УДК 004.056:174 **DOI:10.30837/rt.2025.4.223.12**

М.О. ЄВДОКИМЕНКО, д-р техн. наук, В.Х. ЧАКРЯН, канд. техн. наук,
В.В. ЄВДОКИМЕНКО

ЕТИЧНІ ЗАСАДИ ТА НОРМАТИВНЕ РЕГУЛЮВАННЯ ПРОФЕСІЙНОЇ ДІЯЛЬНОСТІ В СФЕРІ КІБЕРБЕЗПЕКИ: МІЖНАРОДНІ СТАНДАРТИ, УКРАЇНСЬКИЙ КОНТЕКСТ І ПРАКТИЧНІ ОРІЄНТИРИ

Вступ

У добу цифрової трансформації питання етики в сфері кібербезпеки набуває особливої актуальності. Зі зростанням залежності суспільства від інформаційних технологій, відповідальність за їхній захист стає не лише технічною, але й моральною проблемою. Кожен інцидент порушення конфіденційності, витоку даних чи неправомірного моніторингу викликає резонанс не лише в професійному середовищі, але й у суспільстві в цілому. Кібербезпека більше не обмежується шифруванням, фаєрволами чи реагуванням на інциденти – вона – вимагає етичної свідомості та стратегічного мислення.

Особливої ваги це набуває у сферах, де обробляються критично чутливі дані: охорона здоров'я, фінанси, енергетика, освіта. У подібних випадках від дій спеціаліста з кібербезпеки залежить не лише цілісність інформації, а й добробут, права і навіть життя людей. Професійна етика тут визначає межу між захистом і порушенням приватності.

Крім того, із впровадженням концепцій "Zero Trust", "Data Sovereignty", "Digital Identity" тощо, фахівець з кібербезпеки все частіше виступає не просто адміністратором системи, а агентом впливу на політику конфіденційності, прозорості та управління цифровими ризиками. Саме тому питання етики має розглядатися як фундаментальний елемент професійної компетентності, поряд із технічними знаннями.

Складність етичних дилем також зумовлюється багатоаспектністю ситуацій: від легітимності соціальної інженерії в тестуванні до повідомлення про вразливості в умовах національної безпеки. У таких випадках не існує однозначно правильного рішення без врахування правової, технічної та етичної площин.

Водночас нормативно-правове забезпечення діяльності у сфері кібербезпеки ще не завжди враховує динамічні зміни цифрового середовища. Багато міжнародних стандартів – таких як ISO/IEC 27001 [1], ISO/IEC 27032 [2] – лише окреслюють загальні рамки поведінки, залишаючи багато етичних питань відкритими для тлумачення.

Україна, яка стрімко впроваджує європейські принципи цифрової безпеки та прагне до кіберстійкості, потребує формування зрозумілої етичної моделі для підготовки професіоналів. Ця модель має включати як елементи права, так і м'які навички прийняття рішень в умовах невизначеності.

Таким чином, актуальність дослідження етичних засад діяльності у сфері кібербезпеки зумовлена необхідністю формування довіри до цифрової екосистеми, запобігання зловживанням владними повноваженнями фахівців, та забезпечення балансу між безпекою і правами людини.

Це дослідження спрямоване на систематизацію ключових етичних проблем, аналіз нормативної бази та розробку практичних орієнтирів для майбутніх фахівців. Його результати можуть бути використані у навчальному процесі, при підготовці політик інформаційної безпеки та у міждисциплінарних дослідженнях кіберетики.

Етичні основи професійної діяльності

Робота фахівця з кібербезпеки вимагає постійного балансу між захистом цифрових активів та дотриманням прав і свобод людини. У цифрову епоху, коли приватна інформація може бути зібрана, оброблена, збережена або скомпрометована за лічені секунди, етична

відповідальність спеціаліста виходить далеко за рамки технічної компетентності. Це зобов'язання перед суспільством, роботодавцем, клієнтами та самою професією.

Основні етичні принципи, що мають бути дотримані в професійній діяльності фахівця з кібербезпеки, представлені на рис. 1.

Конфіденційність	**Цілісність**	**Підзвітність**	**Справедливість**
Зобов'язання зберігати інформацію, до якої є доступ, в таємниці, не допускаючи її розголошення без дозволу.	Вимога діяти чесно, не спотворюючи інформацію та не маніпулюючи результатами.	Готовність пояснити свої дії і не перекладати відповідальність на інших.	Рівне ставлення до всіх користувачів та недопущення упередженості, дискримінації чи зловживань.

Рис. 1. Основні етичні принципи

На практиці ці принципи мають бути вбудовані в щоденну діяльність: від аналізу журналів подій до роботи з персональними даними користувачів. Наприклад, навіть якщо фахівець з кібербезпеки має технічну можливість доступу до приватної інформації (медичної документації, листування працівників, історії фінансових транзакцій тощо), він не має морального права використовувати ці знання поза межами своєї функції.

