УДК 004.056:174:004.9
DOI: 10.31673/2409-7292.2025.031152

Легомінова С.В., Капелюшна Т.В., Щавінський Ю.В., Мужанова Т.М.

КОНЦЕПТУАЛЬНІ ПІДХОДИ ІНТЕГРАЦІЇ ЕТИЧНИХ НОРМ У ПОЛІТИКУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У статті проаналізовано ключові концептуальні підходи до інтеграції етики в політику інформаційної безпеки. Визначені на основі аналізу наукових публікації ключові етичні дилеми, що виникають у сфері інформаційної безпеки, зокрема проблеми конфіденційності, прозорості, автоматизації прийняття рішень та моніторингу персоналу. Обґрунтовано необхідність формалізації етичних принципів у внутрішніх нормативних документах з метою підвищення відповідальності, прозорості та довіри в цифровому середовищі. Запропоновано класифікацію існуючих підходів до впровадження етики в інформаційну безпеку з визначеними характеристиками, етичним виміром та критеріями оцінювання: нормативно-правового, професійно-етичного, корпоративно-етичного, освітнього, технологічно-етичного. Розроблені критерії дозволяють в подальшому сформувати цілісну систему оцінювання ефективності підходів. Створена концептуальна модель інтеграції етичних норм, яка передбачає етапи діагностики, формалізації, впровадження, навчання, моніторингу та критерії оцінки етичного впливу. Модель дозволяє систематизувати процес впровадження етичних принципів в організаційні документи інформаційної безпеки. Представлено рекомендації щодо розробки внутрішніх політик з урахуванням етичних принципів, проведення етичного аудиту, та заснування етичного комітету в структурі організації. Запропоновані рекомендації дозволяють забезпечити формування етично зрілої корпоративної культури, де безпека ґрунтується на моральних принципах, довірі та повазі до прав людини у цифровому середовищі.

Ключові слова: інформаційна безпека, етика кібербезпеки, корпоративні етичні кодекси, політика інформаційної безпеки.

Вступ

У сучасному цифровому середовищі, де інформація стає ключовим ресурсом, питання захисту даних виходить за межі суто технічного чи правового забезпечення. Зростаюча кількість кіберзагроз, витоків персональних даних, маніпуляцій інформацією та конфліктів інтересів вказує на необхідність включення етичних засад у політику інформаційної безпеки. Технічні засоби самі по собі не гарантують дотримання конфіденційності, чесності та відповідальності у поводженні з інформацією. Водночас, законодавче регулювання не завжди встигає за технологічними змінами, залишаючи моральні дилеми на розсуд окремих працівників або організацій.

Інтеграція етичних норм у політику інформаційної безпеки (ІБ) дозволяє сформувати систему внутрішніх цінностей і стандартів поведінки, які підтримують довіру до цифрових сервісів, знижують ризики внутрішніх загроз та посилюють культуру кібергігієни. Зокрема, в умовах поширення штучного інтелекту, Big Data, віддаленої роботи та хмарних обчислень зростає потреба в етичному осмисленні дій, пов’язаних з обробкою та використанням інформації.

Таким чином, дослідження концептуальних підходів до інтеграції етичних норм у політику ІБ є актуальним і необхідним для формування сталих, прозорих та етично обґрунтованих стратегій управління інформаційними ресурсами в державному та корпоративному секторах.

Формулювання проблеми

Сьогодні компанії та організації будь-якого розміру активно працюють над збором, зберіганням та аналізом даних, щоб збільшити свій прибуток та підвищити рейтинг лояльності клієнтів. Таким чином, конфіденційність даних продовжує бути головною етичною проблемою в ІТ.

Сучасне суспільство дедалі більше залежить від інформаційних технологій, що робить інформацію цінним активом, а її захист – стратегічним пріоритетом. Однак традиційні підходи до ІБ, які зосереджені на технічних та правових аспектах, часто виявляються недостатніми для запобігання ризикам, пов’язаним з людським фактором – недоброчесністю, недовірою, байдужістю чи свідомим зловживанням правами доступу.

