпатії та інтерпретації. Вони можуть помилятись, відтворювати упередження (bias) або залишатися непрозорими – саме це породжує етичну напругу між ефективністю контролю та повагою до прав і свобод особи. Зокрема, особа втрачає суб'єктність, оскільки її поведінку передбачають і коригують у реальному часі – часто без її активної участі або згоди.

В умовах цифрової трансформації суспільства нагляд за поведінкою, комунікацією та активністю користувачів набуває нових форм і масштабів. Інформація подана в таблиці 6.1, демонструє три рівні етики цифрового нагляду: засадничі принципи, потенційні ризики та вектори відповідальності. Такий підхід дозволяє критично осмислити, як саме має відбуватись цифровий контроль – у спосіб, що не порушує приватності, не зловживає владою та зберігає гідність людини.

Таблиця 6.1 – Рівні цифрового контролю в IT-сфері

Рівень контролю	Суб'єкти / мета контролю	Інструменти	Етичні виклики
Державний	державні органи, спецслужби, регулятори / забезпечення безпеки, правопорядку, кіберзахист, регулювання	законодавство, нагляд за трафіком, реєстри, інтерсепція, автоматичний моніторинг	порушення прав людини, масове стеження, непрозорість, цензура
Корпоративний	IT-компанії, служби безпеки, HR-відділи / контроль ефективності, захист активів, відповідність політикам	системи логування, моніторинг дій працівників, камери, email-трекери	порушення приватності працівника, невидимий нагляд, нерівність влади
Алгоритмічний	автоматизовані системи, ШІ-модулі, API / прогнозування, прийняття рішень, виявлення ризиків	алгоритми поведінкового аналізу, оцінки, нейромережі, великий масив даних	відсутність пояснюваності, упередженість, делегування відповідальності алгоритмам

У такому контексті важливо розглядати контроль не лише як інструмент законного регулювання, а як етичну практику, яка повинна:

– мати чітко визначені цілі та межі;

– бути підзвітною та прозорою;

– не порушувати гідність та автономію особи;

– передбачати механізми оскарження та відповідальності.

Цифровий нагляд, який реалізується державними, корпоративними та алгоритмічними механізмами, потребує не лише правового регулювання, а й чітких етичних орієнтирів.

В таблиці 6.2, представлено три ключові компоненти етики цифрового контролю: принципи, що мають лежати в його основі; ризики, що супроводжують його впровадження; а також напрями відповідальності суб'єктів контролю. Така структура дозволяє оцінити, наскільки системи цифрового спостереження відповідають вимогам прозорості, підзвітності та поваги до прав людини.

Таблиця 6.2 – Етика цифрового нагляду: принципи, ризики та відповідальність

Принципи етичного нагляду	Потенційні ризики	Форми відповідальності
пропорційність – контроль має бути співмірним із метою	масове стеження – відсутність вибірковості або обґрунтованості	правова – порушення закону, що регулює обробку даних
прозорість – користувач має знати, що його моніторять	невидимість алгоритмів – людина не усвідомлює факт нагляду	інституційна – підзвітність контролюючих структур перед суспільством
мінімізація даних – збираються лише ті дані, що необхідні	надмірний збір інформації – порушення приватності	професійна – дотримання етичних кодексів (наприклад, IT-спеціалістів)
підзвітність – наявність чітких ролей і контролю за контролем	зловживання повноваженнями – контроль стає інструментом тиску	етична – внутрішній вибір не допускати порушень прав особи

Цифрова ера створила ситуацію, в якій відсутність контролю є загрозою, але й його надмірна або непрозора реалізація – не менш небезпечна. У цьому полягає головна етична дилема: як поєднати потребу в контролі з повагою до свободи і приватності, не допустивши цифрового абсолютизму.

6.2 Державний контроль: етичні межі регуляції, приклади з практики

Державні органи у сфері ІТ здійснюють контроль, керуючись такими пріоритетами:

- національна безпека (захист від кібератак, терористичних загроз);
- інформаційна безпека (боротьба з дезінформацією, пропагандою, фейками);
- правоохоронна діяльність (розслідування кіберзлочинів, моніторинг підозрілої активності);
- захист даних громадян (контроль за обробкою персональної інформації);
- ліцензування та регуляція ІТ-середовища (сертифікація, аудит, нагляд за платформами).

Контроль реалізується через спеціальні органи (в Україні – Держспецзв'язку, СБУ, НКЦК, Кіберполіція), а також через правові механізми – Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [14], Закон України «Про захист персональних даних» [16], Кримінальний кодекс (ст. 361-363) [17] тощо.

У теорії держава повинна гарантувати захист прав громадян. Проте на практиці держава може стати джерелом надмірного контролю, що не відповідає принципам пропорційності та прозорості. Основні етичні проблеми:

- недостатня поінформованість громадян про масштаби стеження (пасивний нагляд);
- використання без рішення суду (масове зняття трафіку, геолокації, перехоплення повідомлень);
- цензура або блокування сайтів під приводом національної безпеки (без чіткої юридичної процедури);
- відсутність незалежного нагляду за структурами, що здійснюють контроль.

У контексті цифрового нагляду держава нерідко опиняється в ситуації одночасного захисника і порушника приватності – особливо у державах із слабкими демократичними інститутами або під час воєнного стану.

Щоб державне втручання в цифрову сферу не перетворилось на зловживання, воно має відповідати таким принципам:

- законність – регулювання повинно базуватися на чітких нормах права;
- необхідність – контроль має виправдовуватись потребою захистити інтереси суспільства;
- пропорційність – засоби нагляду не повинні перевищувати мету;
- підзвітність – органи, що здійснюють нагляд, мають бути відкритими для перевірки;
- оскаржуваність – особа має право знати, що її дані обробляються, і захищати себе.

Ці принципи закріплені, зокрема, у ст. 8 Європейської конвенції з прав людини, рішеннях ЄСПЛ, рекомендаціях Ради Європи, Організації Об'єднаних Націй.

6.2.1 Відомі кейси масового нагляду

– США – програма PRISM (2007-2013): розголошення Едвардом Сноуденом інформації про масове перехоплення електронної комунікації з боку АНБ викликало глобальний скандал. Контроль вівся через Google, Facebook, Microsoft – без судових ордерів. Це поставило під сумнів відповідність дій демократичним стандартам.

– Китай – система соціального рейтингу: на основі даних із камер, банківських систем, соцмереж формуються цифрові профілі громадян. Високий бал відкриває доступ до послуг, а низький – блокує кредити, квитки, освіту. Це приклад тотального державного алгоритмічного контролю, що поєднує законність і масове порушення автономії особи.

– Україна – Системи «Фільтр», «Мегазвіт», «Мережа»: у мирний час здійснювались спроби регулювання доступу до онлайн-платформ (у т. ч. російських), а в умовах війни – контроль за кіберзагрозами та інформаційними впливами. Питання пропорційності, ефективності та прозорості таких систем залишаються відкритими.

6.2.2 Ціна безпеки: етичні обмеження державного нагляду

Питання співвідношення між безпекою та свободою не є новим у філософії політики та прав людини, однак у цифрову епоху ця дилема набуває нової якості. Технології дозволяють забезпечувати безпеку значно ефективніше, ніж у минулому, але водночас – здійснювати безпрецедентно глибокий моніторинг особистості, зокрема без її згоди або знання. Це загрожує поступовим знищенням самої природи свободи як усвідомленого вибору, а не поведінки під наглядом.

Цифровий авторитаризм – термін, що дедалі частіше використовується для опису практик, де держава обґрунтовує масове стеження потребами громадської безпеки. Такі підходи можуть бути ефективними короткостроково, але в довгостроковій перспективі вони підривають довіру до інституцій, сприяють самоцензурі громадян, пригнічують креативність і політичну активність. Парадоксально, але надмірний контроль може знизити загальну стійкість суспільства, роблячи його залежним від централізованих рішень і пригнічуючи ініціативу.

З етичної точки зору, безпека не є абсолютною цінністю, яка дозволяє знехтувати іншими. Навіть у критичних обставинах держава має дотримуватися принципів:

- необхідного мінімального втручання;
- тимчасовості заходів;
- демократичного контролю за діями силових і розвідувальних структур;
- правової визначеності щодо меж втручання в цифрове життя.

Отже, етика державного контролю повинна виходити не лише з технологічних можливостей чи політичної доцільності, а з поваги до гідності людини як цінності, що не може бути відкладена «до кращих часів».

6.3 Корпоративний контроль: стеження за працівниками, аудит активності

У сучасних IT-компаніях контроль над поведінкою працівників і користувачів інформаційних систем розглядається як інструмент безпеки, продуктивності та управління ризиками. Його застосовують з метою:

– виявлення порушень внутрішньої політики компанії;

– захисту комерційної та технічної інформації;

– дотримання вимог ISO/IEC, GDPR та інших стандартів;

– контролю за дотриманням робочої дисципліни.

У практиці поширені такі форми:

– моніторинг інтернет-активності (історія браузера, пошукові запити);

– логування електронної пошти (внутрішньої та зовнішньої);

– контроль застосування програмного забезпечення (встановлення, частота використання);

– відеоспостереження в офісах;

– аналіз продуктивності через трекери часу, клавіатурні логери, AI-оцінювання ефективності.

Основна етична дилема – де закінчується законний інтерес роботодавця і починається право працівника на приватність. З одного боку, компанія має легітимні підстави для контролю з міркувань безпеки. З іншого – персонал залишається суб'єктом основоположних прав, включно з правом на особисту комунікацію та недоторканність приватного життя.

Європейський суд з прав людини у справі *«Барбулеску проти Румунії»* [40] визнав, що роботодавець повинен попереджати працівника про моніторинг і не має права на повний перегляд приватної переписки без чіткої мети. Це рішення стало прецедентом, що окреслив етичні та юридичні межі корпоративного контролю в Європі.

Щоб контроль не порушував гідності, автономії та довіри в колективі, його впровадження має ґрунтуватися на таких принципах:

–прозорість – моніторинг не може бути прихованим;

–необхідність – контроль лише там, де існує ризик;

–мінімізація – збираються лише дані, що справді потрібні;

–інформована згода – працівники мають бути поінформовані й погоджуватись;

–виключення надмірної автоматизації – алгоритмічні оцінки не повинні бути єдиною підставою для санкцій;

–підзвітність – контроль має супроводжуватись аудитами, логами доступу та механізмами оскарження.

Сучасні засоби моніторингу включають:

–SIEM-системи (Security Information and Event Management);

–DLP-рішення (Data Loss Prevention);

–EPM-платформи (Employee Productivity Monitoring);

–AI-нагляд (нейромережі для виявлення «ненормальної» поведінки).

Етичні загрози:

–втрата довіри персоналу;

–цифрове перевантаження – відчуття постійного спостереження;

–непропорційне покарання на основі машинного аналізу;

–стигматизація працівників з низькою продуктивністю або індивідуальними особливостями.

6.4 Проблема прозорості: хто контролює контролера?

В умовах зростаючої складності цифрових інфраструктур, централізації доступу до інформації та автоматизації нагляду, питання прозорості механізмів контролю набуває ключового значення. Етична дилема, сформульована ще у філософських працях Платона й повторена латинським виразом *Quis custodiet ipsos custodes?* («Хто контролює самих контролерів?»), залишається надзвичайно актуальною в контексті цифрової епохи.

У цифровому середовищі контроль здійснюється багаторівнево – державними інституціями, приватними компаніями та алгоритмічними системами. Проте у більшості випадків:

– суб’єкти нагляду не є прозорими у своїх діях;

– не існує механізмів незалежного аудиту контролюючих органів;

– відсутня звітність перед громадськістю або користувачем;

– інструменти стеження самі по собі не піддаються зовнішній оцінці.

У результаті виникає інформаційна асиметрія: ті, хто контролюють, знають усе про інших, але самі залишаються в тіні.

Непрозорий контроль спричиняє низку етичних і соціальних загроз:

– зловживання владою – без зовнішнього нагляду контроль може перетворитись на інструмент тиску, дискримінації або цензури;

– відсутність довіри – користувачі не розуміють, як саме їхні дані використовуються і ким;

– неможливість оскарження – у разі порушення прав особа не знає, як довести факт контролю;

– самоцензура – людина змінює свою поведінку, знаючи, що її можуть моніторити, навіть без офіційного підтвердження.

Додатково, якщо контроль делегується алгоритмам або штучному інтелекту, виникає ще глибша проблема: алгоритмічна непрозорість (*black-box AI*), коли навіть оператор не здатен пояснити логіку ухваленого рішення.

У цифровій етиці прозорість означає не лише доступ до інформації, але й:

– пояснення логіки контролю;

– наявність механізмів оскарження та перевірки;

– фіксація логів доступу до даних;

– публічність політик моніторингу;

– аудит з боку незалежних структур (у т. ч. громадянського суспільства).

Такий підхід закріплений у міжнародних документах:

– OECD Privacy Guidelines [26];

– GDPR – ст. 5, 12, 15 [19];

– Рекомендації CM/Rec(2022)20 Ради Європи щодо впливу цифрових технологій на свободу висловлення думки.

В демократичному суспільстві існує кілька потенційних механізмів зовнішнього контролю за суб’єктами цифрового нагляду (табл. 6.3).

Важливо, щоби жоден суб’єкт контролю не залишався без спостереження, незалежно від того, наскільки благими є його наміри. Саме етична підзвітність і мультиакторна перевірка є основою легітимності цифрового нагляду.

Проблема прозорості – це не лише технічне або управлінське завдання, а етичний виклик цифрової цивілізації. Свобода особи, її гідність і довіра до цифрових систем напряму залежать від того, чи здатне суспільство

контролювати контролерів, забезпечуючи баланс між технологічною потугою і гуманістичними цінностями.

Таблиця 6.3 – Хто має контролювати контролера?

Суб'єкт контролю	Хто його перевіряє?	Інструменти
державні служби нагляду	парламент, суди, омбудсман, ЗМІ, правозахисні НУО	запити, публічні звіти, судовий нагляд
IT-компанії	відомства з кіберетики, органи захисту даних, суспільство	аудит, законодавчі вимоги, журналістські розслідування
алгоритми (AI-модулі)	етичні комітети, технічні аудитори, наукові інституції	алгоритмічна інтерпретованість, валідація моделей

6.5 Конфлікт між безпекою і приватністю

У цифрову епоху одним із найбільш суперечливих етичних викликів стало зіткнення двох фундаментальних цінностей – безпеки та приватності. Обидві мають статус базових прав у демократичному суспільстві, проте в контексті кіберзагроз, воєнного стану, тероризму чи глобальної нестабільності саме безпека часто починає домінувати у публічному дискурсі, витісняючи приватність із порядку денного.

Цей конфлікт особливо загострюється з розвитком технологій, що дозволяють збирати, обробляти й зберігати величезні обсяги даних – від геолокації та пошукових запитів до біометричних зразків і моделей поведінки. У цьому контексті держава, компанії чи служби безпеки можуть здійснювати майже невидимий нагляд, не лише попереджуючи інциденти, а й обмежуючи автономію особи без її згоди.

Відповідно до статті 8 Європейської конвенції з прав людини [21], втручання у приватне життя можливе лише тоді, коли воно є «необхідним у демократичному суспільстві» – тобто, обґрунтованим, пропорційним і підконтрольним. Утім, на практиці ці умови часто ігноруються.

Історичні приклади порушення балансу:

– Програма PRISM (США, 2007-2013). Розсекречена Едвардом Сноуденом, програма дозволяла АНБ отримувати доступ до електронної кореспонденції користувачів без судового ордера. Під гаслом національної

безпеки було порушено конфіденційність мільйонів людей – включно з журналістами, активістами та невинними громадянами [41].

– «Пакет Ярової» (РФ, 2016). Передбачає масове зберігання усіх комунікацій громадян, включно із текстовими повідомленнями та метаданими. Обов'язок щодо дешифрування інформації покладено на провайдерів, що створює прецедент тотального цифрового контролю без достатніх судових гарантій.