У відповідь на потребу в етичній регуляції в сфері IT та кібербезпеки, провідні професійні організації розробили відповідні кодекси поведінки.

Одним із найвпливовіших є (ISC)² Code of Ethics [3], який базується на чотирьох основних канонах:

1. Захищати суспільство, загальне благо, довіру та інфраструктуру.
2. Чесно виконувати свої обов'язки та діяти у найкращих інтересах клієнта.
3. Забезпечувати чесну та законну поведінку у професійній діяльності.
4. Підтримувати та вдосконалювати свою професійну компетентність.

Кожен сертифікований спеціаліст (наприклад, власник сертифіката CISSP) зобов'язаний неухильно дотримуватись цього кодексу. Його порушення може призвести до дисциплінарного розгляду і навіть втрати сертифікату.

Іншим авторитетним джерелом є ACM Code of Ethics and Professional Conduct [4], прийнятий Асоціацією обчислювальної техніки (Association for Computing Machinery). Він базується на таких принципах:

- діяти на благо суспільства і людства;
- уникати заподіяння шкоди;
- бути чесним і прозорим;
- поважати конфіденційність та приватність інших осіб;
- покращувати технічну компетентність і відповідати за свою діяльність.

ACM Code of Ethics передбачає як загальні моральні принципи, так і специфічні вказівки для фахівців у галузі розробки ПЗ, інформаційних систем та кібербезпеки. Наприклад, в ньому наголошується, що спеціалісти повинні уникати будь-якої діяльності, яка може завдати шкоди іншим, навіть якщо вона не є прямо забороненою законом.

Проте, попри наявність таких кодексів, у сфері кібербезпеки залишається чимало сірих зон. Зокрема, відсутність універсального міжнародного стандарту етики призводить до неоднозначного трактування ролі спеціаліста в умовах кібервійни, кіберспостереження чи роботи у приватному секторі. Також бракує чітких механізмів моніторингу та контролю етичної поведінки в професійній спільноті.

У зв'язку з цим, важливо не лише популяризувати наявні етичні кодекси, а й інтегрувати етику в системи підготовки фахівців, внутрішні політики компаній і процедури оцінки діяльності. Це дозволить зробити етику невід'ємною частиною цифрової безпеки, а не формальною декларацією.

Таким чином, етичні основи є не лише засадничою складовою професійної репутації, а й фактором підвищення стійкості кіберпростору в цілому.

Відповідальність і цифрова довіра

Цифрова довіра (digital trust) є фундаментальним елементом у сфері кібербезпеки, яка дедалі більше впливає на економічну, правову та соціальну стабільність сучасного інформаційного суспільства. Без належного рівня довіри жодна система не може функціонувати ефективно – ані технологічна, ані організаційна. Відповідальність фахівця з кібербезпеки охоплює не лише захист систем і даних, а й забезпечення прозорості, правомірності та етичності в кожній операції, пов'язаній із цифровими активами.

Центральним концептом, що лежить в основі цифрової довіри, є "надійна поведінка" (trustworthy behavior), яка поєднує правову відповідальність, професійну етику та дотримання міжнародних стандартів (наприклад, ISO/IEC 27001, ISO/IEC 27701). Принципи прозорості, достовірності, відповідальності (accountability), доступності, конфіденційності та мінімізації втручання формують основу цифрової довіри в контексті діяльності як окремого фахівця, так і організації загалом.

Один із ключових аспектів відповідальності полягає у своєчасному розкритті інцидентів. Замовчування зламів або компрометацій є серйозним етичним і правовим порушенням, що прямо шкодить довірі з боку клієнтів, партнерів та держави. Прикладом стала ситуація з Uber у 2016 р., коли компанія приховала факт витоку персональних даних понад 57 мільйонів користувачів і водіїв, заплативши хакерам за мовчання. Це порушення як законодавства з питань захисту персональних даних, так і фундаментальних етичних норм взаємодії з користувачами.

Концепція цифрової довіри передбачає також впровадження політики "ethics by design" – тобто закладення етичних принципів безпосередньо в архітектуру IT-рішень, алгоритмів та інтерфейсів взаємодії. Це означає не лише створення безпечного продукту, але і такого, що враховує приватність користувача, справедливий розподіл повноважень, і відсутність дискримінаційних моделей доступу чи контролю.

Іншим важливим підходом є "accountable cybersecurity" – концепція, згідно з якою кожен суб'єкт, залучений у процес управління безпекою, несе не лише технічну, але і юридичну відповідальність за прийняті рішення та їх наслідки. Такий підхід вимагає ведення чіткої документації, звітності, регулярного перегляду рішень та етичних аудитів (наприклад, шляхом впровадження внутрішніх кодексів поведінки, незалежних комітетів з етики та наглядових рад).