Це породжує потребу у доповненні політик ІБ етичними нормами, які регламентують крім дозволеного, ще й те, що є правильним і відповідальним. Зокрема, у фокусі – чесність у використанні інформації, повага до приватності, прозорість алгоритмічного прийняття рішень, уникнення конфлікту інтересів і соціальна відповідальність за наслідки порушення ІБ.

Також проблемою є відпрацювання підходів для оцінювання дотримання етичних норм при організації інформаційної безпеки в організаціях. Тому метою цієї статті є розробка та обґрунтування концептуальних підходів до інтеграції етичних норм у політику інформаційної безпеки організацій з урахуванням сучасних викликів цифрового середовища, технологічного розвитку та соціальних очікувань до відповідального поводження з інформацією.

Аналіз літератури

В наукових публікаціях етика та ІБ розглядаються як одна з найважливіших сфер занепокоєння та інтересу науковців-дослідників та практиків галузі. Науковці розглядають фундаментальні етичні проблеми, що виходять за рамки всіх видів ІТ, а також нові та виникаючі дилеми, що супроводжують будь-який технологічний прогрес. Наприклад, нещодавні досягнення в галузі штучного інтелекту та машинного навчання започаткували нову еру етичних проблем, що вимагають від фахівців з ІТ переоцінки своїх етичних рамок прийняття рішень. Етичні наслідки ІТ впливають на окремих осіб, організації та суспільство, підкреслюючи важливість прийняття відповідальних рішень в цифрову епоху.

Враховуючи актуальність та необхідність вирішення проблем та новітню сферу досліджень, пов’язану з впливом етичних принципів у сфері захисту інформації, розробленню підходів до дотримання етичних норм в ІБ присвячена достатня кількість вітчизняних та зарубіжних наукових публікацій.

В роботах [1, 2] проведений історичний аналіз етичних проблем, питань моралі та моральності тих чи інших вчинків, які переслідують людську цивілізацію зі стародавніх часів, показана актуальність етики кіберзахисту, важливість вивчення даної проблеми із залученням більшої кількості спеціалістів не тільки з галузі ІБ.

У дослідженні [3, 4] висвітлені етичні принципи та стандарти, що стосуються ІБ, з розкриттям значних прогалин в дотриманні етичних принципів. Автори вважають, що при необхідності застосування заходів, необхідних для забезпечення кібербезпеки, важливо знайти баланс між різними вимогами всіх зацікавлених сторін. Ця мета досягається за допомогою детального етичного аналізу, що супроводжується широким дослідженням. Найважливішим результатом цього аналізу в дослідженнях є те, що кібербезпека конкурує або навіть конфліктує з іншими цінностями та інтересами і що забезпечення кібербезпеки завжди передбачає компроміс.

Інформаційна безпека та етика визначаються науковцями як всеохоплюючий термін, що стосується всіх видів діяльності, необхідних для захисту інформації та систем, що її підтримують, з метою сприяння її етичному використанню [5-8]. Після широкого обговорення інструментів та технологій, що використовуються для досягнення цілей ІБ та етики, дослідники у своїх роботах обговорюють рекомендації щодо подальших напрямків досліджень впливу етичних принципів на організацію ІБ та оцінювання управлінських, організаційних та соціальних наслідків цього впливу.

Для оцінювання етичного мислення в контексті кібербезпеки, в роботах [9, 10] використано п'ять етичних принципів, розроблених у принципалістській системі: благодійність, незавдання шкоди, справедливість, автономія та пояснення. Автори зазначають, що принципалізм є найпоширенішим підходом у прикладній етиці та широко використовується в суміжних галузях, таких як біоетика та штучний інтелект. Ці п’ять принципів також використані в нещодавньому огляді етичних питань, що виникають у сфері кібербезпеки завдяки квантовим обчисленням [11-13]. Автори стверджують, що принципи можуть бути використані для вирішення конфліктів у сфері управління ІБ, що дозволяє збалансувати конфліктуючі сторони та знайти етично правильне рішення.