– Європейські виклики під час пандемії COVID-19. Деякі країни (Південна Корея, Італія, Німеччина) тимчасово застосовували цифрові паспорти, мобільні трекери, соціальні баланси для контролю переміщення та контактів. Хоча мета була виправдана (громадське здоров'я), постала проблема: чи залишаться ці інструменти у використанні після завершення кризи?

Підміна приватності безпекою поступово формує культуру підозри**,** в якій кожен користувач є потенційною загрозою. Це не лише змінює комунікативну поведінку (самоцензура, уникнення дискусій), але й послаблює соціальний капітал, знижуючи рівень довіри до держави та технологій. Як слушно зауважує Едвард Сноуден, «суспільство, яке жертвує приватністю заради безпеки, зрештою втрачає і те, й інше» [41].

Конфлікт між безпекою і приватністю не має однозначного вирішення. Проте етичне суспільство повинно створювати рамки, де жодна з цінностей не знищується, а реалізується у взаємозалежності. Цифровий контроль має бути службовим, обмеженим і підзвітним, і лише тоді він не становитиме загрози для гідності людини.

6.6 Алгоритмічний контроль: системи нагляду, оцінки, поведінковий аналіз

Алгоритмічний контроль – це форма цифрового нагляду, в основі якої лежить збір, обробка та аналіз великих обсягів даних (Big Data) з подальшим використанням автоматизованих рішень. Такий контроль активно впроваджується в публічному й приватному секторах: у сфері безпеки,

банківській галузі, HR-аналітиці, кримінальному правосудді, охороні здоров'я та освіті. Його мета – забезпечити швидкість, ефективність і прогнозованість управлінських рішень.

Алгоритмічний контроль передбачає використання штучного інтелекту, аналітики великих даних та поведінкових моделей для автоматизованого моніторингу та ухвалення рішень.

Приклади алгоритмічного контролю:

–Predictive policing – технології прогнозування злочинності, які аналізують історичні дані для ідентифікації потенційних «гарячих точок» злочинів. Застосовуються, зокрема, у США (*COMPAS*, *PredPol*) та Великобританії. Проблема – упередження до расових і соціальних груп, що закріплюється в алгоритмах [42].

–Соціальний рейтинг у Китаї – система, що оцінює «соціальну надійність» громадян на основі поведінкових даних: покупок, онлайн-активності, спілкування. Алгоритми використовуються для автоматичного блокування доступу до авіаквитків, кредитів або держпослуг при «низькому» рейтингу.

–Алгоритмічний скринінг кандидатів – компанії використовують AI-інструменти для аналізу резюме, відеозаписів інтерв'ю або соцмереж. Проте такі моделі можуть відтворювати існуючі упередження за віком, статтю чи національністю [43].

–Фінансовий скоринг – банки та платформи аналізують поведінкову аналітику клієнтів (затримки платежів, стиль онлайн-комунікації, частота покупок), щоб прогнозувати їхню кредитоспроможність або оцінювати ризики шахрайства.

Алгоритмічний контроль загрожує принципам цифрової етики через такі проблеми:

– Black-box ефект – відсутність пояснень: користувач не знає, як і чому система ухвалила рішення. Це обмежує можливість оскарження;

– алгоритмічна упередженість (bias) – дані, на яких навчаються системи, відображають соціальні нерівності та дискримінацію. В результаті навіть «нейтральна» система відтворює дискримінаційні патерни;

– позбавлення процесуальної справедливості – особа не має можливості взаємодіяти з системою, яка її оцінює, або виправити помилку;

– ілюзія об’єктивності – рішення алгоритму сприймаються як технічно нейтральні, хоча базуються на людських припущеннях, пріоритетах і обмеженнях;

– автоматизація санкцій – штрафи, блокування або відмови можуть застосовуватись автоматично, без участі людини.

На міжнародному рівні контроль алгоритмів регулюється:

– ст. 22 GDPR – право не підлягати рішенню, що базується виключно на автоматизованій обробці [19];

– OECD Principles on AI – міжнародна декларація про етику ШІ [44];

– AI Act ЄС – нове законодавство, яке класифікує рівень ризику систем ШІ та передбачає заборону на найбільш небезпечні форми алгоритмічного нагляду (наприклад, соціальний скоринг) [45].

Європейська комісія у своїх Рекомендаціях з етики для надійного ШІ [44] сформулювала базові принципи для впровадження етичного алгоритмічного нагляду (табл. 6.4).

Таблиця 6.4 – Етичні принципи алгоритмічного контролю

Принцип	Зміст
Explainability	рішення повинні бути зрозумілими для людини; пояснення мають бути доступні
Accountability	хтось має нести відповідальність за результати дій алгоритму
Fairness	алгоритм не повинен посилювати нерівність або упередження
Human oversight	має бути можлива людська перевірка або скасування рішень AI
Privacy and data governance	захист приватності має бути вбудований у проєктування системи
Societal and environmental well-being	розробка систем повинна враховувати інтереси суспільства

Алгоритмічний контроль – це не лише технологічне досягнення, а й потужний виклик демократичним цінностям, правам людини та етичній відповідальності. Його ефективність має супроводжуватись публічною прозорістю, правом на пояснення, механізмами перегляду рішень та постійним

етичним моніторингом. Інакше існує ризик створення цифрового середовища, де рішення ухвалюються без участі людини, а цифрова автономія замінюється алгоритмічним контролем.

6.7 Міжнародні стандарти, етичні принципи, цифрові права

З огляду на глобальний характер цифрового середовища, проблема контролю, приватності та автономії особи не може вирішуватись лише на національному рівні. Тому міжнародна спільнота – включно з урядами, міжурядовими організаціями, технологічними компаніями та науковцями – сформувала систему багаторівневих стандартів і принципів, що визначають рамки етичного й правового контролю в IT-сфері. Вони охоплюють правові норми, технічні рекомендації, філософські засади і новітні концепції цифрових прав людини.

Наведена графічна карта на рисунку 6.1, візуалізує ключові міжнародні акти, стандарти та декларації, що формують основу сучасної цифрової етики – від європейського GDPR і Конвенції 108+ до рекомендацій ЮНЕСКО та етичних настанов IEEE.

Рисунок 6.1 – Глобальні документи з цифрової етики

Ці документи визначають глобальні орієнтири для створення справедливого, прозорого та людиноцентричного цифрового простору.

6.7.1 Міжнародні правові акти

Правові документи мають пряму дію або рекомендаційний характер, забезпечуючи захист базових цифрових свобод:

– Європейська конвенція з прав людини (ст. 8) гарантує право на повагу до приватного та сімейного життя [21], що застосовується і до цифрового простору. Європейський суд з прав людини неодноразово розглядав кейси, пов'язані з незаконним цифровим наглядом, встановлюючи чіткі межі державного втручання (наприклад, рішення *Barbulescu v. Romania [40]*);

– Міжнародний пакт ООН про громадянські та політичні права (ст. 17) закріплює заборону на «довільне або незаконне втручання в приватне життя», включаючи листування, цифрову комунікацію, дані особистого характеру [46];

– Конвенція Ради Європи №108+ (2018) – єдиний міжнародний правовий документ, який прямо стосується автоматизованої обробки персональних даних. Вона вводить поняття «системи ризику», захищає біометричні дані, вимагає етичного оцінювання впливу на права людини та накладає зобов'язання щодо прозорості у цифровій сфері [47].

6.7.2 Технічні стандарти

Міжнародні стандарти в IT визначають процедури, вимоги та методи забезпечення безпеки й конфіденційності, якими мають керуватися компанії, уряди та розробники:

– ISO/IEC 27001 – найвідоміший стандарт з управління інформаційною безпекою. Передбачає створення, впровадження, моніторинг і постійне вдосконалення систем управління інформацією (ISMS) [3];

– ISO/IEC 27701 – доповнення до 27001, що фокусується на управлінні приватністю, включаючи зберігання згоди, політики конфіденційності, права суб'єктів даних. Визначає ролі володільця та оператора даних відповідно до вимог GDPR [3];

– NIST Privacy Framework (США, 2020) – модель управління ризиками приватності, розроблена Національним інститутом стандартів і технологій США.

Вона дозволяє компаніям будувати ризик-орієнтовані політики приватності, включно з оцінкою впливу технологій (наприклад, ШІ) на користувачів [48].

6.7.3 Етичні принципи в IT (EU, UNESCO, IEEE)

Окрім правового і технічного регулювання, зростає роль глобальної цифрової етики, яка закріплюється у формі принципів та декларацій:

– Human-centric AI – головна вимога сучасної етики: будь-яка технологія повинна слугувати людині, а не навпаки. Розробка алгоритмів має враховувати соціальний контекст і права суб'єктів.

– Transparency (прозорість) – суб'єкти цифрового нагляду зобов'язані пояснювати механізми збору, аналізу і зберігання даних. Це включає логіку алгоритмів, мету контролю і можливість доступу до власної інформації.

– Fairness (справедливість) – автоматизовані системи не повинні дискримінувати за ознаками раси, статі, віку, соціального походження, а результати їхніх рішень мають бути оскаржуваними.

– Right to contest (право на оскарження) – кожна особа має право знати, що її профілюють, та оскаржити результат алгоритмічного рішення.

Ці принципи відображені в документах:

– Ethics Guidelines for Trustworthy AI [44];

– UNESCO Recommendation on the Ethics of Artificial Intelligence [49];

– IEEE Ethically Aligned Design [50].

6.7.4 Цифрові права як розширення прав людини

У XXI столітті сформувалась концепція цифрових прав (табл. 6.5), які розглядаються як логічне продовження класичних прав людини в умовах інформаційного суспільства.

Ці права формалізуються через закони, декларації цифрових прав та практики приватних компаній, які впроваджують етичні політики використання даних.

Глобальна архітектура захисту цифрових прав формується на перетині правових норм, етичних декларацій та технічних стандартів. Впровадження міжнародних механізмів не тільки захищає особу від надмірного контролю, але

й встановлює етичні межі для технологічного розвитку, які забезпечують сталий баланс між інноваціями та людською гідністю.

Таблиця 6.5 – Цифрові права як розширення прав людини

Цифрове право	Сутність
інформаційна самовизначеність	особа має право вирішувати, які її дані збирають і як їх використовують.
право бути забутим (GDPR, ст. 17)	кожен може вимагати видалення своїх персональних даних із баз даних.
право на приватність	захист від невиправданого стеження, витоку чи втручання в особисте життя.
право на цифрову автономію	можливість діяти у цифровому середовищі без маніпуляцій або примусів.
право на безпечну цифрову ідентичність	захист облікових записів, біометрії, автентифікаційних ключів.

ЛЕКЦІЯ 7
СОЦІАЛЬНА ВІДПОВІДАЛЬНІСТЬ ІТ-КОМПАНІЙ ТА ВПЛИВ ТЕХНОЛОГІЙ НА СУСПІЛЬСТВО

Мета – сформувати у здобувачів освіти розуміння концепції соціальної відповідальності ІТ-компаній у глобальному й локальному контексті, розкрити морально-етичні аспекти взаємодії технологічного бізнесу з суспільством, а також дослідити вплив сучасних ІТ на соціальні структури, поведінку, економіку й екологію.

7.1 Поняття соціальної відповідальності в ІТ-сфері

Корпоративна соціальна відповідальність (КСВ) – це стратегія ведення бізнесу, яка передбачає добровільне дотримання ІТ-компаніями етичних норм, дбайливе ставлення до працівників, суспільства та довкілля. У контексті ІТ ця відповідальність поширюється на:

- етичність продуктів і сервісів (наприклад, прозорі алгоритми, конфіденційність користувачів);
- внесок у цифрову інклюзію;
- екологічну та енергетичну ефективність інфраструктур;
- захист цифрових прав і свобод;
- вплив на цифрову грамотність населення.

Етичний дизайн продуктів передбачає створення цифрових сервісів і технологій, які враховують гідність користувача, його автономію та право на інформований вибір. ІТ-компанії відмовляються від маніпулятивних інтерфейсів (наприклад, «темних патернів»), не впроваджують алгоритмів, які навмисно формують залежність, та забезпечують прозорість у механізмах збору даних. Етичний дизайн включає принципи «privacy by design», недискримінації та інклюзивності вже на етапі архітектури продукту.

Відкрите програмне забезпечення (Open Source). Поширення відкритого коду стало важливою практикою соціальної відповідальності, оскільки сприяє

інноваціям, прозорості та глобальній співпраці. Розміщення проєктів у відкритому доступі дозволяє незалежній спільноті перевіряти безпеку, підвищує доступність технологій у країнах з низьким рівнем ресурсів та формує культуру колективного цифрового добра.

Цифрова інклюзія та доступність. Соціально відповідальні IT-компанії прагнуть усунути бар'єри у доступі до цифрових сервісів – мовні, фізичні, фінансові. Це включає розробку доступних інтерфейсів для людей з інвалідністю (звукові описи, масштабування, альтернативний текст), підтримку локалізованих версій програм і впровадження технологій у сільських, малозабезпечених чи маргіналізованих регіонах. Такий підхід розширює цифрові права для всіх.

Екологічна відповідальність. Технологічна інфраструктура споживає великі обсяги енергії та ресурсів, тому екологічна КСВ набуває актуальності. Компанії інвестують у зменшення вуглецевого сліду дата-центрів, використовують відновлювані джерела енергії, розробляють енергоефективне обладнання. Важливою є також підтримка принципу "right to repair", що передбачає ремонтоздатність цифрових пристроїв як спосіб зменшити електронні відходи.

Підтримка освіти та соціальних ініціатив. IT-компанії активно інвестують у розвиток цифрової грамотності, особливо в молодіжному середовищі та в країнах, що розвиваються. Це реалізується через навчальні платформи, стипендії, освітні гранти, партнерства з університетами, а також організацію хакатонів, спрямованих на вирішення соціальних проблем. Така діяльність сприяє формуванню цифрово компетентного громадянського суспільства.

Інфографіка на рисунку 7.1, візуалізує основні сфери, у яких технологічні компанії реалізують свій етичний і соціальний вплив.

Інфографіка охоплює ключові вектори дій – від етичного дизайну продуктів до підтримки цифрової інклюзії, екологічної відповідальності та освітніх ініціатив. Такий підхід демонструє, що соціальна відповідальність у сфері інформаційних технологій – це не лише зовнішній імідж, а глибокий і системний внесок у сталий розвиток цифрового суспільства.

Рисунок 7.1 – Напрями корпоративної соціальної відповідальності в IT-компаніях

На відміну від традиційних галузей, IT-компанії мають унікальну здатність масово змінювати поведінкові моделі та соціальні процеси**,** тому їхня соціальна відповідальність має проактивний характер.

7.2 Форми соціальної відповідальності в IT-компаніях

IT-компанії у XXI столітті дедалі частіше позиціонують себе не лише як постачальники технологічних продуктів, а й як суб'єкти, що впливають на соціальні, культурні та екологічні процеси. Корпоративна соціальна відповідальність (КСВ) у сфері інформаційних технологій охоплює кілька ключових форм, що стали частиною стратегічного бачення провідних гравців індустрії.

1) Етичний дизайн продуктів. Сутність цієї форми КСВ полягає у створенні цифрових продуктів, що зберігають повагу до користувача, не маніпулюють його поведінкою й не експлуатують вразливості:

– інтерфейси без «dark patterns» – компанії, як-от Mozilla чи Signal, уникають створення кнопок або повідомлень, що підштовхують користувача до небажаних дій (наприклад, примусове погодження на обробку даних);

– алгоритми без дискримінації – Google у 2020 році зупинив використання певних моделей ШІ для розпізнавання обличь, аби не поширювати расову упередженість;

– Privacy by design – концепція, впроваджена в продуктах Apple (наприклад, обробка Face ID локально на пристрої, а не на сервері).

2) Відкрите програмне забезпечення (Open Source). Цей підхід демонструє відкритість, прозорість та довіру до спільноти. Компанії, які підтримують open source, сприяють технологічному розвитку суспільства, зокрема в регіонах з обмеженим доступом до комерційного ПЗ:

– Red Hat зробила свій дистрибутив Linux основою для навчання в університетах по всьому світу;

– GitHub надає безкоштовні акаунти освітнім організаціям та розміщує тисячі соціально важливих проєктів (від COVID-ресурсів до інструментів для людей з порушенням зору).