Не менш важливим є забезпечення відповідності принципам "data stewardship" – етичного управління даними, яке передбачає, що доступ до інформації здійснюється лише на основі чітко визначеної мети, з належними дозволами, із дотриманням принципу мінімізації збирання та обробки. Будь-яка маніпуляція з даними поза рамками призначення – наприклад, моніторинг листування працівників без юридичних підстав – прямо підриває цифрову довіру та порушує фундаментальні права особи.

Цифрова довіра також є предметом регуляторного нагляду. Наприклад, Загальний регламент захисту даних (GDPR) [5] вимагає обов'язкового повідомлення про витоки протягом 72 годин. Аналогічні вимоги включено у новітні директиви ЄС з кіберстійкості (наприклад, NIS 2 Directive) [6] та відповідні нормативні акти у США (як-от SEC Cybersecurity Rules) [7].

Слід також підкреслити роль культури відповідальності в організаціях. Етична поведінка не може бути забезпечена виключно технічними засобами – вона формується через інституційну культуру, де працівники отримують чіткі інструкції, навчання, мають канали для повідомлення про порушення без ризику репресій (whistleblowing policies), а також доступ до незалежного етичного консультанта.

Інноваційною концепцією є також впровадження довіри на основі блокчейн-рішень – auditability and transparency by design. Наприклад, зберігання логів подій у незмінному вигляді на блокчейні унеможливлює їх фальсифікацію та дозволяє здійснювати незалежну перевірку без компрометації джерела.

Крім того, актуальними залишаються питання відповідальності у випадку використання штучного інтелекту в безпеці: як бути, якщо рішення про блокування доступу було прийняте автоматичною системою, яка мала помилкові вхідні дані або містить упередженість у моделях? Це вимагає розробки чіткої процедури оскарження рішень (algorithmic accountability), які б дозволяли людині відновити свої права.

Отже, цифрова довіра не є абстрактним поняттям, а системою взаємопов'язаних етичних, правових та організаційних рішень, що впроваджуються в щоденну практику кіберзахисту. Вона вимагає усвідомлення відповідальності, постійного етичного рефлексування та розвитку систем внутрішнього контролю. Успішний фахівець з кібербезпеки має бути не лише технічно грамотним, а й морально відповідальним – здатним приймати рішення, які водночас захищають систему та поважають гідність особистості.

Саме тому, у контексті зростаючого значення цифрової довіри та професійної відповідальності особливого значення набуває нормативне закріплення етичних принципів у міжнародних та національних стандартах. Впровадження таких стандартів дозволяє формалізувати етичні вимоги до фахівців з кібербезпеки, забезпечити єдині правила взаємодії в цифровому середовищі, а також створити основу для механізмів оцінювання, сертифікації та нагляду за дотриманням професійної етики. Наступний розділ буде присвячено аналізу ключових етичних та професійних стандартів, прийнятих у США, ЄС та Україні, а також їх ролі у формуванні цифрової відповідальності в глобальному контексті.

Інституціональні та нормативні засади цифрової етики

У сучасному цифровому середовищі, де кіберзагрози набувають все більш витончених форм, а обсяг чутливих даних стрімко зростає, потреба в чітких нормативно-правових регулюваннях стає надзвичайно актуальною. Етика в галузі кібербезпеки не може залишатися суто моральною категорією – вона має отримати правову інституціалізацію. З огляду на міждержавний характер Інтернету, важливо враховувати як національні законодавства, так і міжнародні стандарти, що встановлюють правила поведінки для фахівців з кібербезпеки. Особливо вагому роль у цьому контексті відіграють підходи Європейського Союзу та Сполучених Штатів Америки, які стали прикладами для впровадження етичних рамок на інституційному рівні. Ці стандарти визначають не лише технічні вимоги до безпеки, а й засади цифрової етики, відповідальності та прозорості. Вони мають імплементаційний вплив на організаційну культуру підприємств, освітні програми, державну політику у сфері цифрової трансформації. Дотримання таких норм є не лише показником професіоналізму, а й передумовою легітимності та суспільної довіри до цифрових рішень. У цьому розділі ми детально розглянемо, як побудована система етичних стандартів у ЄС та США, які принципи лежать в її основі та як вони реалізуються на практиці. Цей аналіз дозволяє виявити сильні сторони та потенційні напрями вдосконалення нормативно-правового поля в Україні з урахуванням кращих міжнародних практик.

Етичні стандарти та цифрова довіра: порівняльний аналіз підходів ЄС та США

Європейський Союз та Сполучені Штати Америки виступають провідними юрисдикціями у формуванні етичної інфраструктури для цифрового суспільства. Обидві системи враховують фундаментальні права людини, забезпечення цифрової довіри та відповідальність професійної спільноти.