© Легомінова С.В., Капелюшна Т.В., Щавінський Ю.В., Мужанова Т.М. (2025) Концептуальні підходи інтеграції етичних норм у політику інформаційної безпеки. Сучасний захист інформації, 3(63), 90–98. https://doi.org/10.31673/2409-7292.2025.031152

Найбільш повно фундаментальні етичні принципи, які включають конкретні аспекти професійної відповідальності, наведені в Кодексі етики та професійної поведінки ACM (Association for Computing Machinery – англ. Асоціація обчислювальної техніки) [14]. Етичний Кодекс ACM – це набір принципів та норм, які визначають етичні зобов'язання та професійну відповідальність для членів ACM та фахівців у сфері інформаційних технологій. Він слугує орієнтиром для прийняття етичних рішень у складних ситуаціях та сприяє підтримці високих стандартів професійної поведінки. Загальними принципами є: публічне благо; уникнення шкоди; чесність та справедливість; повага до приватності; відповідальність; компетентність; об'єктивність; збереження конфіденційності; прозорість; відповідальність за якість.

В дослідженні [15] розглянуті кілька етичних питань у сфері кібербезпеки. Автор підкреслює, що, хоча від фахівців у сфері інформаційно-комунікаційних технологій (ІКТ) очікується дотримання кодексу етики, такого як кодекс етики ACM, який виражає загальні етичні принципи та професійні обов'язки, для кінцевих користувачів такого кодексу не існує.

Таким чином, аналіз наукової літератури підтверджує висновок про вплив етичних принципів на організацію ІБ. Разом з тим, у дослідженнях науковці обмежуються теоретичними висновками щодо такого впливу, недостатньо відпрацьовані конкретні практичні пропозиції з інтеграції етичних принципів в організаційні документи інформаційної та кібербезпеки.

Метою цієї статті є розробка та обґрунтування концептуальних підходів до інтеграції етичних норм у політику інформаційної безпеки організацій з урахуванням сучасних викликів цифрового середовища, технологічного розвитку та соціальних очікувань до відповідального поводження з інформацією. Для досягнення поставленої мети передбачено вирішення таких завдань:

- визначити ключові етичні дилеми, що виникають у сфері ІБ;
- проаналізувати сучасні наукові підходи до визначення ролі етики в сфері ІБ;
- сформувати концептуальну модель інтеграції етичних норм у політику ІБ;
- розробити рекомендації щодо впровадження етичних стандартів на рівні організаційної політики ІБ.

Основна частина

1. Ключові етичні дилеми, що виникають у сфері інформаційної безпеки

У зв’язку з швидким розвитком технологій, який випереджає етичні та правові стандарти, ключові етичні дилеми в інформаційній безпеці існують сьогодні в комплексній взаємодії технологій, прав людини, корпоративних інтересів та соціального контексту. Нові технології (штучний інтелект, біометрія, великі дані, блокчейн) виникають значно швидше, ніж встигають сформуватися чіткі етичні та правові рамки їх використання. При застосуванні машинного навчання для навчання моделей часто використовують великі масиви особистих або чутливих даних без інформування чи згоди користувачів. .Складні системи безпеки та штучного інтелекту мають розподілену відповідальність, де складно визначити хто винен у помилці – програміст, компанія чи сам алгоритм. Інформаційна безпека передбачає контроль, моніторинг, обмеження доступу, що може вступати в конфлікт із правами на приватність, свободу слова та самовираження.

Компанії з метою отримання максимального прибутку часто ставлять пріоритет на прибуток, ринок і конкурентні переваги, нехтуючи етичними питаннями використання персональних даних користувачів без прозорого інформування (наприклад, у рекламі або поведінковій аналітиці).

Різні країни й культури мають свої уявлення про приватність, свободу інформації, цензуру. Тому контент, дозволений в одній країні, блокується в іншій через етичні чи правові міркування, що створює колізії в глобальній інформаційній взаємодії. Встановлення державою масового нагляду під приводом національної безпеки створює дисбаланс між безпекою і правами людини. А використання заходів кібербезпеки в політичних або маніпулятивних цілях

© Легомінова С.В., Капелюшна Т.В., Щавінський Ю.В., Мужанова Т.М. (2025) Концептуальні підходи інтеграції етичних норм у політику інформаційної безпеки. Сучасний захист інформації, 3(63), 90–98. https://doi.org/10.31673/2409-7292.2025.031152

приводить до того, що інструменти кіберзахисту можуть застосовуватися не лише для захисту, але й для репресій, цензури, контролю, маніпуляцій (блокування інтернету під час протестів чи політичних заворушень).