3) Цифрова інклюзія та доступність. Забезпечення рівного доступу до цифрових сервісів незалежно від соціального, фізичного чи культурного стану користувача є ключовим елементом КСВ:

– Microsoft у 2018 році запустила програму AI for Accessibility – набір інструментів для розробників, що дозволяють інтегрувати функції розпізнавання мови, екранні читачі, опис зображень для людей з вадами зору;

– Google Translate розширив підтримку понад 100 мов, включно з регіональними та малопоширеними, задля підтримки мовної інклюзії;

– Meta (Facebook) адаптує платформи для людей з порушенням моторики, впроваджуючи альтернативи управління без використання клавіатури або миші.

4) Екологічна відповідальність. Енергоспоживання дата-центрів і виробництво цифрових пристроїв мають серйозний екологічний слід. Соціально відповідальні компанії впроваджують політики енергоефективності та циклічного використання ресурсів:

– Google з 2017 року повністю переходить на відновлювані джерела енергії для всіх офісів та дата-центрів;

– Apple заявила, що її ланцюги поставок будуть вуглецево нейтральними до 2030 року, а нові моделі iPhone створено з використанням перероблених матеріалів;

– Fairphone – приклад нідерландського стартапу, який створює смартфони, що легко ремонтуються, підтримуючи «right to repair».

5) Підтримка освіти та соціальних проєктів. Технологічні компанії інвестують у розвиток людського капіталу, сприяють цифровій грамотності та підтримують інновації в освіті:

– Coursera, за підтримки Google і IBM, пропонує безкоштовні курси з IT для молоді у країнах, що розвиваються;

– Amazon Web Services (AWS) співпрацює з університетами у програмах хмарної сертифікації, допомагаючи студентам здобувати затребувані навички;

– Cisco Networking Academy навчає понад 2 мільйони студентів щороку в понад 180 країнах, пропонуючи сертифіковані програми з мережевих технологій.

Таким чином, корпоративна соціальна відповідальність в IT-компаніях – це багатоаспектна стратегія, яка виходить за межі бізнесових інтересів і перетворює технології на інструмент соціального добра, інклюзії та сталого розвитку.

7.3 Вплив IT-технологій на соціальну динаміку

Інформаційні технології не лише трансформують виробництво, комунікації та послуги, а й суттєво змінюють структуру суспільних відносин, способи ідентифікації, праці, соціальної взаємодії та навіть сприйняття реальності. Цей вплив має як позитивні, так і амбівалентні наслідки, які слід розглядати з позицій соціальної етики, критичного аналізу та цифрової грамотності.

Медіатизація суспільства. Цифрові платформи – від YouTube до Telegram – стали основними каналами формування публічного дискурсу, політичної активності та колективної пам’яті. Люди споживають новини, формують думки та беруть участь у громадських кампаніях через цифрові медіа. Наприклад, масові флешмоби на кшталт #MeToo або #StandWithUkraine організовувалися та поширювались переважно через соціальні мережі.

Втім, така медіатизація супроводжується небезпеками: фрагментація інформаційного простору, поляризація суспільства, алгоритмічні бульбашки (filter bubbles), які обмежують різноманітність думок. Це створює нову етичну

реальність, де кожен користувач водночас є і споживачем, і ретранслятором інформації.

Економіка платформи. Сервіси на кшталт Uber, Amazon, Upwork, Glovo змінили уявлення про роботу: тепер доступ до праці визначається алгоритмами, а взаємодія між замовником і виконавцем часто є безособовою. З одного боку, це дає гнучкість та можливість для додаткового заробітку. З іншого – призводить до нестабільності, відсутності соціальних гарантій, гіперконкуренції та емоційного вигорання серед працівників (gig economy).

Критики зазначають, що працівники не мають інституційного захисту й не розглядаються як повноцінні учасники трудових відносин. Це породжує етичне питання: чи можуть цифрові платформи бути роботодавцями без відповідальності?

Зміни в освіті та зайнятості. ІТ-технології докорінно трансформують освітні моделі та ринок праці. Автоматизація витісняє цілу низку традиційних професій (наприклад, касири, стенографісти, кур'єри), водночас підвищуючи попит на навички у сфері ІТ, аналітики, креативних індустрій. Це зумовлює потребу у безперервному навчанні, перекваліфікації (reskilling) та цифровій грамотності.

Прикладом є ініціатива Google Career Certificates – короткотермінові онлайн-курси, що дають змогу освоїти затребувану професію без академічного диплома. Однак нерівність у доступі до таких програм, а також відсутність критичного мислення щодо цифрових платформ, може посилити соціальні розриви.

Цифрова соціалізація. Формування стосунків, спільнот, ідентичностей значною мірою відбувається в онлайн-середовищі. Молодь дедалі частіше знаходить друзів, однодумців і навіть партнерів через соціальні мережі, геймерські платформи, форуми. Утворення спільнот більше не прив'язане до географії, а визначається спільністю інтересів, мемів чи ідеології.

Втім, цифрова соціалізація може сприяти ізоляції в реальному житті, формуванню «цифрових племен» та онлайн-радикалізації. Платформи, що спрощують комунікацію, водночас можуть стати інструментом соціальної

ізоляції або викривленої самоідентифікації (наприклад, через надмірну фільтрацію контенту, онлайн-шеймінг).

Вплив на емоційне здоров'я. Цифрова присутність безперервна: сповіщення, лайки, коментарі, push-повідомлення – все це впливає на психологічний стан користувачів. Дослідження підтверджують зв'язок між надмірним користуванням соцмережами і тривожністю, FOMO (fear of missing out), депресією, зниженням самооцінки.

TikTok, Instagram, YouTube часто виступають тригерами для порівнянь, перегорання, цифрового виснаження. У відповідь деякі компанії (наприклад, Apple або Google) впроваджують функції контролю часу використання або режиму «цифрового добробуту», проте етична відповідальність за психологічний вплив поки що лишається розмита.

У результаті вплив ІТ на соціальну динаміку має комплексний характер. Він формує нові виклики для етики, прав людини та державної політики, водночас відкриваючи унікальні можливості для соціального прогресу. Роль ІТ-фахівців у цьому контексті – не лише технічна, а й соціальна, адже кожне рішення щодо продукту чи платформи має реальний суспільний наслідок.

Рисунок 7.2 демонструє, як цифрові технології впливають на ключові аспекти соціального життя: від медіа-споживання та трудових відносин до освіти, формування спільнот і психоемоційного стану людини. ІТ стають не лише інструментом комунікації, а й чинником трансформації суспільних структур, що вимагає етичного переосмислення їхнього впровадження.

Соціальна відповідальність ІТ-компаній – це не просто набір PR-ініціатив, а стратегічне бачення технологічного розвитку, що ставить у центрі людину, її гідність, права та екосистему. Етичний вплив ІТ на суспільство формується через вибір дизайну, моделей обробки даних, корпоративної поведінки та публічної позиції. У добу, коли технології стають рушієм соціальних трансформацій, відповідальність розробника, дизайнера та менеджера є не менш важливою, ніж відповідальність політика чи журналіста**.**

Медіатизація суспільства

соціальні мережі як основне джерело новин;
онлайн-ідентичність формує громадянську активність;
вплив цифрових флешмобів (#MeToo, #StandWithUkraine)

Економіка платформи

гіг-економіка (Uber, Upwork, Amazon);
відсутність соціальних гарантій;
алгоритми як безособові роботодавці

Освіта та зайнятість

перекваліфікація (reskilling) через онлайн-курси;
витіснення рутинних професій ШІ;
платформи для цифрового навчання (Coursera, Google Certificates)

Цифрова соціалізація

формування спільнот у віртуальному просторі;
спільності за інтересами, а не місцем проживання;
ризики ізоляції, фільтр-бульбашок та радикалізації

Емоційне здоров'я

вплив лайків і реакцій на самооцінку;
тривожність, FOMO, цифрове перегорання;
відповідальність платформ за психічне благополуччя користувачів

Рисунок 7.2 – Основні напрями впливу ІТ на соціальну динаміку

ТЕМА 8
ДЕЗІНФОРМАЦІЯ, ЕТИЧНІ ПИТАННЯ В АЛГОРИТМАХ ТА ШТУЧНОМУ ІНТЕЛЕКТІ

Мета – ознайомити здобувачів освіти із ключовими етичними викликами, пов'язаними з використанням алгоритмічних систем та ШІ в сучасному цифровому суспільстві, зокрема щодо розповсюдження дезінформації, упередженості моделей, прозорості рішень та впливу на права людини.

8.1 Проблема дезінформації в цифровому середовищі

Дезінформація – це навмисне поширення неправдивої або маніпулятивної інформації з метою впливу на поведінку, думки або рішення людей. У цифрову епоху вона поширюється з безпрецедентною швидкістю через соціальні мережі, месенджери та відеоплатформи, часто без належної перевірки фактів або джерел. В таблиці 8.1 структуровано проблеми дезінформації, вказуючи на джерела відповідальності та можливі шляхи етичного реагування.

Ключові етичні проблеми:

– руйнування демократичного діалогу (через фейкові новини, маніпулятивні кампанії);

– використання ботів і алгоритмів для нав'язування певного порядку денного;

– підрив довіри до експертів, ЗМІ, наукових установ.

Відповідальність за стримування дезінформації лежить як на платформах (Facebook, X/Twitter, YouTube), так і на розробниках алгоритмів модерації, що визначають, які повідомлення бачить користувач.

Етична оцінка дезінформації вимагає міждисциплінарного підходу, що враховує як цифрову архітектуру платформ, так і людський чинник. Боротьба з фейками – це не лише питання технічної модерації, а насамперед захист прав людини на достовірну інформацію, прозорість і цифрову гідність. Формування

етичної культури в IT-середовищі є передумовою довіри до технологій у демократичному суспільстві.

Таблиця 8.1 – Механізми, приклади та етичні ризики дезінформації

Категорія	Зміст / приклади
механізми поширення	– алгоритмічні стрічки новин; – боти та тролі; – персоналізоване таргетування; – deepfake та генеративні моделі
типові приклади	– скандал *Cambridge Analytica [20];* – боти під час виборів (Brexit, США) [51]; – фейки про COVID-19 у Telegram/YouTube [52]
основні етичні ризики	– руйнування довіри до інституцій; – поляризація суспільства; – ускладнення відокремлення правди від маніпуляцій
хто відповідальний?	– соціальні платформи (Meta, X, YouTube); – розробники алгоритмів; – контент-модератори ; – самі користувачі
рекомендовані рішення	– підтримка медіаграмотності; – прозора модерація; – маркування сумнівних джерел; – вбудована перевірка фактів

8.2 Етичні дилеми алгоритмів

Алгоритми, що керують пошуком, рекомендаціями, персоналізацією та рекламою, істотно впливають на формування інформаційної картини світу кожного користувача. Їхня дія непрозора, оскільки логіка функціонування часто прихована за комерційною або технічною таємницею. Це ускладнює контроль за їхнім впливом та породжує низку етичних викликів.

Основні проблеми:

– black-box problem: користувачі й навіть інженери не завжди можуть пояснити, як алгоритм приймає рішення, що обмежує можливість оскарження або перевірки;

– упередження (bias): алгоритми можуть відтворювати дискримінаційні патерни з навчальних даних (наприклад, упередженість за статтю або расою в системах добору персоналу);

– фінансовий пріоритет: алгоритми віддають перевагу контенту, що генерує більше переглядів, навіть якщо він шкідливий або маніпулятивний (наприклад, сенсаційні відео на YouTube).

Етична дилема: хто несе відповідальність за зміст, що споживається аудиторією? Чи повинна платформа втручатись у потік контенту, якщо це може обмежити свободу слова? Як забезпечити баланс між свободою вираження, безпекою користувача й інформаційною доброчесністю?

Приклади:

– система рекомендацій TikTok або Instagram може створювати залежність, повторно підсовуючи певні типи контенту;

– Amazon, Netflix або Facebook часто не повідомляють, чому той чи інший товар чи пост показаний користувачу;

– сервіси, що використовують персоналізовану рекламу, збирають надмірну кількість даних, не розкриваючи повністю, як ці дані використовуються.

Етична відповідальність:

– розробники повинні впроваджувати принципи *explainability* (пояснюваність) і *fairness* (справедливість). Це означає створення моделей, логіка роботи яких є зрозумілою не лише інженерам, а й кінцевим користувачам. Справедливість передбачає запобігання дискримінації, рівний доступ і незалежний аудит навчальних даних;

– компанії мають публічно декларувати політики модерації та алгоритмічного сортування контенту. Це сприяє прозорості, підзвітності перед суспільством і знижує ризики зловживання цифровою владою. Регулярне оновлення таких політик – необхідна умова етичного управління технологіями;

– користувачі мають право знати, як працює алгоритмічне середовище, у якому вони щодня взаємодіють. Це включає доступ до пояснення, чому їм показано певний контент (наприклад, «чому я це бачу») і можливість змінити параметри персоналізації. Підвищення цифрової грамотності користувачів – ключ до етичного використання технологій.

8.3 Штучний інтелект і етика автономних рішень

З розвитком штучного інтелекту (ШІ) дедалі частіше виникає питання етичної відповідальності за ухвалення рішень, що мають безпосередні соціальні наслідки. Системи на базі ШІ уже сьогодні беруть участь в ухваленні критично важливих рішень у сферах охорони здоров'я, правосуддя, фінансів та безпеки.

Основні сфери застосування автономних систем:

– медичне діагностування: моделі машинного навчання аналізують симптоми, зображення (МРТ, рентген) і медичні записи для прогнозування хвороб. Хибно позитивні або негативні рішення можуть мати фатальні наслідки;

– судове прогнозування (predictive policing): алгоритми прогнозують імовірність повторного правопорушення або локації потенційних злочинів. Часто ці моделі базуються на історичних даних, які вже містять упередження;

– автоматизовані системи оцінки кандидатів: у HR-практиках ШІ використовується для сортування резюме, аналізу відеоінтерв'ю та прогнозування ефективності кандидатів, але ці системи часто дискримінують за віком, статтю або походженням;

– розпізнавання обличь та системи нагляду: застосовуються в аеропортах, торговельних мережах, органах безпеки. Часто вони працюють менш точно для окремих демографічних груп і порушують приватність громадян.

Етичні загрози автономних систем:

– дискримінація через необ'єктивні дані: тренувальні набори даних часто містять історичні соціальні перекоси (наприклад, расову чи гендерну нерівність), які відтворюються у рішеннях ШІ.

– відсутність можливості оскарження: у випадках, коли рішення ухвалюється автоматично, користувач позбавлений можливості зрозуміти або змінити результат. Це суперечить принципу процесуальної справедливості.

– розмитість відповідальності: у разі помилкового або дискримінаційного рішення важко ідентифікувати винного – розробник, постачальник, компанія-інтегратор чи кінцевий користувач.

– порушення автономії: алгоритмічні рішення можуть змінювати поведінку людей (наприклад, системи рекомендацій у навчанні або кар'єрі), не залишаючи місця для особистого вибору.

Етична відповідь:

– ШІ не повинен замінювати людину у рішеннях, що мають моральну вагу, без механізмів контролю. Алгоритмічні системи не повинні остаточно вирішувати питання, які зачіпають права людини – такі як винність у суді або термінове лікування. Людина має залишатися остаточним арбітром, а ШІ – лише асистентом.

– Потрібні системи прозорості, де кожне рішення ШІ має бути пояснюваним (explainable AI). Пояснюваність означає, що користувач і регулятор мають доступ до логіки прийняття рішень. Це зменшує ризики несправедливості та дозволяє виявляти потенційні упередження.

– Необхідне незалежне етичне тестування ШІ перед впровадженням у чутливих сферах. Подібно до клінічних випробувань у медицині, застосування ШІ у праві, охороні здоров'я або фінансах має проходити незалежну перевірку на предмет дискримінації, зловживань і технічної надійності.