В ЄС основною нормативною опорою для етичних принципів у цифровій сфері є Загальний регламент захисту даних (General Data Protection Regulation, GDPR), який встановлює високі стандарти прозорості, підзвітності та прав суб'єктів даних. Окрім суто правових вимог, GDPR формує культурний стандарт – розуміння, що обробка даних є не лише технічною, а й етичною дією. До регламенту додано принципи "privacy by design" та "privacy by default", що змушують компанії закладати етичні підходи вже на етапі розробки продуктів.

Європейська комісія також ініціювала створення Етичних настанов зі штучного інтелекту (Ethics Guidelines for Trustworthy AI, 2019) [8], які визначають 7 ключових вимог до систем ШІ: зокрема, людський контроль, технічну надійність, конфіденційність та підзвітність. Ці настанови стали основою для майбутнього законодавства про AI Act.

Крім того, у рамках ініціативи Digital Europe та Cybersecurity Act, ЄС просуває ідею сертифікації спеціалістів і рішень, в яких етичні принципи становлять обов'язковий компонент [9]. Так, сертифікати відповідності вимагають не лише технічної безпеки, а й відповідності етичним нормам та доброчесності.

На рівні професійних об'єднань Європейський Союз підтримує розробку етичних кодексів для фахівців з кібербезпеки, наприклад, рекомендації ENISA (Агентство ЄС з кібербезпеки) щодо стандартів поведінки та рішень у сфері кіберризиків. ENISA підтримує створення стандартів на основі компетентностей та етики, включаючи рекомендації щодо кар'єрного шляху та етичного лідерства [10].

У США ключовим документом у сфері цифрової етики вважається ACM Code of Ethics and Professional Conduct (Кодекс етики та професійної поведінки Асоціації обчислювальної техніки), який зобов'язує спеціалістів діяти в інтересах суспільства, дотримуватись чесності, поважати конфіденційність і уникати шкоди. Кодекс є обов'язковим для всіх членів ACM і часто включається до навчальних програм з IT.

Ще один важливий документ – (ISC)² Code of Ethics, розроблений Міжнародним консорціумом сертифікованих спеціалістів з безпеки інформаційних систем. Цей кодекс чітко формулює чотири основні принципи: захист суспільства, чесність і справедливість, повага до довіри та обов'язок до розвитку знань. Він обов'язковий для всіх сертифікованих спеціалістів CISSP, SSCP, CCSP та інших.

У США також діє NIST Cybersecurity Framework [11], який не є кодексом етики, але включає положення щодо забезпечення відповідальності, прозорості та етичного управління ризиками. Рамка містить компоненти "Govern" та "Identify", які стосуються етичної оцінки впливу технологій і обліку інтересів користувача.

Важливо відзначити, що американські компанії часто створюють внутрішні етичні комітети, особливо у великих корпораціях, які працюють з персональними даними або штучним інтелектом. Така практика вважається "best practice" в управлінні цифровими ризиками.

Таким чином, як ЄС, так і США демонструють багаторівневий підхід до етичного регулювання цифрового середовища – від загальних правових рамок до галузевих і професійних стандартів. Ці моделі є прикладом інтеграції етики в усі етапи життєвого циклу цифрових систем – від архітектурного дизайну до повсякденного використання. Україна, адаптуючи свої підходи до етичного врядування в ІКТ, може скористатися цими прикладами як основою для побудови власної національної системи цифрової етики.

Етичні норми та цифрова довіра в українському законодавстві

У контексті цифрової трансформації держави, побудови інформаційного суспільства та активної інтеграції у європейський кіберпростір, Україна поступово формує нормативно-правову базу, що включає етичні засади й принципи цифрової довіри. Хоча більшість українських законів не містять терміну "етика" у формальному визначенні, багато з них прямо чи опосередковано закладають фундамент етичної поведінки у сфері інформаційних технологій і кібербезпеки.

Закон України "Про національну безпеку" № 2469-VIII (2018) прямо визначає кібербезпеку як невід'ємну складову національної безпеки [12]. У Стратегії національної безпеки України акцент зроблено на необхідності формування культури довіри до цифрових сервісів і забезпечення захисту прав громадян у кіберпросторі.

Закон України "Про основні засади забезпечення кібербезпеки України" № 2163-VIII (2017) містить визначення кібербезпеки як стану захищеності кіберпростору та інтересів

особи, суспільства й держави [13]. У законі закладено принципи законності, пропорційності втручання, поваги до прав людини, конфіденційності та добросовісності, які відповідають етичним стандартам демократичних країн.

Закон України "Про захист персональних даних" № 2297-VI (2010, в останній редакції 2022 р.) є ключовим актом, що гарантує право на приватність [14]. Він встановлює підзвітність операторів персональних даних, принципи цільовості, пропорційності, обмеження строку зберігання даних, заборону на обробку чутливої інформації без згоди суб'єкта. Норма про обов'язок уповноваженої особи із захисту даних узгоджується з європейським підходом до етичного управління даними (GDPR).