2. Класифікація підходів до інтеграції етики в інформаційну безпеку

Інтеграція етики в ІБ передбачає розробку та впровадження етичних принципів та норм у процеси розробки, впровадження та використання інформаційних систем та технологій. Етичні принципи мають вирішальне значення для ефективної ІБ, вони забезпечують конфіденційність, цілісність та доступність інформації, водночас дотримуючись конфіденційності та прав людини. Дотримання етичних стандартів – це не лише моральний імператив а й стратегічний спосіб побудови довіри та зменшення ризиків [15-16]. Узагальнення світового досвіду застосування етичних норм в ІБ дозволило виділити три основні концептуальні підходи:

- реактивний підхід – етичні норми формуються у відповідь на кризові події, інциденти або зловживання;
- превентивний підхід – організація завчасно інтегрує етичні стандарти у формі кодексів поведінки, тренінгів, етичних комітетів;
- інтегрований підхід – етика розглядається як складова корпоративної культури та управління ризиками, інтегрується в усі етапи життєвого циклу інформаційних систем.

Інтеграційний підхід розглядається як найбільш ефективний у сучасних умовах, оскільки дозволяє враховувати як зовнішні вимоги (законодавчі та регуляторні), так і внутрішні особливості організації, її культуру, технологічну інфраструктуру та управлінські моделі. Аналіз наукових досліджень дозволяє розширити визначені основні концептуальні підходи (рис. 1).

Рис. 1. Концептуальні підходи до інтеграції етики в інформаційну безпеку

Порівняння підходів з доданою колонкою "Етичний вимір" для кожного з підходів до впровадження етики в ІБ зведене в таблицю 1.

Для оцінювання ефективності кожного з підходів пропонуються критерії, які охоплюють як кількісні, так і якісні показники (табл. 2). Їх можна адаптувати до конкретного підприємства або дослідження.

Таблиця 1

Порівняння підходів до інтеграції етики в інформаційну безпеку

Підхід	Основна характеристика	Переваги	Обмеження	Приклади реалізації	Етичний вимір
Нормативно-правовий	Базується на законодавстві, міжнародних стандартах та регулюючих документах	Чіткість правил; правова відповідальність	Повільна адаптація до нових загроз; формалізм	GDPR, ISO/IEC 27001, Закон України «Про інформаційну безпеку»	Встановлює етичні обов'язки через правові норми, гарантує мінімальні стандарти доброчесності
Професійно-етичний	Передбачає дотримання кодексів честі фахівців	Підвищує відповідальність працівників, сприяє формуванню культури доброчесності	Не є обов'язковим до виконання; залежить від професійного середовища	Кодекси ISACA, ACM, (ISC)²	Орієнтований на внутрішні моральні цінності фахівців, формує етичну ідентичність професіоналів
Корпоративно-етичний	Включає етичні політики в корпоративне управління безпекою	Узгоджує етичні принципи з місією компанії; сприяє довірі	Може бути декларативним без практичної реалізації	Етичні кодекси компаній Google, Microsoft	Інтегрує етику в бізнес-процеси, враховує вплив рішень на суспільство
Освітньо-просвітницький	Спрямований на формування етичної свідомості через навчання	Довготривалий вплив, формує стійкі установки	Повільний ефект. Залежить від якості освіти	Курси з цифрової етики, тренінги з етичного хакінгу	Розвиває критичне мислення; навчає відповідальності у прийнятті рішень
Технологічно-етичний	Передбачає етичне програмування, аудит систем ШІ, прозорість алгоритмів	Забезпечує "етичність за замовчуванням", масштабованість	Високі витрати, потреба в мультидисциплінарності	Етичний аудит ШІ, концепції Explainable AI	Інституціоналізує етику на рівні технологій, вимагає обґрунтованих рішень у проєктуванні