– Суспільство повинно вимагати законодавчих обмежень на використання автономних рішень там, де це може зашкодити правам людини. Розробка етичних і юридичних рамок – обов'язок не лише компаній, а й держав. Прикладом є Регламент ЄС з етики ШІ (AI Act), який вводить обмеження на використання технологій високого ризику.

Міжнародні організації (EU, OECD, UNESCO, IEEE) розробили основні етичні принципи для розробки й використання систем штучного інтелекту. Вони закликають компанії, уряди й дослідницькі установи дотримуватись таких норм:

–прозорість (Transparency) – ШІ має працювати за чітко визначеними і доступними правилами. Алгоритми повинні бути зрозумілими для аудиту та пояснення кінцевому користувачу. OECD AI Principles підтримують вимогу до explainability.

–підзвітність (Accountability) – має бути чітко визначено, хто відповідає за дії системи ШІ: розробник, інтегратор чи оператор. Наприклад, IEEE Ethically

Aligned Design [50] наголошує на необхідності юридичної й технічної відповідальності за наслідки роботи ШІ$

–недискримінація (Fairness) – алгоритми не повинні створювати або посилювати соціальні нерівності. Рекомендації ЄС щодо етики ШІ [44] передбачають попереднє тестування моделей на предмет упереджень (bias mitigation).

–повага до автономії – людина має зберігати контроль над рішеннями, особливо у чутливих сферах, як-от охорона здоров'я чи правосуддя. UNESCO вимагає гарантій, що ШІ не буде нав'язувати рішення без інформованої згоди користувача.

–безпека та надійність (Safety and Robustness) – системи ШІ мають бути захищені від технічних збоїв, зовнішніх атак і неконтрольованої поведінки. Стандарти ISO/IEC JTC 1/SC 42 [53] закладають основу технічної безпеки при проектуванні ШІ.

ЛЕКЦІЯ 9
ДОТРИМАННЯ ЕТИЧНИХ НОРМ ПРИ СТВОРЕННІ ТА ВИКОРИСТАННІ ЦИФРОВИХ ТЕХНОЛОГІЙ

Мета – сформувати у здобувачів освіти розуміння етичних зобов'язань ІТ-фахівців на всіх етапах життєвого циклу цифрових продуктів: від проєктування й розробки до впровадження та експлуатації.

9.1 Етика цифрового дизайну та інтерфейсів користувача

У цифровому середовищі взаємодія користувача з технологією часто відбувається через графічний інтерфейс, що має вирішальний вплив на поведінку, сприйняття інформації, ухвалення рішень і навіть психологічне здоров'я. Етика дизайну в цьому контексті – це не лише про естетику чи функціональність, а насамперед про відповідальність за те, як інтерфейс впливає на користувача**.**

9.1.1 Відповідальність дизайнерів за вплив на поведінку користувачів

Дизайнери цифрових продуктів мають етичний обов'язок враховувати соціальні, психологічні та поведінкові наслідки рішень, які вони впроваджують. Інтерфейс здатен:

- підштовхувати до дії (наприклад, зробити кнопку «Купити» яскравою і помітною);
- створювати або зменшувати напругу (через кольорову палітру, анімацію, звукові сигнали);
- вводити в оману або навпаки – допомагати прийняти зважене рішення.

Наприклад, кнопка «Погоджуюсь» у політиці конфіденційності часто набагато більш помітна, ніж кнопка «Відмовитись», що є маніпулятивною практикою.

Дизайнери повинні дотримуватись принципу «design for trust» – створювати інтерфейси, які сприяють чесності, автономності користувача та прозорості.

Приклади етичних рішень у дизайні:

– наявність можливості легко скасувати підписку;

– чітке інформування про збирання персональних даних;

– відсутність надмірної кількості кроків для виходу з системи або видалення облікового запису.

9.1.2 Уникнення патернів темного дизайну (dark patterns)

Dark patterns – це елементи інтерфейсу, які свідомо вводять користувача в оману або маніпулюють його діями в інтересах компанії, а не користувача. Поняття вперше було введено UX-дизайнером Гаррі Бригноллом у 2010 році [54].

В таблиці 9.1 наведено найбільш поширені типи dark patterns, їх опис і приклади з реального цифрового середовища.

Таблиця 9.1 – Основні типи dark patterns

Тип патерну	Опис
Privacy Zuckering	користувача змушують розкрити більше даних, ніж він планував
Roach Motel	легко зареєструватись, але важко відписатись або видалити акаунт
Forced Continuity	після безкоштовної пробної версії автоматично стягуються кошти
Confirmshaming	гумор чи сором у кнопках «Ні, я не хочу бути успішним»
Sneak into Basket	додатковий товар додається в кошик без явної згоди

Такі практики викликають недовіру, можуть шкодити репутації компанії та порушувати етичні стандарти UX/UI-дизайну, а в деяких випадках – навіть законодавство (наприклад, згідно з GDPR ст. 5, ст. 7) [19].

Етичні альтернативи:

– забезпечення явної та зворотної згоди (opt-in, а не opt-out);

– чесна структура навігації;

– відсутність «пасток» у кнопках чи повідомленнях.

9.1.3 Побудова етичного та інклюзивного UX/UI

Інклюзивний UX/UI означає проєктування з урахуванням усіх користувачів, зокрема осіб з інвалідністю, людей похилого віку, людей із

низькою цифровою грамотністю чи представників різних культур. Це не лише про доступність, а й про рівність у цифровому досвіді.

Принципи етичного та інклюзивного дизайну:

–доступність (Accessibility) – використання кольорів із контрастом, адаптація до екранних читалок, підтримка навігації клавіатурою WCAG [55];

–універсальність – забезпечення логіки та зрозумілості інтерфейсу для різних груп користувачів;

–локалізація та культурна чутливість – уникнення культурно неоднозначних або образливих символів, правильний переклад;

–прозорість – інформування користувачів про цілі дій (наприклад, «Натискаючи тут, ви надаєте згоду на обробку даних»).

Приклади:

- можливість масштабування шрифтів;
- підтримка темної/світлої теми для людей із зоровими проблемами;
- прості інструкції, зрозумілі і для новачків.

Організації як Mozilla Foundation чи Microsoft Inclusive Design мають розроблені гайдлайни з інклюзивного дизайну [56].

Етика у дизайні – це не додатковий шар, а невіддільна частина інженерного та дизайнерського процесу. Етичний UX/UI сприяє довірі, ефективності цифрових сервісів і позитивному суспільному впливу. Застосування принципів етики в дизайні не тільки відповідає професійним стандартам, а й формує довготривалі цінності бренду та компанії.

9.2 Етичне програмування: інтеграція етичних принципів у життєвий цикл ПЗ

Етичне програмування – це не окремий етап, а безперервна практика, яка пронизує весь життєвий цикл розробки програмного забезпечення (Software Development Life Cycle – SDLC). Воно передбачає врахування людських цінностей, прав користувачів, прозорості та безпеки від етапу ідеї до супроводу

готового продукту. Такий підхід формує довіру до технологій і мінімізує негативні соціальні наслідки від їх впровадження.

Життєвий цикл ПЗ складається з таких основних фаз:

–ініціювання / планування;

–аналіз вимог;

–проєктування;

–розробка;

–тестування;

–впровадження;

–супровід та оновлення.

На кожному з цих етапів можуть виникати етичні ризики, тому розробники мають:

– розглядати наслідки використання продукту;

– враховувати потреби вразливих груп;

– забезпечувати відповідальність за алгоритмічні рішення.

Моделі етичної інтеграції:

Ethics-by-design – цей підхід передбачає систематичне впровадження етичних міркувань у кожну фазу SDLC. Наприклад, при створенні системи рекомендацій для медичного застосунку – передбачити механізм контролю лікарем, а не лише автоматичну відповідь ШІ.

Value-Sensitive Design (VSD) – методологія, що враховує людські цінності, такі як приватність, справедливість, автономність, ще на етапі проєктування [57].

Обидва підходи вимагають співпраці розробників, етиків, соціологів, юристів для об’єктивної оцінки впливу ПЗ.

Паралельно з функціональним тестуванням, важливо проводити етичну перевірку (ethical audit) (табл. 9.2).

Наприклад, *тестування алгоритмів найму на предмет дискримінації за віком або статтю.*

Етичне програмування потребує чіткої внутрішньої документації, яка:

– фіксує цілі, пріоритети й можливі ризики;

– описує механізми ухвалення рішень в умовах моральної невизначеності;

– забезпечує трасованість рішень (тобто пояснення, чому було реалізовано саме таке рішення).

Таблиця 9.2 – Етичне тестування та ревізія програмного забезпечення

Вид етичної перевірки	Приклад питання
прозорість	Чи може користувач зрозуміти, як працює система?
приватність	Які дані збираються? Чи є згода?
недискримінація	Чи немає упередженості в алгоритмах?
безпека	Як захищені особисті та фінансові дані?
підзвітність	Хто відповідальний за помилкові дії системи?

Відомі організації, такі як OpenAI, Google AI, Mozilla, публікують етичні гайдлайни та impact reports до своїх технологічних рішень.

Програміст виступає не лише технічним виконавцем, а й співтворцем наслідків, які несе продукт. Це означає:

– відмову від реалізації завідомо шкідливих або неетичних функцій;

– відкритий діалог із замовниками щодо можливих етичних ризиків;

– участь у розробці політик організації з питань етики розробки.

Наприклад, *програміст може ініціювати включення механізмів інформування користувача про збирання даних – навіть якщо замовник про це не подбав.*

Інтеграція етики у життєвий цикл ПЗ – це не розкіш, а необхідність у сучасному цифровому світі**,** де алгоритми дедалі частіше впливають на реальні людські долі. Етичне програмування формує не лише якісний продукт, але й відповідальне технологічне середовище**,** в якому ключовими є не лише інновації, а й мораль.

9.3 Добровільне саморегулювання та ініціативи етичної відповідальності

У сучасному технологічному світі державне регулювання часто не встигає за швидкістю інновацій, тому важливу роль відіграє добровільне саморегулювання, тобто внутрішнє зобов’язання компаній, спільнот і окремих фахівців дотримуватись високих етичних стандартів без примусу з боку закону.

Такі ініціативи спрямовані на зниження соціальних ризиків, зміцнення довіри користувачів та формування культури відповідального програмування.

Ініціативи Tech Pledge, Partnership on AI, Mozilla Manifesto:

Tech Pledge – це форма добровільної декларації етичної поведінки для IT-фахівців, компаній та розробників. Вона містить зобов'язання:

– не створювати інструментів, які порушують права людини;

– дотримуватись принципів прозорості, недискримінації, доступності;

– сприяти сталому цифровому розвитку.

Partnership on AI – міжнародна коаліція, до якої входять Google, Apple, Amazon, Microsoft, Meta, IBM, OpenAI та університетські й неурядові організації. Заснована з метою:

– сприяти етиці та прозорості у сфері штучного інтелекту;

– обговорювати дилеми, пов'язані з автономними системами;

– поширювати кращі практики.

Mozilla Manifesto – декларація етичних цінностей, якої дотримуються розробники Firefox та інших відкритих цифрових продуктів Mozilla. Основні принципи:

– інтернет як глобальний публічний ресурс має бути відкритим і доступним;

– безпека і приватність – фундаментальні права;

– компанії несуть відповідальність перед суспільством, а не лише акціонерами.

Відкритість та самоперевірка стали новою нормою для багатьох IT-компаній, які створюють етичні платформи, де вони публічно звітують про вплив своїх продуктів або політик. Приклади таких механізмів:

– Open Source Ethics Statements – етична декларація, що додається до open-source проєктів;

– AI Model Cards – документація, яка описує поведінку, обмеження та цілі алгоритмів ШІ;

– Privacy Nutrition Labels – аналог «етикеток» для даних, які показують, які саме дані збираються (ініціатива Apple у 2021 році);

– Ethical Review Boards – внутрішні комітети етичної експертизи продуктів перед запуском.

Такі платформи допомагають суспільству оцінити ризики, а також створюють умови для громадського контролю над цифровими продуктами.

Звіт про вплив цифрових продуктів (Ethical Impact Report) – це документ, який публікується разом із запуском або оновленням цифрового продукту й містить:

- оцінку соціального впливу (на користувачів, суспільство, екологію);
- опис потенційних ризиків для прав людини;
- аналіз конфліктів інтересів;
- заходи з пом'якшення негативного впливу.

Компанії, які вже впровадили подібні звіти:

- Google (AI Principles Report);
- Facebook (Human Rights Report);
- Microsoft (Responsible AI Impact Assessment).

Університетські дослідницькі центри, як-от Berkman Klein Center (Harvard) чи Oxford Internet Institute, також пропонують методології для створення таких звітів.

Добровільне етичне саморегулювання – це новий стандарт корпоративної поведінки в цифрову епоху. Воно дозволяє бути на крок попереду законодавства, підтримувати довіру користувачів і демонструвати, що технології можуть працювати на благо суспільства, а не лише задля прибутку. Участь в етичних ініціативах – не лише прояв відповідальності, а й маркер зрілості компанії чи розробника.

9.4 Аналіз кейсів порушення етичних норм при створенні та впровадженні цифрових технологій

Етичні принципи в IT-сфері набувають реального змісту тоді, коли вони застосовуються на практиці. В таблиці 9.3 наведено **аналіз гучних кейсів**, у яких цифрові технології були використані всупереч етичним нормам.

Таблиця 9.3 – Розбір відомих кейсів

Назва кейсу	Суть	Порушені етичні принципи	Наслідки
Cambridge Analytica	збір даних 87+ млн користувачів Facebook без згоди для політичних маніпуляцій (Brexit, США)	– відсутність інформованої згоди; – непрозорість алгоритмів; – маніпуляція думкою; – недотримання приватності	– $5 млрд штраф Facebook; – розпуск Cambridge Analytica; – падіння довіри до соцмереж
Uber і Greyball	Uber використовував «Greyball» для обману правоохоронців у країнах, де сервіс працював незаконно	– цілеспрямований обман держави; – обхід законодавства; – застосування технологій для порушення суспільних норм	– скандал; – звільнення керівників; – репутаційні втрати; – посилення нагляду
Amazon AI Hiring Tool	алгоритм дискримінував жінок при відборі резюме через навчання на упереджених даних	– алгоритмічна упередженість; – непрозорий процес; – порушення принципу рівності	– відмова від використання; – перегляд тестування ШІ; – громадська дискусія про дискримінацію

Аналіз порушень етичних норм у відомих кейсах цифрових технологій дозволяє глибше зрозуміти джерела проблем, етапи, на яких вони виникають, та рівень відповідальності різних учасників процесу. Нижче наведено короткі відповіді на ключові запитання, які допомагають структурувати етичну оцінку таких ситуацій:

1) Чи були ці порушення наслідком людських рішень, або проблемою системи/алгоритму?

– Cambridge Analytica – наслідок свідомих людських рішень (зловживання доступом до даних);

– Uber – свідоме рішення менеджменту створити систему обходу законів;

– Amazon AI Hiring – технічна проблема алгоритму, але через відсутність належного етичного нагляду.

2) На якому етапі можна було запобігти порушенню?

–на етапі проєктування систем (включення етичних обмежень);

–під час тестування (виявлення дискримінаційної поведінки алгоритмів);

–через внутрішній аудит або етичну експертизу до публічного запуску.

3) Яку відповідальність несуть розробники, менеджери, компанія в цілому?

–розробники – часткова відповідальність, якщо знали про ризики й не повідомили;

–менеджери – основна відповідальність за рішення щодо впровадження та замовлення таких функцій;

–компанія – юридична та репутаційна відповідальність, включаючи штрафи, регуляторний нагляд, втрату користувачів.

4) Як суспільство може реагувати на такі інциденти?

– через суди – подання позовів до компаній (класові позови, компенсації);

– через ЗМІ – викриття зловживань, громадський тиск;

– через бойкот – відмова від продукту, падіння доходів;

– через політичний тиск – вимога до законодавців змінити норми й посилити контроль.

Аналіз кейсів порушення етики в ІТ дозволяє не лише побачити наслідки рішень у цифровій сфері, але й сформувати власну позицію, критичне мислення та відповідальність за майбутні розробки.