Закон України "Про електронні комунікації" № 1089-IX (2020) встановлює правові засади діяльності провайдерів, у тому числі щодо захисту прав споживачів, прозорості умов надання послуг, а також контролю за OTT-сервісами (Over-the-top) [15]. Він містить положення про обов'язкове дотримання принципу недискримінації, забезпечення конфіденційності та безпеки електронних повідомлень.

Закон України "Про інформацію" № 2657-XII (1992, чинна редакція) визначає правові засади доступу, поширення, обробки інформації, зокрема принципи достовірності, відкритості, об'єктивності. Стаття 5 закріплює право на приватність і обов'язок не допускати порушення інформаційної безпеки [16]. Закон регламентує етичні аспекти обробки інформації, обмежуючи зловживання владою, пропаганду ворожнечі та втручання в особисте життя.

Закон України "Про електронні довірчі послуги" № 2155-VIII (2017) встановлює поняття довіри в цифровому середовищі через інституалізацію електронного підпису, електронної печатки, часових міток, сертифікації послуг [17]. В основі лежить принцип правової визначеності та цілісності інформації, що передбачає етичну відповідальність постачальників послуг перед користувачами.

Закон України "Про публічні електронні реєстри" № 2170-IX (2022) запроваджує стандарти надійності, прозорості та захисту даних у роботі державних інформаційних систем [18]. Закон визначає вимоги до забезпечення захисту персональної інформації в реєстрах та встановлює критерії етичного управління державними даними, зокрема щодо мінімізації збору, обмеження доступу та контролю на основі ризик-орієнтованого підходу.

Закон України "Про відкритість використання публічних коштів" № 183-VIII (2015) хоча і не стосується напряму ІКТ, але встановлює принципи прозорості, підзвітності та недопущення зловживань, що є базовими категоріями цифрової етики при адмініструванні електронних систем закупівель, бюджетного контролю тощо [19].

Законопроєкт "Про захист критичної інформаційної інфраструктури" (в процесі ухвалення) передбачає створення нормативних механізмів для управління ризиками, прозорого аудиту та відповідального поводження з технологіями в об'єктах критичної інфраструктури [20].

Окрім законів підзаконні акти та стратегії, такі як "Національна стратегія з кібербезпеки України" (Указ Президента № 47/2021) [21], Стратегія цифрової трансформації сектору безпеки й оборони (2022) [22], програма "Дія.Цифрова держава", акти КМУ та Держспецзв'язку закріплюють засади етичного поводження з даними, необхідність дотримання принципів "security by design" і "privacy by design".

Також Методичні рекомендації НАЗК щодо доброчесності у державному секторі прямо включають принципи прозорості, добросовісності, етичного врядування, що застосовні і до цифрових сервісів.

У сфері освіти, стандарти вищої освіти зі спеціальності "Кібербезпека" (галузь знань 12) затверджені МОН, містять компонент етичної поведінки та правових знань як обов'язкову складову професійної підготовки. Студенти повинні демонструвати здатність діяти етично в ситуаціях, пов'язаних з обробкою конфіденційної інформації, тестуванням безпеки та взаємодією з особистими даними.

На рівні професійних об’єднань, як-от IT Ukraine Association, ISACA Kyiv Chapter, Ukrainian Cyber Alliance, також діють ініціативи щодо розробки професійних стандартів поведінки, кодексів доброчесності, антикорупційних положень та норм захисту цифрових прав.

Отже, українське законодавство поступово формує системну етичну рамку для функціонування цифрового середовища, базуючись на таких принципах як прозорість, підзвітність, недискримінація, безпека і повага до прав людини. Проте відчутною є потреба в консолідації норм, прийнятті національного кодексу етики для кіберфахівців і гармонізації із міжнародними підходами. Наступним логічним кроком у цьому напрямку є формування етичних стандартів, які стали б обов’язковими в сертифікації, публічних закупівлях та акредитації цифрових послуг.

Перспективи гармонізації етичних та правових підходів України з моделями ЄС і США

В умовах стратегічного курсу України на євроінтеграцію та розвиток цифрової держави особливого значення набуває гармонізація національного правового поля з етичними стандартами, що діють у Європейському Союзі та Сполучених Штатах Америки. Відповідність таким стандартам не лише сприятиме інтеграції у спільний цифровий ринок ЄС, а й підвищить загальний рівень довіри до українських IT- та кібербезпекових рішень.