Таблиця 2

Критерії оцінювання підходів до інтеграції етики в інформаційну безпеку

Підхід	Критерії ефективності
Нормативно-правовий	- Відповідність законодавству та стандартам (ISO, GDPR, тощо) - Наявність внутрішніх політик, що працюють - Дотримання термінів реагування на інциденти - Частота виявлення порушень і дисциплінарних заходів
Інституційно-організаційний	- Ступінь інтеграції етики в структуру управління - Частота етичних тренінгів - Рівень залучення персоналу до ініціатив з етики - Показники прозорості та підзвітності
Технологічний	- Захищеність систем (від атак, витоків тощо) - Частка автоматизованих етичних перевірок - Співвідношення між інцидентами і вчасним реагуванням - Надійність журналювання і зберігання логів
Освітньо-виховний	- Кількість/якість програм з етики для персоналу - Динаміка зміни етичних установок (за опитуваннями) - Зменшення порушень після навчання - Участь у зовнішніх навчальних ініціативах
Культурно-ціннісний	- Внутрішній рівень довіри в команді - Емоційний клімат і задоволеність персоналу - Соціальна відповідальність організації - Кількість етичних кейсів, вирішених без примусу

© Легомінова С.В., Капелюшна Т.В., Щавінський Ю.В., Мужанова Т.М. (2025) Концептуальні підходи інтеграції етичних норм у політику інформаційної безпеки. Сучасний захист інформації, 3(63), 90–98. https://doi.org/10.31673/2409-7292.2025.031152

У поєднанні з етичним виміром з попередньої таблиці (табл. 1) визначення критеріїв оцінювання підходів до інтеграції етики в ІБ (табл. 2) дозволяє в подальшому сформувати цілісну систему оцінювання ефективності таких підходів.

3. Концептуальна модель інтеграції етичних норм у внутрішню політику безпеки

З метою формування цілісної внутрішньої політики ІБ, яка базується не лише на технічних та юридичних аспектах, а й на етичних принципах, що гарантують повагу до прав користувачів, прозорість рішень та довіру до організації, створена концептуальна модель, яка включає структуру (рис. 2), ключові компоненти моделі (табл. 3), етапи інтеграції етичних норм у політику ІБ (табл. 4).

Рис. 2. Структура концептуальної моделі

Таблиця 3

Ключові компоненти моделі

Компонент	Зміст
Етичні принципи	Конфіденційність, прозорість, справедливість, згода, відповідальність
Політика інформаційної безпеки	Комплекс внутрішніх правил, процедур і технічних механізмів
Механізми імплементації	Кодекси етики, політики, навчання, моніторинг, звітування
Етична оцінка рішень	Процедури оцінки наслідків дій на приватність, справедливість тощо
Залучення зацікавлених сторін	Працівники, користувачі, аудитори, етичний комітет
Зворотний зв'язок і коригування	Канали для повідомлень про порушення, періодичний перегляд політик

Таблиця 4

Етапи інтеграції етичних норм у політику безпеки

Етап	Назва	Зміст
1	**Аналіз ризиків і дилем**	Визначення етичних ризиків (порушення конфіденційності, дискримінація)
2	**Формалізація етичних принципів**	Розробка Кодексу етики, впровадження принципів у політику ІБ
3	**Навчання та комунікація**	Підготовка персоналу, етичні тренінги, інформування
4	**Імплементація процедур**	Технічні та організаційні заходи відповідно до етичних норм
5	**Моніторинг і звітування**	Виявлення порушень, оцінка відповідності, внутрішнє звітування
6	**Коригування та вдосконалення**	Зворотний зв'язок, перегляд політик, адаптація до нових викликів

© Легомінова С.В., Капелюшна Т.В., Щавінський Ю.В., Мужанова Т.М. (2025) Концептуальні підходи інтеграції етичних норм у політику інформаційної безпеки. Сучасний захист інформації, 3(63), 90–98. https://doi.org/10.31673/2409-7292.2025.031152

4. Рекомендації щодо впровадження етичних стандартів на рівні організаційної політики інформаційної безпеки

У сучасних умовах зростання ризиків зловживання інформацією особливого значення набуває інтеграція етичних принципів у систему управління ІБ. Етична складова політики ІБ має не лише нормативний, але й превентивний характер, формуючи морально вмотивовану поведінку персоналу. З огляду на це, пропонується комплекс рекомендацій для організацій, спрямований на посилення етичної зрілості внутрішньої політики ІБ:

4.1. Інституціоналізація етичних норм у політиці безпеки

Етичні принципи доцільно включити у загальну Політику ІБ організації або розробити окремий Кодекс етичної поведінки у сфері ІБ. Ці документи мають визначати моральні орієнтири для працівників при роботі з інформаційними системами, зокрема щодо питань конфіденційності, прозорості дій, поваги до прав суб'єктів даних, недискримінації та відповідальності.