ЛЕКЦІЯ 10
КОНФЛІКТИ ІНТЕРЕСІВ ТА НЕЕТИЧНА ПОВЕДІНКА В IT-КОМАНДАХ

Мета – ознайомити здобувачів освіти з етичними викликами, які виникають у командній взаємодії під час розробки цифрових рішень, та навчити розпізнавати, запобігати й ефективно реагувати на неетичну поведінку і конфлікти інтересів в IT-середовищі.

10.1 Неетична поведінка в команді: форми, причини, наслідки

У сучасних IT-командах, особливо в умовах високої конкуренції, швидких дедлайнів і гнучких методологій розробки, питання командної етики стає критично важливим. Неетична поведінка в команді порушує довіру, демотивує колег, знижує якість продукту і створює ризики для всієї організації. Важливо розуміти, які форми неетичності можуть виникати, чим вони викликані і до чого призводять.

10.1.1 Маніпуляції, саботаж, приховання помилок

Маніпуляції:

– використання психологічного тиску або дезінформації з метою досягнення власної вигоди (наприклад, маніпулювання пріоритетами спринту);

– ігнорування фактів або свідоме перебільшення значущості своєї ролі.

Саботаж:

– свідоме уповільнення роботи, зниження продуктивності або перешкоджання роботі інших членів команди;

– пасивна форма протесту або помста за управлінські рішення.

Приховання помилок:

– замовчування критичних багів, недоліків у коді чи архітектурі;

– страх втратити репутацію або уникнути відповідальності.

Наслідки: порушення цілісності проєкту, втрати фінансування, зниження довіри клієнтів, розвал команди.

10.1.2 Привласнення авторства, відмова від командної відповідальності

Привласнення авторства:

– один із членів команди або керівник представляє результат роботи всієї команди як свій власний;

– ігнорування внеску менш досвідчених учасників.

Відмова від відповідальності:

– спроба уникнути відповідальності за помилки, перекладання провини на колег;

– ігнорування колективного ухвалення рішень.

Наслідки: втрата довіри, демотивація команди, підвищений рівень плинності кадрів.

10.1.3 Мікроагресія, пасивно-агресивна поведінка, токсичне лідерство

Мікроагресія:

– систематичні зневажливі або саркастичні зауваження, що зачіпають особистість (гендер, вік, акцент тощо);

– може виглядати як «жарт», але має кумулятивний шкідливий ефект.

Пасивно-агресивна поведінка:

– демонстрація незадоволення через ігнорування, мовчазний саботаж, уникаючі відповіді;

– створює напружену атмосферу в команді.

Токсичне лідерство:

– домінування через страх, погрози, приниження або публічну критику;

– відсутність емпатії, жорстка ієрархічність, придушення ініціативи.

Наслідки: професійне вигорання, зниження продуктивності, конфлікти, плинність персоналу.

10.1.4 Вплив стресу, дедлайнів і змагання на етичність рішень

Інтенсивні дедлайни, багатозадачність, нестача сну та конкуренція в IT-сфері створюють середовище ризику для етичних компромісів. Приклади:

– програміст іде на свідоме порушення правил безпеки задля вчасного релізу;

– команда замовчує проблеми, щоб не втратити контракт;

– колега навмисно не ділиться знаннями, щоб зберегти унікальність своєї ролі.

Згідно з дослідженням ACM Code of Ethics, етичність рішень різко знижується під тиском термінів і конкуренції, особливо в умовах відсутності чітких етичних стандартів у компанії.

Неетична поведінка в IT-командах не лише впливає на психологічний клімат і добробут співробітників, але й несе пряму загрозу якості, безпеці та ефективності цифрових продуктів. Її вчасне виявлення та профілактика мають стати складовою етичної культури колективу, а також компетенцією кожного фахівця у сфері інформаційних технологій.

10.2 Конфлікт інтересів на керівних посадах

Керівники в IT-командах – тімліди, менеджери, технічні директори (CTO), HR-спеціалісти – мають вплив на стратегічні рішення, кар'єрний розвиток співробітників і розподіл ресурсів. Водночас вони можуть опинитися в ситуації, коли їхні особисті інтереси суперечать інтересам команди або компанії, що становить конфлікт інтересів. Етична поведінка в управлінській ролі вимагає особливої обережності, прозорості та самоконтролю.

10.2.1 Етичні ризики для тімлідів, технічних директорів, HR

Тімліди (Team Leads):

– можуть зловживати владою: призначати завдання не за компетенцією, а з особистих симпатій;

– ігнорувати об'єктивні результати через емоційне ставлення до підлеглих;

– впроваджувати суб'єктивні методи оцінювання (performance review).

Технічні директори (CTO, Senior Devs):

– мають вплив на вибір технологій, які можуть бути обрані не з міркувань ефективності, а через особисті зв'язки з вендорами або партнерами;

– можуть блокувати інноваційні рішення молодших колег, які сприймаються як загроза авторитету.

HR-спеціалісти:

– відповідають за добір персоналу, вирішення конфліктів, збереження корпоративної етики;

– ризикують потрапити в ситуацію, коли підтримують рішення менеджменту всупереч інтересам працівників;

– можуть упереджено проводити рекрутинг через особисту зацікавленість (кумівство, конфлікти, замовчування порушень).

Приклад конфлікту інтересів: СТО просуває кандидатуру на підвищення, з якою має неофіційні ділові зв'язки (наприклад, спільний стартап).

10.2.2 Непрозорий підбір персоналу

Конфлікт інтересів особливо гостро проявляється при непрозорому рекрутингу, коли:

– перевага надається «своїм» кандидатам без об'єктивної оцінки;

– ігноруються внутрішні політики добору (технічні тести, рекомендації, співбесіди);

– приховується інформація про зв'язки з кандидатом (наприклад, родич, колишній співзасновник).

Це не лише неетично, але й підриває довіру команди до керівництва, створює ґрунт для конфліктів, пасивного саботажу й демотивації.

10.2.3 Використання повноважень у власних цілях

До типових проявів зловживання службовим становищем належать:

– використання службового часу або ресурсів на сторонні проєкти, не погоджені з роботодавцем;

– лобіювання сторонніх бізнес-інтересів всередині компанії;

– вплив на бюджет, закупівлі, вибір підрядників у власних комерційних інтересах;

– прийняття рішень щодо найму, премій чи звільнень з упередженням.

Наприклад, *керівник віддає підряд на аутсорсинг компанії, де є співзасновником, без відкритого тендеру.*

ISO 37001 і OECD Guidelines вимагають запровадження систем внутрішнього моніторингу таких дій.

Конфлікт інтересів на керівних посадах – одна з найнебезпечніших форм неетичної поведінки в IT-команді, оскільки її важко виявити, але вона глибоко підриває довіру й ефективність управління. Етична поведінка управлінців вимагає прозорості, саморефлексії, вміння відмовитись від рішень, які можуть бути вигідними особисто, але шкідливими для організації.

10.3 Виявлення та врегулювання конфліктів інтересів

Політики розкриття інтересів передбачають, що працівники (особливо керівного рівня) відкрито повідомляють про свої особисті, фінансові або родинні зв'язки, які можуть вплинути на прийняття рішень. Це дозволяє:

- попередити конфлікт, перш ніж він стане проблемою;
- делегувати прийняття рішень нейтральним сторонам;
- забезпечити прозорість управлінських процесів.

В IT-компаніях disclosure policies часто включаються в onboarding-процедури. Це формальна частина пакета документів або електронних форм, які працівник заповнює або підписує при працевлаштуванні, де:

- повідомляє про наявність родинних, ділових чи фінансових зв'язків із іншими працівниками компанії;
- вказує на участь у зовнішніх проєктах, стартапах чи партнерствах, що потенційно можуть впливати на прийняття рішень;
- підтверджує відсутність (або наявність) конфліктів інтересів відповідно до визначених критеріїв.

Переваги включення disclosure policy в onboarding:

- прозорість з першого дня: формує атмосферу довіри та взаємної відповідальності;
- раннє виявлення ризиків: дозволяє HR/менеджменту вчасно відреагувати або змінити розподіл ролей;
- юридичний захист: у разі майбутніх інцидентів компанія має документальне підтвердження;

– уніфікація процесів: працівники чітко розуміють, що очікується в контексті етики.

Інтеграція disclosure policy в onboarding – це етична профілактика, яка дозволяє компанії ще до початку співпраці окреслити кордони професійної відповідальності та мінімізувати майбутні ризики. Це сучасна практика, що демонструє відповідальність і зрілість корпоративної культури в IT-індустрії.

Системи внутрішнього контролю допомагають структуровано реагувати на виявлені порушення. Вони включають:

– етичні комітети або відповідальні особи в HR/Legal;

– конфіденційні канали для скарг (whistleblowing);

– механізми ескалації для конфліктних ситуацій;

– процедури незалежного розгляду (наприклад, через зовнішніх аудиторів).

Важливо, щоб такі процедури були зрозумілими, доступними і захищали працівників від репресій за повідомлення.

HR-стандарти (внутрішні нормативні документи компанії або зовнішні галузеві рекомендації, які регламентують кадрові процеси) містять конкретні процедури щодо підбору, просування, оцінювання персоналу з урахуванням етичних критеріїв. У контексті професійної етики, HR-стандарти виконують важливу роль у забезпеченні чесності, прозорості та недискримінації в роботі з персоналом.

Комплаєнс-офіцер (compliance officer) – особа, відповідальна за контроль за дотриманням внутрішніх політик, міжнародних норм і етичних стандартів.

У сфері IT його завдання включають:

– виявлення та попередження конфліктів інтересів;

– контроль за захистом персональних даних (наприклад, відповідність GDPR);

– моніторинг дотримання кодексів поведінки, антикорупційних та етичних норм;

– проведення внутрішніх перевірок і аудитів, консультування керівництва;

– реагування на скарги працівників щодо етичних або правових порушень.

Комплаєнс-офіцер є посередником між працівниками, менеджментом і регуляторами, забезпечуючи етичну цілісність та юридичну безпеку компанії.

У середніх і великих компаніях ці ролі є частиною системи корпоративної відповідальності (CSR).

У таких компаніях як Google, Microsoft, Atlassian, disclosure policy є частиною стандартного корпоративного onboarding-порталу, де новий працівник у цифровому вигляді:

– підписує NDA (угоду про нерозголошення),

– погоджується з політикою боротьби з дискримінацією,

– подає декларацію конфлікту інтересів (або засвідчує її відсутність).

10.4 Запобігання неетичній поведінці в команді

Корпоративна культура – це невидимий регулятор поведінки**,** який формує норми взаємодії. Етична культура ґрунтується на:

– повазі до особистості;

– чесності у зворотному зв’язку;

– орієнтації на довгостроковий результат, а не короткострокову вигоду.

Лідери мають бути прикладом у дотриманні етичних норм.

10.4.1 Прозорі правила співпраці, система зворотного зв’язку

У командній ІТ-роботі прозорість є основою етичної взаємодії. Вона зменшує ризики непорозумінь, уникання відповідальності, маніпуляцій і конфліктів. Чітко визначені правила співпраці та ефективна система зворотного зв’язку створюють умови для довіри, відповідальності й професійного зростання всіх учасників процесу.

Прозорість починається з чітких рамок:

– Job descriptions – формалізовані посадові інструкції з описом завдань, очікувань, KPI;

– RACI-матриці – таблиці, що фіксують ролі кожного учасника проєкту:

1) R – responsible (виконує);

2) A – accountable (несе відповідальність);

3) C – consulted (дає поради);

4) I – informed (поінформований).

– договори в командах (team working agreements) – узгоджені правила комунікації, дедлайнів, способів вирішення конфліктів.

Результат: кожен учасник знає, що він має робити, з ким взаємодіє, хто ухвалює рішення, а хто надає підтримку.

Метод 360-градусного зворотного зв'язку передбачає отримання оцінок:

– від керівника;

– від колег (горизонтальна оцінка);

– від підлеглих (якщо є);

– від самого працівника (самооцінка).

Переваги:

– зменшення суб'єктивності оцінювання;

– виявлення прихованих проблем (токсична поведінка, саботаж, пасивність);

– розвиток саморефлексії й особистої відповідальності.

Анонімність у процесі гарантує чесність і безпечність висловлювань.

Багато IT-компаній (Google, Atlassian, Basecamp) впровадили регулярні peer-review цикли щоквартально або двічі на рік із обов'язковою участю всіх рівнів команди.

Технічні інструменти дозволяють фіксувати й візуалізувати поточний стан роботи, мінімізуючи маніпуляції, приховування або подвійні трактування. Найбільш поширені серед IT-команд:

Slack bots – автоматичні нагадування, інформування про дедлайни, stand-up боти для щоденного звітування; опитування щодо самопочуття команди, виявлення проблем ще до їх ескалації.

Trello, Jira, Asana – візуалізація задач у Kanban/Agile-дошках, доступних усій команді; публічне відстеження прогресу, відповідальних, статусів задач.

Confluence, Notion – централізоване зберігання документації, специфікацій, командних угод; прозорість процесу прийняття рішень, історія змін.

Приклади використання:

– Sprint Retrospective документується в Confluence з відкритим доступом для перегляду й коментарів;

– Trello Board фіксує дедлайни, відповідальних і ризики по кожній задачі – усі бачать прогрес.

Прозорість співпраці – це етична технологія управління командами, яка запобігає конфліктам і підвищує ефективність. Чітко задокументовані ролі, регулярний зворотний зв'язок і прозорі цифрові інструменти допомагають не лише координувати роботу, а й створюють культуру відповідальності, довіри та поваги в IT-середовищі.

10.4.2 Навчання з етики, тренінги з конфліктології

Успішне функціонування IT-команд залежить не лише від технічних знань, а й від розвиненої етичної культури, комунікативної гнучкості та здатності вирішувати конфлікти без ескалації. Саме тому регулярне навчання з етики та конфліктології є ключовим елементом профілактики деструктивної поведінки в організаціях.

Цілі періодичних тренінгів:

1) розпізнавання проявів неетичної поведінки:

– навчання працівників виявляти мікроагресію, приховану дискримінацію, маніпуляції, фаворитизм тощо;

– ознайомлення з прикладами типових етичних дилем в IT (конфлікт інтересів, обхід безпеки, непрозорий рекрутинг);

– пояснення, коли і як варто реагувати, до кого звертатися.

2) формування soft skills для вирішення конфліктів:

– розвиток навичок активного слухання, неконфліктного зворотного зв'язку (non-violent communication), медіації;

– створення сценаріїв вирішення побутових і професійних суперечок без емоційної ескалації;

– практика ведення складних розмов у парах/групах.

3) тренування емоційної компетентності:

– уміння розпізнавати власні емоції і контролювати їх у конфліктних ситуаціях;

– підвищення толерантності до стресу і професійної саморегуляції;

– розвиток емпатії, як базової складової лідерства й командної роботи.

Навчання з етики та конфліктології – це інвестиція в командну стабільність та довготривалу ефективність. У динамічному середовищі ІТ саме соціальні навички й емоційна культура стають незамінними складниками професіоналізму, поряд із технічними компетенціями.

10.4.3 Психологічна безпека та підтримка в колективі

Психологічна безпека (psychological safety) – це командна характеристика, що означає, що кожен член команди може вільно висловлювати свої ідеї, запитання, занепокоєння або помилки без страху бути покараним, осміяним або проігнорованим. Вона є основою для етичної комунікації, ефективного зворотного зв’язку, інновацій і довіри.

Основні ознаки психологічної безпеки в команді:

– можна відкрито говорити про проблеми, не боячись осуду;

– кожна думка розглядається як цінна, незалежно від посади чи досвіду;

– немає страху поставити «дурне» запитання або попросити про допомогу;

– помилки сприймаються як частина навчання, а не як причина для покарання;

– ініціатива заохочується, навіть якщо вона не призвела до успіху.