Першочерговим напрямом має стати повноцінна імплементація принципів GDPR (General Data Protection Regulation). Попри те, що Закон України «Про захист персональних даних» частково враховує окремі положення регламенту, він потребує суттєвого оновлення. Необхідно чітко закріпити обов’язок Data Protection Officer (уповноваженої особи з питань захисту даних), вимоги до обробки даних на основі згоди, право на забуття, право на доступ, портативність даних, а також ввести ефективні механізми контролю та санкцій, які мають стримувальний і превентивний характер.

Наступним кроком є розробка та впровадження національного етичного кодексу для фахівців з кібербезпеки. Такий кодекс може бути створений за зразком ACM Code of Ethics або (ISC)² Code of Ethics і включати обов’язки перед суспільством, замовниками, колегами та професією загалом. Він має стати обов’язковою складовою програм професійної сертифікації, ліцензування та державного замовлення у сфері ІКТ.

Крім того, важливим є створення системи сертифікації та нагляду за дотриманням етичних стандартів, аналогічної до практик ENISA у ЄС. Така система дозволить перевіряти не лише технічну відповідність продуктів чи послуг, але й рівень їхньої етичності – наприклад, наскільки вони враховують вимоги до конфіденційності, справедливості, недискримінації, захисту персональних даних.

Особливої уваги потребує створення механізму захисту етичних дослідників, які діють за моделлю coordinated vulnerability disclosure. У США та ЄС подібні механізми підтримуються державними інституціями, зокрема CERT, NIST, ENISA. В Україні такі ініціативи можуть бути закріплені через відповідні положення в законі про кібербезпеку або окрему постанову Кабінету Міністрів. Це дозволить захистити «білих хакерів» від кримінального переслідування за добросовісне повідомлення про вразливості.

У сфері освіти доцільним є введення обов’язкових навчальних модулів з цифрової етики у програми вищих навчальних закладів за спеціальностями «Кібербезпека», «Комп’ютерні науки», «Інженерія програмного забезпечення» тощо. Такий підхід відповідає практикам США та ЄС, де цифрова етика є стандартним компонентом підготовки IT-фахівців. Освітні стандарти мають бути доповнені компетентностями з етичного аналізу ризиків, управління конфліктами інтересів та дотримання приватності.

Ще одним напрямом є гармонізація практик захисту прав користувачів цифрових платформ. Це включає підвищення вимог до прозорості алгоритмів, використання штучного інтелекту, принципів fairness, accountability, transparency (FAT). Україна може запровадити

адаптовану версію підходів Trustworthy AI, сформованих Єврокомісією, із обов'язковим аудитом етичних наслідків IT-рішень, які впливають на поведінку користувачів або обробку даних.

Також необхідним є посилення міжвідомчої та міжнародної координації в етичній сфері. Зокрема, Україна може ініціювати приєднання до програм етичної сертифікації ENISA, участі в Global Forum on Cyber Expertise (GFCE), розвитку проєктів з ITU, OECD та Ради Європи в галузі цифрових прав.

Усі ці ініціативи мають бути об'єднані у національну стратегію цифрової етики, яка визначатиме пріоритети, принципи, механізми впровадження та оцінки ефективності. Такий документ може стати логічним продовженням Стратегії кібербезпеки України та синергією з цифровими трансформаційними проєктами «Дія», «Paperless», «Дія. Освіта» тощо.

Таким чином, узгодження українського підходу до цифрової етики з європейськими та американськими практиками є не лише доцільним, а й необхідним кроком для забезпечення довіри, прозорості та сталого розвитку цифрового середовища в Україні.

Практичні рекомендації щодо впровадження етики в діяльності фахівця з кібербезпеки

У контексті стрімкого зростання обсягів цифрових даних, активного впровадження інформаційно-комунікаційних технологій (ІКТ) та зростання ризиків кібератак особливої ваги набуває питання дотримання етичних принципів у сфері кібербезпеки. Етика фахівця з безпеки не лише формує довіру до конкретного спеціаліста, а й створює умови для стійкого цифрового розвитку суспільства загалом. Нижче запропоновано низку практичних рекомендацій, які можуть бути використані як основа для етичного врядування в галузі інформаційної безпеки.

1. Використання виключно етичних методів аудиту та тестування безпеки.

Усі форми тестування інформаційних систем, зокрема аудит, оцінка вразливостей чи проведення пентестів, повинні здійснюватися виключно за умови отримання письмового дозволу від власника інформаційної системи. Це відповідає як положенням кримінального законодавства України (зокрема, статтям 361–361-2 Кримінального кодексу), так і міжнародним стандартам етичної поведінки в галузі IT. Проведення тестувань без згоди суперечить базовим етичним принципам і може бути розцінене як незаконне втручання в роботу систем.

2. Формулювання та дотримання особистого або командного "етичного компаса".