Що потрібно для підтримки психологічної безпеки:

1) Заохочення відкритості та ініціативності:

– керівники мають демонструвати емпатію, повагу й увагу до кожної думки;

– регулярні зустрічі формату «safe space», де обговорюються труднощі без тиску;

– визнання ініціатив і “сміливих ідей”, навіть у разі їхнього провалу.

2) Наявність внутрішнього психолога або EAP (Employee Assistance Program):

– внутрішній психолог або доступ до анонімної психологічної допомоги;

– консультації з питань вигорання, стресу, міжособистісних конфліктів;

– проведення м’яких HR-опитувань щодо психологічного клімату в колективі.

Більші IT-компанії (Google, EPAM, Grammarly, SoftServe) впроваджують EAP-платформи або «well-being programs», що включають психоемоційну підтримку.

3) Негайна реакція на токсичну поведінку та булінг:

– фіксація скарг, навіть якщо вони надходять неформально або анонімно;

– визначені санкції проти агресії, сексизму, приниження, публічного сорому;

– навчання лідерів і HR щодо виявлення прихованих форм токсичності (наприклад, мікроагресія, емоційний шантаж).

За даними Harvard Business Review [58], токсична поведінка є основною причиною звільнення з роботи серед молодих фахівців у IT-сфері. А також наголошується, що «токсична культура в 10 разів сильніше впливає на рішення звільнитися, ніж рівень зарплати». Це підкреслює важливість створення психологічно безпечного, етичного середовища в IT-командах.

Психологічна безпека – це не «м'який» компонент, а стратегічна умова командної ефективності, особливо у високотехнологічному середовищі. Компанії, що інвестують у психологічну підтримку та створення відкритого середовища, отримують лояльніших, креативніших та стійкіших фахівців, здатних приймати етичні рішення навіть у стресових умовах.

ЛЕКЦІЯ 11
ВІДПОВІДАЛЬНІСТЬ ЗА КІБЕРЗЛОЧИНИ ТА ПОРУШЕННЯ БЕЗПЕКИ ІНФОРМАЦІЇ

Мета – сформувати в здобувачів освіти розуміння юридичної, професійної та етичної відповідальності ІТ-фахівців за участь або сприяння кіберінцидентам, навчити аналізувати наслідки цифрових дій, класифікувати типи кіберзлочинів і відрізняти навмисне порушення від службової недбалості.

11.1 Основні типи кіберзлочинів і пов'язані з ними етичні порушення

Кіберзлочини порушують не лише правові норми, а й фундаментальні етичні принципи: повагу до приватності, чесність, прозорість, безпеку і відповідальність. Кожен тип кіберзлочину має свої моральні наслідки, які потрібно враховувати при формуванні професійної етики в ІТ-сфері:

1) зломи інформаційних систем (hacking) призводять до витоку конфіденційної інформації, порушення приватності та знищення довіри користувачів до цифрових сервісів. Компанії зазнають репутаційних втрат, юридичних позовів і значних витрат на відновлення безпеки.

Злом серверів Yahoo (2013-2014) став одним із найбільших витоків даних в історії: хакери отримали доступ до понад 3 мільярдів облікових записів, включаючи імена, адреси електронної пошти, дати народження, хешовані паролі та контрольні запитання користувачів [61].

Етичні порушення:

- недостатній захист особистих даних користувачів;
- несвоєчасне інформування про злом (реальну інформацію компанія оприлюднила лише в 2016 році);
- нехтування відповідальністю перед мільйонами користувачів, які постраждали від подальшого несанкціонованого використання їхніх акаунтів.

Наслідки:

- різке падіння довіри до Yahoo;

– зниження вартості компанії на $350 млн під час її придбання Verizon;

– сотні мільйонів доларів витрат на юридичні врегулювання та компенсації.

2) DDoS-атаки можуть паралізувати інфраструктуру цілих компаній або державних органів. Наслідки включають зупинку онлайн-сервісів, збитки у мільйони доларів, втрату бізнес-можливостей та підрив критичних цифрових функцій (наприклад, систем охорони здоров'я чи електропостачання).

Атака на DNS-провайдера Dyn (2016) [62] була однією з найбільших у світі DDoS-атак, під час якої ботнет Mirai, що складався з десятків тисяч IoT-пристроїв, вивів із ладу роботу ключового інтернет-посередника – компанії Dyn, яка обслуговувала DNS-запити для багатьох глобальних сервісів.

Унаслідок атаки мільйони користувачів втратили доступ до таких популярних платформ, як Twitter, Netflix, Reddit, Spotify, GitHub, Airbnb, PayPal, що спричинило масштабний інтернет-колапс у США та Європі.

Етичне значення:

– використання незахищених пристроїв (IP-камер, роутерів) для створення ботнету без відома їхніх власників;

– демонстрація вразливості критичної інфраструктури інтернету;

– підняття питання відповідальності не лише атакувальних сторін, а й виробників ненадійних IoT-пристроїв.

Наслідки:

– порушення функціонування великої кількості онлайн-послуг;

– перегляд стандартів безпеки для пристроїв IoT;

– створення нових ініціатив для запобігання ботнет-атакам, зокрема з боку урядових структур США.

3) фішинг і соціальна інженерія завдають шкоди не тільки окремим людям, які втратили доступ до своїх акаунтів чи грошей, але й підривають довіру до цифрових технологій загалом. Постраждалі особи часто не знають, як захистити себе, що робить їх уразливими повторно.

Кейс Google і Facebook (2013–2015, виявлено у 2017) [63]: упродовж кількох років обидві компанії стали жертвами масштабного шахрайства з боку

одного хакера, який підробляв рахунки-фактури від імені тайванської фірми Quanta Computer – постачальника обладнання.

Шахрай Евалдас Римасаускас створив підроблені електронні листи, контракти та печатки, надсилаючи їх на фінансові відділи компаній, які без перевірки здійснювали грошові перекази на підконтрольні йому рахунки.

Сума викрадених коштів склала понад $100 мільйонів, перш ніж шахрайство було виявлено у 2017 році.

Етичне значення:

– недостатня перевірка контрагентів навіть у найбільших IT-компаніях;

– проблема сліпої довіри до електронного документообігу;

– відсутність багаторівневої перевірки рахунків, що свідчить про прогалини в цифровій етиці управління фінансами.

4) шкідливе програмне забезпечення (malware) має ефект «цифрової епідемії».

WannaCry (2017) – глобальна атака програмою-здирником (ransomware), яка за лічені години поширилася більш ніж у 150 країнах, зашифрувавши файли на сотнях тисяч комп'ютерів із вимогою викупу у біткоїнах [64].

Особливо серйозно постраждали державні структури, транспортні системи та лікарні у Великій Британії (NHS) – десятки медичних закладів були змушені скасувати операції та перевести пацієнтів через недоступність даних. Також ураження зазнали Renault, Deutsche Bahn, FedEx та інші інфраструктурні об'єкти.

Етичні аспекти:

– навмисне порушення роботи критичних сервісів, що поставило під загрозу здоров'я та життя людей;

– використання вразливості EternalBlue, розробленої АНБ США, яка раніше була викрадена хакерами;

– використання шкідливого коду без розбору – жертви не вибиралися адресно, а зараження було масовим.

Втрати:

– прямі збитки, за оцінками, сягнули $4 мільярдів;

– репутаційні втрати для держав і розробників уразливих систем;

– прискорення процесів переходу на безпечніші ОС та автоматичного оновлення.

5) крадіжка персональних або фінансових даних призводить до вторинних злочинів: шахрайства з кредитами, шантажу, викрадення особистості (identity theft). Люди не лише втрачають гроші, а й стикаються з тривалими юридичними проблемами.

Equifax Data Breach (2017) – один із найбільших витоків персональних даних у світі, який стався через експлуатацію уразливості в вебдодатку компанії Equifax, одного з найбільших кредитних бюро США [65].

Хакери отримали доступ до системи Equifax, викравши персональні дані понад 147 мільйонів осіб, включно з іменами, датами народження, адресами, номерами соціального страхування та, у деяких випадках, номерами водійських посвідчень і банківськими реквізитами.

Етичні аспекти:

– нехтування базовими стандартами кібербезпеки: компанія ігнорувала відоме оновлення системи (Apache Struts);

– відсутність своєчасного повідомлення постраждалих користувачів про витік;

– проблема прозорості та відповідальності фінансових інститутів перед суспільством.

Наслідки:

– масові випадки шахрайства та крадіжки ідентичності (identity theft);

– втрата довіри до Equifax та інших бюро кредитної історії;

– судові позови на мільярди доларів і штрафи, включаючи $700 млн врегулювання з FTC.

6) алгоритмічна упередженість (bias) у системах ШІ не завжди сприймається як «злочин», проте її наслідки – дискримінація, втрата рівності шансів, обмеження доступу до послуг для маргіналізованих груп. Це може призводити до соціальної поляризації.

Amazon AI Hiring Tool (2014-2017) – експериментальна система автоматичного відбору резюме, яка мала допомогти Amazon швидко фільтрувати кандидатів на технічні посади. Проте алгоритм почав системно дискримінувати жінок [66].

Алгоритм був натренований на даних про попередні успішні кандидати – переважно чоловіків, тому система почала занижувати оцінку резюме, де згадувалося «жіноче походження», наприклад: участь у «women's chess club» або випуск із жіночого коледжу.

Етичні аспекти:

– алгоритмічна упередженість (bias), що виникає з некоректних тренувальних даних;

– відсутність прозорого процесу оцінювання кандидатів;

– порушення принципів рівності у доступі до працевлаштування;

– проблема «чорної скриньки» – неможливість пояснити рішення ШІ.

Наслідки:

– Amazon відмовилася від цієї AI-системи до офіційного впровадження;

– утворився міжнародний резонанс і критика щодо непрозорого впровадження AI у HR;

– стимулювання дискусій щодо відповідального AI (Responsible AI) і справедливих моделей машинного навчання.

7) використання технологій з метою обману регуляторів (як-от Greyball від Uber) демонструє, як технічна експертиза може бути використана для обходу законів. Наслідками стали публічні скандали, посилення нагляду та зміни законодавства в окремих країнах.

Uber Greyball (2014-2017) – інструмент, розроблений компанією Uber для виявлення та обходу дій регуляторів і правоохоронних органів у містах, де сервіс працював без офіційного дозволу [67].

Програма «Greyball» використовувала дані з додатку, кредитних карток, соціальних мереж та поведінки користувачів, щоб ідентифікувати чиновників,

які могли проводити перевірки, і підмінити їм інтерфейс Uber – наприклад, показувати їм фейкові авто або скасування замовлень.

Етичні аспекти:

– маніпуляція технологіями з метою уникнення регулювання;

– недобросовісна конкуренція та відсутність прозорості;

– свідоме введення в оману урядових інституцій – саботаж законодавчого поля;

– порушення суспільного договору між технологічною компанією та громадою.

Наслідки:

– широкий суспільний резонанс після розслідування The New York Times;

– звільнення кількох керівників, включно з керівником правового відділу;

– посилення перевірок Uber у США, Франції, Італії та Австралії;

– удар по репутації Uber як технологічного новатора.

В таблиці 11.1 узагальнено основні типи кіберзлочинів, їхню етичну оцінку та приклади з практики.

Розгляд семи гучних цифрових кейсів – Cambridge Analytica, Uber Greyball, Amazon AI Hiring Tool, Dyn DDoS-атака, Google/Facebook фінансова афера, WannaCry та Equifax data breach – демонструє, що етичні порушення в IT є багатогранним явищем, яке зачіпає як індивідуальні дії фахівців, так і організаційні політики, а також помилки або упередженість в алгоритмах.

У кожному з випадків етичні ризики не були враховані на етапі проєктування, тестування або управлінського прийняття рішень, що призвело до:

– порушення приватності мільйонів користувачів (Cambridge Analytica, Equifax);

– маніпуляцій та дезінформації (Cambridge Analytica, Google/Facebook scam);

– алгоритмічної дискримінації (Amazon AI Hiring Tool);

– підриву цифрової інфраструктури та довіри до онлайн-сервісів (Dyn, WannaCry);

– цілеспрямованого обходу законів (Uber Greyball).

Ці приклади яскраво ілюструють важливість етики цифрової відповідальності, потребу в внутрішньому контролі та аудиті технологій, а також відповідальності не лише розробників, а й топменеджменту компаній.

Таблиця 11.1 – Типові кіберзлочини та їх етичне значення

Тип кіберзлочину	Етичне порушення	Приклад
1	2	3
злом систем (hacking)	порушення конфіденційності, приватності, довіри	Yahoo breach (2013-2014) – витік даних 3 млрд акаунтів The New York Times [61]
DDoS-атаки	навмисне перешкоджання цифровому сервісу, шкода користувачам	Dyn attack (2016) – вплив на Twitter, Netflix, Reddit, Spotify CSO Online [62]
фішинг	шахрайство, маніпуляція довірою, крадіжка персональних даних	Google/Facebook (2017) – втрати на $100 млн BBC [63]
соціальна інженерія	експлуатація людських слабкостей, введення в оману	дзвінки «з банку» з проханням назвати CVV-код чи OTP
поширення шкідливого ПЗ (malware)	умисне заподіяння шкоди, маніпуляція ресурсами, вимагання	WannaCry (2017) – глобальний шантаж, ураження лікарень NCSC [64]
крадіжка персональних / фінансових даних	порушення прав людини, спричинення особистих втрат	Equifax (2017) – викрадено дані 147 млн людей FTC [65]
алгоритмічна дискримінація	упереджене ставлення, відтворення соціальної нерівності через ШІ	Amazon AI Hiring Tool – дискримінація жінок при відборі резюме Reuters [66]
використання технологій для обману	навмисна маніпуляція державними або регуляторними органами	Uber Greyball – приховування активності NYT [67]

Суспільство також має відігравати активну роль – через регуляцію, освітні ініціативи, незалежний аудит та інформування користувачів. Саме поєднання технічної компетентності з етичною зрілістю дає змогу запобігти подібним порушенням у майбутньому.

11.2 Етична оцінка наміру та наслідків цифрових правопорушень

Згідно з Будапештською конвенцією про кіберзлочинність [59], кіберзлочини поділяються на ті, що спрямовані проти комп'ютерної системи (наприклад, злом), і ті, що вчиняються через неї (наприклад, шахрайство).

ІТ-професіонали можуть бути причетні до неетичних або протизаконних дій, навіть ненавмисно:

- зловживання правами адміністратора – доступ до чужих листів, файлів без дозволу;
- ігнорування кібербезпеки – використання слабких паролів, відсутність шифрування;
- інсайдерські витоки – передача даних третім сторонам;
- використання бекдорів після звільнення.

Щороку Verizon [60] публікує один з найавторитетніших звітів у сфері інформаційної безпеки, що базується на аналізі тисяч реальних кіберінцидентів по всьому світу.

У професійній етиці ІТ-сфери важливо розглядати не лише юридичний аспект цифрового правопорушення, а й моральну оцінку дій: що саме було зроблено, з якою метою та до чого це призвело. Така оцінка базується на аналізі наміру (intent) і наслідків (impact).

Намір – це мотив, внутрішня мета особи, яка вчинила дію. В етиці, зокрема за деонтологічними підходами (Кант), намір є визначальним у моральній оцінці.

Етична оцінка ситуації часто змінюється залежно від того, чи було порушення свідомим і зловмисним, чи воно сталося внаслідок незнання, помилки або недбалості. Наведена таблиця 11.2 ілюструє різні варіанти наміру та відповідні етичні наслідки. Етична оцінка вимагає врахування не лише наміру, а й результатів вчинків, які можуть бути як безпосередніми (втручання в систему, витік даних), так і опосередкованими (поширення дезінформації, втрати довіри). Саме тому етика в ІТ оперує поняттям відповідальності за наслідки**,** включаючи ситуації, коли шкоду було завдано ненавмисно.

Таблиця 11.2 – Намір як ключовий етичний критерій

Намір	Етична оцінка
зловмисний (malicious intent)	однозначно неетичний
нейтральний / неусвідомлений	потребує контексту, можливе пробачення
добросовісний (benevolent intent)	може бути етично виправданий, навіть якщо дія формально незаконна

Наслідки – це реальний вплив дій або бездіяльності на інших осіб, компанії, суспільство. У етиці наслідків (утилітаризм) важливо оцінити баланс шкоди і користі, який спричинила дія.

У таблиці 11.3 наведено приклади цифрових дій і можливі наслідки, що мають етичну вагу в оцінці вчинків спеціалістів.

Таблиця 11.3 – Наслідки цифрових дій

Наслідки	Етична оцінка
масова шкода (дані, фінанси, здоров'я)	неетично, незалежно від наміру
обмежена шкода	залежить від співвідношення з користю
очікувана суспільна користь	може бути етично допустимою (але ризикована)

Для повноцінної етичної оцінки дій у цифровому середовищі важливо враховувати обидва аспекти – і намір, і наслідок. Такий комбінований підхід дозволяє глибше аналізувати ситуації, в яких, наприклад, добрі наміри призводять до шкідливих результатів, або ж навпаки – негативні наміри не спричиняють суттєвої шкоди. Цей підхід застосовується у професійній етиці, комплаєнсі та при розслідуванні кіберінцидентів, де важливо диференціювати навмисні порушення, недбалість і нещасні випадки. Таблиця 11.4 ілюструє типові сценарії, поєднуючи наміри та наслідки, і дозволяє сформувати більш зважене етичне судження.

Таблиця 11.4 – Комбінований підхід: намір × наслідок

Намір / наслідок	Негативні наслідки	Позитивні наслідки
добросовісний	дилема / професійна помилка	соціально прийнятно
байдужий / неусвідомлений	недбалість / порушення	ситуаційна оцінка
зловмисний	етичне порушення	незаконна доцільність

Етична оцінка цифрових правопорушень повинна враховувати не лише зовнішні обставини чи формальну законність, а насамперед намір виконавця та реальні наслідки для людей і суспільства. Такий підхід допомагає точніше визначити рівень моральної відповідальності фахівця і сприяє формуванню усвідомленої професійної поведінки в ІТ-сфері.

11.3 Відповідальність ІТ-спеціалістів за порушення безпеки

Відповідальність ІТ-спеціалістів за порушення безпеки – це ключовий аспект професійної етики в цифрову епоху, коли наслідки навіть незначних помилок можуть бути масштабними як у технічному, так і в правовому чи репутаційному вимірах. ІТ-фахівці, які працюють із конфіденційними даними або відповідають за безпеку інфраструктури, повинні усвідомлювати, що їхня діяльність напряму пов’язана з питаннями юридичної та етичної відповідальності.

11.3.1 Випадки службової недбалості, перевищення повноважень, бездіяльності

ІТ-фахівці можуть нести персональну відповідальність, якщо:

1) ігнорують базові вимоги безпеки, наприклад, залишають відкриті порти, використовують паролі за замовчуванням або не оновлюють ПЗ вчасно. Це найпоширеніша, але водночас одна з найбільш критичних форм службової недбалості. До неї належать:

- відкриті порти: залишення мережевих портів відкритими без потреби створює уразливість для сканування та експлуатації. Наприклад, порт 22 (SSH) або 3389 (RDP), відкритий для всієї мережі без обмежень, може бути легко використаний для несанкціонованого доступу, що порушує принцип мінімізації привілеїв (principle of least privilege);
- паролі за замовчуванням: використання або незаміна заводських паролів (наприклад, admin:admin) є грубим порушенням політик безпеки. Багато IoT-атак типу Mirai botnet базувалися саме на експлуатації стандартних облікових даних;

– невчасне оновлення програмного забезпечення: це один із головних чинників кіберінцидентів. Уразливість Apache Struts, не оновлена компанією Equifax [65], призвела до викрадення даних 147 млн осіб, що стало прикладом системної технічної і етичної недбалості.

Етична оцінка: ІТ-фахівець, що ігнорує ці базові правила, наражає на ризик мільйони користувачів та підриває довіру до всієї цифрової інфраструктури.

2) Перевищують повноваження, наприклад, отримують доступ до даних, які не мають права переглядати (case of Edward Snowden – один з найвідоміших прикладів). Це стосується ситуацій, коли працівник використовує службові повноваження в особистих або несанкціонованих цілях, наприклад:

– доступ до персональних даних без службової необхідності: це може включати перегляд медичних записів, листування, або фінансових документів користувачів без запиту від вищого керівництва чи без дозволу.

– використання адмін-доступу для зміни логів, обходу політик безпеки або підвищення власних прав доступу без належної фіксації чи погодження.

Випадок Едварда Сноудена – колишнього співробітника АНБ, який мав доступ до засекречених документів та оприлюднив їх. Незалежно від суспільної оцінки його вчинків, з юридичної точки зору це було перевищенням повноважень і порушенням службової присяги.

Етична оцінка: хоча мотиви можуть бути як егоїстичні (саботаж, збагачення), так і альтруїстичні (викриття зловживань), сам факт несанкціонованого доступу порушує і закон, і довіру.

3) Не реагують на інциденти, навіть якщо мають інформацію про загрозу (failure to act може прирівнюватися до службової недбалості згідно з ISO/IEC 27001 [3]). Цей тип порушення стосується бездіяльності, навіть коли фахівець знає про потенційну чи активну загрозу. Приклади:

– не повідомляє про знайдену уразливість (наприклад, в API, системі логування або аутентифікації), сподіваючись, що «нічого не станеться».

– ігнорує лог-файли, які свідчать про спроби злому, або не виконує належного моніторингу, залишаючи систему без нагляду у критичний момент.

Згідно з ISO/IEC 27001, організація має встановити чіткі процедури реагування на інциденти, а працівники – негайно повідомляти про інциденти, навіть потенційні [3].

Етична оцінка: мовчання або байдужість у таких ситуаціях є пасивною формою порушення, що може мати серйозні наслідки. Якщо фахівець не діє, він порушує свій професійний обов'язок забезпечити кібербезпеку.

Наслідки*:* звільнення, фінансові штрафи, кримінальна відповідальність (особливо у сфері захисту персональних даних – згідно з GDPR [19] або Законом України «Про захист персональних даних» [16]).

11.3.2 Обов'язки адміністраторів безпеки, DevOps, розробників

Кожна технічна роль в IT-команді має не лише функціональні, а й етичні зобов'язання. Відповідальність за інформаційну безпеку, конфіденційність даних та стійкість систем лежить не тільки на CISO чи керівнику, а розподіляється між усіма членами технічної команди (табл. 11.5). Ігнорування етичних практик (наприклад, недостатнє тестування, пропуск код-рев'ю, публікація уразливого коду) може призвести не лише до технологічних втрат, а й до масштабних наслідків для користувачів, бізнесу й суспільства загалом.

Таблиця 11.5 – Ролі IT-фахівців, їх обов'язки та типові етичні порушення

Роль	Основні обов'язки	Потенційні порушення
Security Administrator	налаштування політик доступу, контроль міжмережевих екранів, шифрування, аудит логів, реагування на загрози	– ігнорування оновлень безпеки; – неправильне налаштування списків контролю доступу (ACL); – недокументовані backdoor-доступи
DevOps Engineer	підтримка процесів CI/CD, управління інфраструктурою як кодом, конфігурація контейнерів та хмар	– відкрите зберігання конфіденційних даних (API-ключі, паролі) у репозиторіях; – недостатнє логування або його відсутність; – використання застарілих Docker-образів
Software Developer	безпечне програмування, валідація введених даних, впровадження TLS, обробка помилок	– вразливості типу SQL-ін'єкцій або XSS; – незахищене зберігання паролів (plain text); – відсутність input sanitation або rate limiting

Етичні практики, які мають бути обов'язковими для кожної ролі:

– регулярний код-рев'ю: дозволяє виявляти потенційні порушення безпеки ще до релізу;

– принцип найменших привілеїв (PoLP): жоден учасник команди не повинен мати доступу до більшого, ніж потрібно;

– безперервне тестування безпеки (security testing): інтеграція у DevOps-процеси, використання SAST/DAST-інструментів;

– прозоре логування та аудит: важливо не лише для реагування на інциденти, а й для дотримання принципу підзвітності.

Етична поведінка в IT – це не лише про те, що дозволено за законом, а й про те, що є справедливим і безпечним для інших людей. Кожен технічний спеціаліст, незалежно від своєї ролі, має усвідомлювати вплив власних рішень і бути готовим нести відповідальність за безпеку та добробут користувачів.

11.3.3 Питання відшкодування збитків та корпоративна відповідальність

Індивідуальні IT-фахівці також можуть бути притягнуті до відповідальності, якщо:

– завдали збитків через злісне порушення посадових обов'язків або умисну шкоду (наприклад, видалення важливих файлів після звільнення);

– ігнорували політики компанії, що призвело до вразливостей (наприклад, відкритий доступ до репозиторію з секретами);

– діяли поза межами повноважень (наприклад, доступ до персональних даних без належного дозволу).

В Україні це регулюється нормами Цивільного кодексу [68] та законодавством про працю (наприклад, ст. 130-132 КЗпП України про обмежену матеріальну відповідальність працівників [69]). В таблиці 11.6 представлено типові приклади санкцій залежно від характеру правопорушення, що дає змогу усвідомити ризики як для окремих працівників, так і для компаній у цілому.

Таблиця 11.6 – Види санкцій

Тип порушення	Можливі наслідки
недбалість при адмініструванні	виробниче розслідування, догана, штраф
умисне втручання в IT-системи	кримінальна відповідальність, звільнення
порушення GDPR / захисту даних	корпоративні штрафи, компенсації користувачам
командна бездіяльність у разі загрози	сукупна відповідальність + репутаційні втрати

У цифровому середовищі відшкодування збитків не завжди означає лише фінансові втрати**.** Репутація бренду, втрата довіри, відтік клієнтів – це непрямі наслідки етично або технічно неправильних дій. Тому етичне управління ризиками, прозорість дій команди, відповідальність і регулярне навчання є запорукою не лише технічної, а й моральної стійкості ІТ-компаній.

11.4 Роботодавець VS працівник: межі відповідальності за інциденти

У сфері інформаційних технологій межі відповідальності між роботодавцем і працівником щодо порушень безпеки або етичних інцидентів часто є тонкими й залежать від конкретного контексту. Законодавство, внутрішні політики та належна документація відіграють ключову роль у визначенні, чи несе працівник індивідуальну відповідальність, чи інцидент є наслідком організаційної недосконалості. У таблиці 11.7 наведено типові сценарії поділу відповідальності між працівником і компанією.

Таблиця 11.7 – Межі відповідальності за інциденти

Сценарій	Відповідальний	Коментар
працівник здійснив порушення після проходження інструктажу, підписання NDA, чіткого доступу до правил	працівник	вважається, що він діяв усвідомлено. Компанія може притягнути до дисциплінарної або юридичної відповідальності
працівник діяв у межах наданих йому прав доступу, але системні налаштування дозволяли шкідливі дії	роботодавець	відповідальність несе компанія, яка не впровадила достатніх заходів контролю доступу
немає підтвердження, що працівник ознайомлений з політиками безпеки або пройшов навчання	роботодавець	вважається, що організація не створила умов для дотримання етики
компанія не вела журналів аудиту, що унеможливило визначення винного	роботодавець	відсутність логування – це системний недолік, а не особистий промах
порушення спричинене людською помилкою в умовах надмірного навантаження чи дедлайнів	спільна відповідальність	аналіз причин має враховувати стрес-фактори та управлінську культуру

11.5 Системна відповідальність: коли інцидент є наслідком організаційних недоліків

Типові випадки, коли провина за інцидент у сфері IT-безпеки або етики частково або повністю лежить на системі управління, а не на окремому працівнику:

– відсутність чітких політик і процедур. Якщо компанія не затвердила політику безпеки, не провела інструктаж або не забезпечила працівника належною інформацією – відповідальність за інцидент покладається на керівництво. Наприклад, співробітник випадково пересилає конфіденційний файл, не позначений як «internal only», – бо не було політики маркування.

– Недостатній контроль доступу. Якщо працівник отримує надмірні права доступу, які йому не потрібні для виконання роботи, і це призводить до витоку або зловживання – це проблема архітектури доступу (role-based access), а не виключно людського фактору. Наприклад, аналітик отримав повний доступ до даних клієнтів без реальної потреби – і через помилку надіслав їх у відкритому листі.

– Неякісні інструменти безпеки. Компанія не оновлює ПЗ, використовує уразливі системи або не має механізмів журналювання – це створює ситуації, коли неможливо відстежити порушника, або виникають інциденти без прямої вини користувача. Наприклад, уразливість у застарілому CRM дозволяє стороннім особам отримати доступ до бази клієнтів без зламу – через недбалість IT-відділу.

– Неналежний моніторинг та реагування. Якщо система не фіксує спроби несанкціонованого доступу або не сповіщає про них, то подальші порушення можуть бути виявлені із запізненням або взагалі не виявлені. Це може бути не провина працівника, а відсутність належної інфраструктури моніторингу (SIEM, логування).

– Культура замовчування проблем. Якщо в компанії не заохочується повідомлення про вразливості або помилки, а працівників карають за ініціативу – це створює токсичне середовище, в якому помилки або навіть порушення

залишаються без реагування. Наприклад, розробник не повідомив про критичний баг у захисті даних, бо раніше колегу звільнили за подібне «втручання».

У таких випадках інциденти є результатом системних недоліків, а не індивідуальної недбалості. Це підтверджує важливість впровадження етичних політик, технічного аудиту, регулярних інструктажів і відкритої культури відповідальності в ІТ-командах.

11.6 Профілактика та етичне попередження кіберінцидентів

Етична відповідальність ІТ-фахівців не обмежується реагуванням на порушення – важливо впроваджувати проактивні заходи, спрямовані на запобігання кіберінцидентам. Це вимагає не лише технічних практик, а й формування культури відповідальності, прозорості та обізнаності щодо ризиків у всій команді.

11.6.1 Побудова культури безпеки в ІТ-компанії

Культура безпеки – це не сукупність політик, а глибинна норма поведінки в команді, де кожен розуміє свою роль у захисті даних і систем. Вона ґрунтується на трьох ключових рівнях:

– освітній рівень – регулярні тренінги з інформаційної безпеки, навчання щодо фішингу, етика взаємодії з персональними даними.

– поведінковий рівень – закріплення звичок, наприклад, не залишати робоче місце без блокування; не перекидати паролі в месенджерах; перевіряти дозволи перед завантаженням нового ПЗ.

– організаційний рівень – прозорі процедури реагування на інциденти, заохочення повідомлень про підозрілу активність (анонімно, без страху покарання), підтримка внутрішніх ініціатив з етики.

Компанія Google у своєму проєкті Re:Work [70] визначає психологічну безпеку та відкритість у команді як основу для ефективного захисту даних.

11.6.2 Використання політик мінімального доступу, двофакторної автентифікації, Zero Trust

Етичне попередження кіберінцидентів реалізується через технічні механізми обмеження ризиків, які не лише захищають системи, а й забезпечують етичну відповідальність при делегуванні повноважень.

Політика мінімального доступу (*Principle of Least Privilege*) – це ключовий принцип безпеки, згідно з яким кожному користувачу, процесу чи додатку надається тільки той рівень доступу, який є необхідним для виконання його завдань – і не більше. Такий підхід мінімізує потенційні зловживання, знижує ризик витоку або компрометації даних, а також підвищує контроль за цифровими правами. У етичному контексті PoLP запобігає надмірній централізації повноважень, знижуючи ризик зловживань як із боку користувачів, так і системних адміністраторів, оскільки:

- кожен користувач має доступ тільки до тих ресурсів, які йому потрібні для роботи;
- захищає від зловживань, як випадкових, так і навмисних;
- ризики централізуються й легше контролюються;
- етично важливо: менше доступу – менше спокуси порушити правила.