Фахівець з кібербезпеки повинен мати чітко сформульований набір внутрішніх принципів, які допомагають приймати рішення у неоднозначних або конфліктних ситуаціях. Такий "етичний компас" має базуватися на принципах поваги до конфіденційності, прозорості, недопущення шкоди, підзвітності та дотримання справедливості. Документування цих принципів може виступати частиною внутрішнього кодексу поведінки або політики інформаційної безпеки компанії.

3. Інтеграція етичних принципів у внутрішні політики організацій.

Етичні стандарти мають бути не лише декларативними, а й імплементованими в практику через внутрішню нормативну документацію. Це стосується політик щодо моніторингу систем, обробки персональних даних, регламентів реагування на інциденти, а також протоколів взаємодії з третіми сторонами. Наприклад, контроль доступу до логів повинен бути обмежений і підзвітний, з метою запобігання несанкціонованому перегляду приватної інформації.

4. Просування етичних практик у професійному середовищі.

Більш досвідчені фахівці повинні виступати етичними наставниками для молодих спеціалістів, роз'яснюючи значення доброчесної поведінки в умовах технічної переваги. Це можливо через участь у професійних спільнотах, менторство, публічні виступи на конференціях, створення навчальних матеріалів і курсів з етики в ІКТ.

5. Використання моделі відповідального розкриття вразливостей (coordinated disclosure).

При виявленні уразливостей у сторонньому ПЗ або сервісі, фахівець повинен повідомити про неї виробника або відповідальну сторону до її публічного розголошення. Така поведінка узгоджується з рекомендаціями ISO/IEC 29147 та практиками NIST і CERT. Вона дозволяє запобігти зловживанню знайденою уразливістю третіми сторонами та зменшити ризики для користувачів.

6. Неприпустимість використання технічних знань у власних інтересах.

Фахівець повинен утримуватись від застосування знань про незакриті вразливості, обхідні шляхи автентифікації або технічні особливості системи для особистої вигоди або переваги у бізнесі. Такі дії суперечать основоположним етичним кодексам (зокрема, ACM та (ISC)²), а також підпадають під ознаки кримінальних правопорушень.

7. Просування відкритих і прозорих інструментів захисту.

Фахівці повинні популяризувати та впроваджувати у роботу open-source засоби захисту, такі як KeePass, Signal, OpenVPN, GPG, які дозволяють користувачеві самостійно переконатися у відсутності прихованих механізмів збору інформації. Це сприяє формуванню цифрової довіри та підтримці демократичних цінностей у сфері технологій.

8. Уникнення участі в сумнівних або "сірих" проєктах.

Етичний фахівець повинен відмовлятися від співпраці в проєктах, які передбачають несанкціонований доступ до даних, стеження без судового рішення, злом конкурентів або інші дії, що суперечать принципам етичної поведінки. Участь у подібній діяльності підриває репутацію як фахівця, так і галузі загалом.

9. Забезпечення пропорційного моніторингу, який не порушує приватності.

У випадках, коли необхідне ведення журналів дій користувачів або аналіз трафіку, повинні застосовуватись методи, які мінімізують втручання у приватне життя. Наприклад, знеособлення даних, скорочення терміну зберігання журналів, використання фільтрів для чутливої інформації – усе це підвищує рівень етичної відповідності.

10. Сприяння розвитку законодавчих ініціатив щодо захисту етичних дослідників.

В Україні відсутній чіткий механізм правового захисту осіб, які повідомляють про вразливості в системах (white-hat hackers). Професійна спільнота має ініціювати розробку відповідних змін до нормативної бази, які б передбачали добровільну реєстрацію тестувальників, визначення правил відповідального розкриття, а також юридичний захист при дотриманні таких правил.

Реалізація наведених рекомендацій сприятиме формуванню в Україні етичної культури у сфері кібербезпеки, яка базується на прозорості, відповідальності, недопущенні шкоди та повазі до прав людини. В умовах гібридних загроз, швидкого розвитку ШІ та цифровізації всіх сфер життя роль етики в кібербезпеці постає як ключовий компонент не лише професійної діяльності, а й стратегічного розвитку держави.

Висновки

Дослідження підтверджує, що етичні принципи є фундаментальним елементом професійної діяльності у сфері кібербезпеки, а цифрова довіра – ключовим ресурсом для сталого функціонування інформаційного суспільства. Сучасні виклики, зокрема зростання кібератак, впровадження штучного інтелекту та проблеми конфіденційності, вимагають не лише технічних рішень, а й етичної рефлексії та нормативного регулювання. Аналіз міжнародних (GDPR, ISO/IEC, ENISA, ACM, (ISC)²) та національних стандартів (українські закони про кібербезпеку, захист персональних даних, електронні комунікації) демонструє необхідність комплексного підходу до етики.