Двофакторна автентифікація (2FA) – це метод захисту облікових записів, що передбачає використання двох різних факторів перевірки: зазвичай це комбінація чогось, що користувач знає (наприклад, пароль) і чогось, що він має (наприклад, телефон із кодом або апаратний токен). 2FA значно ускладнює несанкціонований доступ, навіть якщо пароль було скомпрометовано. З етичної точки зору, впровадження 2FA – це відповідальне рішення, яке демонструє турботу компанії про безпеку даних користувачів і зменшує ризики кіберінцидентів, оскільки:

- вимагає другого фактору: код з телефона, токена або біометрії;
- значно ускладнює компрометацію навіть при витоку пароля;
- визнається як етичний обов’язок компанії перед користувачами – захищати доступ до персональних даних.

Концепція Zero Trust (буквально – «нульової довіри») передбачає, що жоден користувач чи пристрій не повинен автоматично вважатися надійним, навіть якщо він знаходиться всередині корпоративної мережі. Доступ до ресурсів

надається лише після ретельної перевірки і відповідно до політик мінімального доступу. Zero Trust базується на постійній автентифікації, мікросегментації мережі та моніторингу поведінки користувачів. Етично ця модель сприяє прозорості, відповідальності та зниженню шкоди у випадку компрометації окремих елементів системи. Концепція Zero Trust реалізується через такі ключові принципи:

– не довіряй жодному користувачу чи пристрою за замовчуванням, навіть якщо він всередині корпоративної мережі;

– кожен запит перевіряється: хто, звідки, з якого пристрою, з яким рівнем доступу;

– підхід закріплений у NIST Zero Trust Architecture (Архітектура нульової довіри) як етична альтернатива застарілим perimeter-based системам [71].

Проактивна профілактика кіберінцидентів – це не лише інженерне завдання, а етична вимога до цифрової відповідальності. Культура безпеки, підтримана сучасними технічними стандартами, дозволяє мінімізувати людський фактор, підвищити стійкість систем і зменшити кількість порушень, що виникають через недбалість, зловживання або неосвіченість.

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

Мета – сформувати у здобувачів освіти здатність критично аналізувати практичні ситуації з порушенням етичних норм у цифровому середовищі, ідентифікувати ключові моральні дилеми, визначати відповідальність сторін та розробляти стратегії етичного реагування.

12.1 Роль кейс-аналізу в етичній підготовці ІТ-фахівця

12.1.1 Значення реальних кейсів для формування етичного мислення

- Теоретичні норми етики (чесність, відповідальність, справедливість) є загальними, але в реальному бізнесі вони часто стикаються з інтересами компанії, фінансовими обмеженнями або політичним тиском.
- Реальні кейси перетворюють абстрактні принципи на конкретні приклади, що:
  1) допомагають розвинути емпатію та бачення наслідків для різних сторін;
  2) формують здатність відстоювати професійну честь навіть під тиском;
  3) навчають мислити у категоріях ризиків і довгострокових наслідків, а не лише короткої вигоди.
- Приклади:
  1) Cambridge Analytica та Facebook (2018): незаконний збір персональних даних для політичної реклами.
  2) Uber (2016–2017): приховування витоку даних 57 млн користувачів.
  3) Volkswagen (2015): маніпуляції в софті для заниження показників викидів.

4) Boeing 737 MAX (2018–2019): приховування ризиків у програмному забезпеченні літака, що призвело до катастроф.

Усі ці кейси показують, що «невеликий компроміс із етикою» може мати катастрофічні наслідки.

12.1.2 Метод *case-based learning* в IT-освіті

– Case-based learning (навчання на прикладах) виникло у юридичній та бізнес-освіті, але нині є одним із ключових методів в IT.

– Особливості:

1) студенти не просто слухають лекцію, а обговорюють конкретну проблему;

2) є кілька «правильних» відповідей, а успіх залежить від аргументації;

3) акцент робиться на критичному мисленні та дискусії.

– Використання в IT:

1) аналіз кіберінцидентів (наприклад, атака на Equifax, 2017);

2) обговорення конфліктів інтересів (наприклад, продаж даних користувачів без згоди);

3) оцінка технологічних інновацій (етика ШІ, автономні авто, біометричні бази даних).

12.2 Методика «етичного трикутника»: обов'язки – наслідки – чесноти

Методика дозволяє структурувати аналіз будь-якої ситуації.

– Обов'язки (deontology):

1) Які закони, професійні стандарти, корпоративні політики діють?

2) Приклади: GDPR (Європа), ISO 27001 (інформаційна безпека), кодекс ACM (Association for Computing Machinery).

– Наслідки (consequentialism):

1) Які будуть коротко- та довгострокові наслідки для різних сторін: компанії, користувачів, суспільства?

2) Чи буде шкода більшою, ніж користь?

– Чесноти (virtue ethics):

1) Чи відповідає поведінка спеціаліста якостям «доброчесного професіонала» – чесність, сміливість, відповідальність, справедливість?

2) Приклади: викривачі (whistleblowers) – Сноуден, Маннінг, які поставили суспільну відповідальність вище за інструкції.

Завдяки цій методиці студенти вчаться розглядати ситуацію не однобоко (лише «законно/незаконно»), а комплексно.

12.3 Розгляд вигаданих ситуацій (workshop)

Ситуація 1: Прихована вразливість

Розробник знає, що в продукті є «дірка», яка може призвести до витоку даних, але менеджер наказує ігнорувати проблему до релізу.

- Обов’язки: захист даних клієнта.
- Наслідки: можливий витік → втрата довіри → збитки.
- Чесноти: чесність, відповідальність перед користувачами.

Ситуація 2: Монетизація персональних даних

Стартап планує продавати дані користувачів рекламним компаніям без явної згоди.

- Обов’язки: дотримання GDPR.
- Наслідки: короткостроковий прибуток, але репутаційні та юридичні ризики.
- Чесноти: справедливість, повага до приватності.

Ситуація 3: Алгоритм зі зміщенням

ШІ для рекрутингу відхиляє резюме жінок частіше, ніж чоловіків, через навчальні дані.

- Обов’язки: уникнення дискримінації.
- Наслідки: соціальна несправедливість, юридичні позови.
- Чесноти: справедливість, рівність.

Ситуація 4: Лояльність до компанії чи суспільства

Інженер дізнається, що продукт може бути використаний у військових операціях із сумнівними цілями.

– Обов’язки: слідувати контракту чи захистити суспільство?

– Наслідки: кар’єрні втрати чи моральна провина.

– Чесноти: мужність, гуманізм.

Висновки

– Реальні кейси – це дзеркало ІТ-практики, що показує розрив між «кодексом честі» та бізнес-реальністю.

– Аналіз етичних ситуацій формує професійну ідентичність ІТ-фахівця.

– Методика «етичного трикутника» – універсальний інструмент для балансування між законом, наслідками та цінностями.

– Етична відповідальність у цифрову епоху – це не тільки репутація компанії, але й довіра суспільства до технологій.

ПЕРЕЛІК ВИКОРИСТАНИХ 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)

26. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. *OECD.* URL: https://www.oecd.org/en/publications/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data_9789264196391-en.html (дата звернення: 11.07.2025)

27. Про захист фізичних осіб у зв'язку з обробкою персональних даних та про вільний рух таких даних, а також про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних): Регламент (ЄС) 2016/679 Європейського парламенту та Ради від 27 квітня 2016 року. *Офіційний вісник*

Європейського Союзу. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679 (дата звернення: 11.07.2025)

28. EDPB news. *EDPB.* URL: https://www.edpb.europa.eu/news/news_en?news_type=2&field_edpb_member_state_target_id=All (дата звернення: 11.07.2025)

29. The Principles for Digital Development: a compass for those working to promote sustainable and inclusive development in today's complex digital landscape. *Principles for Digital Development.* URL: https://digitalprinciples.org/ (дата звернення: 11.07.2025)

30. Проект Закону про захист персональних даних від 11.02.2025 № 4229-IX. *Законодавство України.* URL: https://itd.rada.gov.ua/billinfo/Bills/Card/40707 (дата звернення: 11.07.2025)

31. Технологія OpenPGP. *OpenPGP.* URL: https://www.openpgp.org/ (дата звернення: 11.07.2025)

32. Загальний регламент про захист даних (GDPR) / Стаття 32 GDPR. Безпека обробки. *Proton.* URL: https://gdpr.eu/article-32-security-of-processing/ (дата звернення: 11.07.2025)

33. Zero-knowledge Proofs. *IBM.* URL: https://research.ibm.com/projects/zero-knowledge-proofs (дата звернення: 11.07.2025)

34. Solid: Your data, your choice. *Solid.* URL: https://solidproject.org/about (дата звернення: 11.07.2025)

35. Databox – інфраструктура з урахуванням конфіденційності для управління персональними даними. *Дослідження цифрової економіки Horizon.* URL: https://www.horizon.ac.uk/project/databox/ (дата звернення: 11.07.2025)

36. MyData Global. URL: https://mydata.org/about/purposes-principles/ (дата звернення: 11.07.2025)

37. Європейський закон про управління даними. *European Commission.* URL: https://digital-strategy.ec.europa.eu/en/policies/data-governance-act (дата звернення: 11.07.2025)

38. Закон про дані. *European Commission.* URL: https://digital-strategy.ec.europa.eu/en/policies/data-act (дата звернення: 11.07.2025)

39. Загальний регламент про захист даних (GDPR). *Proton.* URL: https://gdpr.eu/tag/gdpr/ (дата звернення: 11.07.2025)

40. Barbulescu v. Romania і нові тенденції в захисті персональних даних. *Інформаційне агенство «ЛІГА:ЗАКОН».* URL: https://jurliga.ligazakon.net/news/139955_barbulescu-v-romania--nov-tendents-v-zakhist-personalnikh-danikh (дата звернення: 11.07.2025)

41. Mass surveillance exposed by Snowden ‘not justified by fight against terrorism’. *Guardian News & Media.* URL: https://www.theguardian.com/world/2014/dec/08/mass-surveillance-exposed-edward-snowden-not-justified-by-fight-against-terrorism (дата звернення: 12.07.2025)

42. Machine Bias. *ProPublica.* URL: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing (дата звернення: 13.07.2025)

43. Robot Eyes Wide Shut: Understanding Dishonest Anthropomorphism. *ACM Journals.* URL: https://dl.acm.org/doi/10.1145/3287560.3287591 (дата звернення: 13.07.2025)

44. Ethics guidelines for trustworthy AI / Етичні принципи для надійного штучного інтелекту. *European Commission.* URL: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai (дата звернення: 13.07.2025)

45. ЄС ухвалив перший у світі закон про штучний інтелект: що в ньому прописали. *UNIAN.* URL: https://www.unian.ua/techno/yes-uhvaliv-pershiy-u-sviti-zakon-pro-shtuchniy-intelekt-shcho-v-nomu-propisali-12572565.html (дата звернення: 13.07.2025)

46. Міжнародний пакт про громадянські і політичні права: Генеральна Асамблея ООН від 16 грудня 1966 року. *Законодавство України.* URL: https://zakon.rada.gov.ua/laws/show/995_043#Text (дата звернення: 13.07.2025)

47. Конвенція про захист осіб у зв’язку з автоматизованою обробкою персональних даних. Страсбург, 28 січня 1981 року. *Законодавство України.*

URL: https://zakon.rada.gov.ua/laws/show/994_326#Text (дата звернення: 13.07.2025)

48. NIST Privacy Framework : a Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0. *NIST Privacy Framework.* January 16, 2020. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf (дата звернення: 13.07.2025)

49. Recommendation on the Ethics of Artificial Intelligence. France, UNESCO 2022. URL: https://unesdoc.unesco.org/ark:/48223/pf0000381137 (дата звернення: 13.07.2025)

50. Автономні та інтелектуальні системи (AIS). *Цифрова бібліотека IEEE Xplore.* URL: https://standards.ieee.org/initiatives/autonomous-intelligence-systems/ (дата звернення: 13.07.2025)

51. Діпфейки і ботоферми Трампа: як штучний інтелект ледь не зірвав президентські вибори у США. *24 Канал.* URL: https://24tv.ua/vibori-prezidenta-ssha-2024-yak-vplinuv-shtuchniy-intelekt-rezultati_n2683098 (дата звернення: 16.07.2025)

52. Як змусити вас повірити, що Земля пласка. Розбираємо технологію / Бульбашка YouTube. Інсайдерський Telegram. *Українська правда.* URL: https://www.pravda.com.ua/articles/2020/06/3/7254228/ (дата звернення: 16.07.2025)

53. ISO/IEC JTC 1/SC 42 Штучний інтелект. *ISO.* URL: https://www.iso.org/committee/6794475.html (дата звернення: 16.07.2025)

54. Deceptive Patterns. *Testimoniun.* URL: https://www.deceptive.design/ (дата звернення: 16.07.2025)

55. Огляд WCAG 2. *W3C Web Accessibility Initiative (WAI). Стратегії, стандарти та допоміжні ресурси, щоб зробити Інтернет доступним для людей з обмеженими можливостями.* URL: https://www.w3.org/WAI/standards-guidelines/wcag/ (дата звернення: 16.07.2025)

56. Інклюзивний дизайн Microsoft. *Microsoft.* https://inclusive.microsoft.design/ (дата звернення: 16.07.2025)

57. Проектування з моральною та технічною уявою. *VSD Lab.* URL: https://vsdesign.org/ (дата звернення: 16.07.2025)

58. Дональд Салл, Чарльз Салл, Бен Цвейг. Токсична культура є рушійною силою Великої відставки. *ACMP NOR CAL.* URL: https://www.acmpnorcalchapter.org/changemanagement-articles/2022/1/26/toxic-culture-is-driving-the-great-resignation (дата звернення: 16.07.2025)

59. Конвенція про кіберзлочинність (Будапештська конвенція, ETS No 185) та протоколи до неї. *Council of Europe.* URL: https://www.coe.int/en/web/cybercrime/the-budapest-convention (дата звернення: 17.07.2025)

60. Звіт про розслідування витоків даних за 2025 рік. *Verizon.* URL: https://www.verizon.com/business/resources/reports/dbir/ (дата звернення: 17.07.2025)

61. Витік даних Yahoo 2013 вдарив по «всіх трьох мільярдах облікових записів». *BBC.* URL: https://www.bbc.com/news/business-41493494 (дата звернення: 17.07.2025)

62. Кібератака на Dyn 2016 року: огляд. *Network Encyclopedia.* URL: https://networkencyclopedia.com/the-2016-dyn-cyberattack-an-overview/ (дата звернення: 17.07.2025)

63. Google і Facebook обдурили у величезній «афері». *BBC.* URL: https://www.bbc.co.uk/news/technology-39744007 (дата звернення: 17.07.2025)

64. Вірус WannaCry пошкодив комп'ютери у 99 країнах світу. *BBC.* URL: https://www.bbc.com/ukrainian/features-39907984 (дата звернення: 17.07.2025)

65. Врегулювання витоку даних Equifax: що варто знати. *FTC.* URL: https://consumer.ftc.gov/consumer-alerts/2019/07/equifax-data-breach-settlement-what-you-should-know (дата звернення: 17.07.2025)

66. Чому автоматизований інструмент найму Amazon дискримінує жінок. *American Civil Liberties Union.* URL: https://www.aclu.org/news/womens-rights/why-amazons-automated-hiring-tool-discriminated-against (дата звернення: 17.07.2025)

67. Як Uber обманює владу по всьому світу. *The New York Times.* URL: https://www.nytimes.com/2017/03/03/technology/uber-greyball-program-evade-authorities.html (дата звернення: 17.07.2025)

68. Цивільний кодекс України від 16 січня 2003 року № 435-IV. *Законодавство України.* URL: https://zakon.rada.gov.ua/laws/show/435-15#Text (дата звернення: 17.07.2025)

69. Кодекс законів про працю України. *Законодавство України.* URL: https://zakon.rada.gov.ua/laws/show/322-08#Text (дата звернення: 17.07.2025)

70. Make work better. *Google re:Work.* URL: https://rework.withgoogle.com/en/ (дата звернення: 17.07.2025)

71. Zero Trust Architecture. *NIST Special Publication 800-207.* URL: https://www.nist.gov/publications/zero-trust-architecture (дата звернення: 17.07.2025)

ДЛЯ НОТАТОК

У П-73 Професійна етика в ІТ-сфері: конспект лекцій 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. 172 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