Особливу увагу слід приділяти гармонізації національного законодавства з європейськими підходами, розвитку професійної сертифікації з етичним компонентом, впровадженню етичних кодексів у компаніях і закладах освіти. Практичні рекомендації, наведені у статті, мають стати основою для формування професійної культури відповідальності, доброчесності та відкритості у сфері кіберзахисту. Подальші дослідження доцільно зосере-

дити на правовому захисті етичних дослідників, оцінці алгоритмічної справедливості та цифрових прав користувачів.

Список літератури:

1. ISO/IEC 27001:2013, Information technology – Security techniques – Information security management systems – Requirements, International Organization for Standardization, 2013.
2. ISO/IEC 27032:2012, Guidelines for cybersecurity, International Organization for Standardization, 2012.
3. (ISC)², Code of Ethics, 2023. Available at: https://www.isc2.org/Ethics.
4. Association for Computing Machinery, ACM Code of Ethics and Professional Conduct, 1992. Available at: https://dl.acm.org/doi/10.1145/129875.129885
5. General Data Protection Regulation (GDPR), European Commission, 2016. Available at: https://gdpr.eu/
6. European Parliament and Council of the European Union, Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union, 14 Dec. 2022. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555
7. U.S. Securities and Exchange Commission, Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Final Rule, Release No. 33-11216, 26 July 2023. Available at: https://www.sec.gov/rules-regulations/2023/07/s7-09-22
8. European Commission, Ethics Guidelines for Trustworthy AI, 2019. Available at: https://op.europa.eu/en/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1
9. European Parliament and Council of the European Union, Regulation (EU) 2019/881 on ENISA (the European Union Agency for Cybersecurity), 17 April 2019. Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32019R0881
10. European Union Agency for Cybersecurity (ENISA), Cybersecurity Skills Development Guidelines, 2022. Available at: https://www.enisa.europa.eu/publications/cybersecurity-skills-development
11. Pascoe C., Quinn S., and. Scarfone K. The NIST Cybersecurity Framework (CSF) 2.0 / National Institute of Standards and Technology, 26 February 2024. Available at: https://www.nist.gov/publications/nist-cybersecurity-framework-csf-20
12. Закон України № 2469-VIII. Про національну безпеку. 21 червня 2018 р. Available at: https://zakon.rada.gov.ua/laws/show/2469-19
13. Закон України № 2163-VIII. Про основні засади забезпечення кібербезпеки України. 5 жовтня 2017 р. Available at: https://zakon.rada.gov.ua/laws/show/2163-19
14. Закон України № 2297-VI. Про захист персональних даних. 1 червня 2010 р. (із змінами). Available at: https://zakon.rada.gov.ua/laws/show/2297-17
15. Закон України № 1089-IX. Про електронні комунікації. 16 грудня 2020 р. Available at: https://zakon.rada.gov.ua/laws/show/1089-20
16. Закон України № 2657-XII. Про інформацію. 2 жовтня 1992 р. (у редакції). Available at: https://zakon.rada.gov.ua/laws/show/2657-12
17. Закон України № 2155-VIII. Про електронні довірчі послуги. 5 жовтня 2017 р. Available at: https://zakon.rada.gov.ua/laws/show/2155-19
18. Закон України № 2170-IX. Про публічні електронні реєстри. 5 жовтня 2022 р. Available at: https://zakon.rada.gov.ua/laws/show/2170-20
19. Верховна Рада України. Закон України "Про відкритість використання публічних коштів" № 183-VIII, 2015. Available at: https://zakon.rada.gov.ua/laws/show/183-19
20. Верховна Рада України. Законопроєкт "Про захист критичної інформаційної інфраструктури" (в процесі ухвалення), 2023. Available at: https://itd.rada.gov.ua/bill/8475-IX
21. Президент України, Національна стратегія кібербезпеки України, Указ № 47/2021, 14 травня 2021 р. Available at: https://www.president.gov.ua/documents/472021-35721
22. Міністерство цифрової трансформації України. Стратегія цифрової трансформації сектору безпеки й оборони України (2022).

Надійшла до редколегії 17.10.2025

Відомості про авторів:

Євдокименко Марина Олександрівна – д-р техн. наук, професор, Харківський національний університет радіоелектроніки, професор кафедри Інфокомунікаційної інженерії ім. В.В. Поповського, Україна; e-mail: marina.ievdokymenko@nure.ua; ORCID: https://orcid.org/0000-0002-7391-3068

Євдокименко Владислав В'ячеславович – Харківський національний університет радіоелектроніки, асистент кафедри філософії, Україна; e-mail: vladyslav.yevdokymenko@nure.ua; ORCID: https://orcid.org/0009-0000-4174-3773

Чакрян Вадим Хазарович – Харківський національний університет радіоелектроніки, старший викладач кафедри інфокомунікаційної інженерії ім. В.В. Поповського, Україна; e-mail: vadym.chakrian@nure.ua; ORCID: https://orcid.org/0000-0003-4827-9779