4.2. Розробка внутрішніх спеціалізованих політик з етичним наповненням

Етичні аспекти доцільно інтегрувати в такі внутрішні документи з ІБ організації (політики):

- управління доступом;
- використання особистих пристроїв;
- резервного копіювання;
- управління інцидентами;
- захисту даних/персональних даних;
- прийнятного використання ІТ-ресурсів;
- тестування вразливостей, оновлень і патч-менеджменту;
- безперервності бізнесу та аварійного відновлення;
- управління ризиками інформаційної безпеки;
- логування та моніторингу;
- управління активами.

4.3. Впровадження системи етичного навчання

Для підвищення етичної грамотності необхідно організовувати періодичне навчання та тренінги з етичної поведінки в цифровому середовищі. Зміст таких програм має включати аналіз типових етичних дилем, ознайомлення з прикладами порушень, а також формування практичних навичок прийняття етично виважених рішень у критичних ситуаціях.

4.4. Створення каналів етичного інформування та захисту викривачів

Організація має забезпечити можливість анонімного повідомлення про потенційні або фактичні етичні порушення. Це можливо шляхом:

- запуску внутрішніх онлайн-платформ (напр., NAVEX, Ethicspoint);
- створення каналу прямої комунікації з етичним комітетом або службою ІБ;
- запровадження механізмів захисту викривачів (whistleblowers), закріплених у внутрішніх організаційних документах.

4.5. Етичний аудит та оцінка політик інформаційної безпеки

Рекомендується проводити періодичну експертизу внутрішніх політик з точки зору їх етичної обґрунтованості та наслідків. Така експертиза має включати:

- оцінку балансу між безпекою і правами користувачів;
- виявлення потенційної упередженості у автоматизованих рішеннях;
- аналіз впливу політик на довіру персоналу та партнерів.

4.6. Призначення відповідальної особи або комітету з етики інформаційної безпеки

Для координації та моніторингу етичних аспектів у сфері безпеки доцільно призначити офіцера з етики або створити спеціалізований етичний комітет. Цей орган має здійснювати консультаційний супровід, розглядати складні кейси, готувати рекомендації для керівництва, а

також контролювати дотримання етичних стандартів у повсякденній практиці. Таким чином, впровадження етичних стандартів на рівні організаційної політики ІБ потребує системного підходу, що охоплює нормативне закріплення, освітні програми, механізми контролю та відповідальності. Це дозволяє не лише мінімізувати внутрішні ризики, але й сприяє формуванню етично зрілої цифрової культури, де домінують принципи чесності, поваги до особистості та відповідального управління інформацією.

Висновки

Таким чином, у процесі дослідження було виявлено, що ефективна політика інформаційної безпеки не може бути зведена лише до технічних та нормативно-правових інструментів. Вона потребує етичного підґрунтя, яке забезпечує: довіру до внутрішніх процесів обробки інформації; передбачуваність поведінки персоналу в умовах конфлікту інтересів чи кіберінцидентів; сталість організаційної культури, орієнтованої на безпечне використання інформаційних ресурсів. Інтеграція етики в інформаційну безпеку є критично важливою для забезпечення довіри до технологій та їхнього позитивного впливу на суспільство. Нехтування етичними аспектами може призвести до серйозних негативних наслідків, включаючи порушення прав людини, втрату довіри до систем та інституцій, а також підрив соціальної стабільності. Тому, розробка та впровадження етичних підходів у сфері інформаційної безпеки має бути пріоритетом для всіх зацікавлених сторін.

Розроблена концептуальна модель інтеграції етичних принципів в політику ІБ, яка включає етапи діагностики, формалізації, впровадження, навчання, моніторингу та критерії оцінки етичного впливу, дозволяє систематизувати процес впровадження етичних принципів в організаційні документи інформаційної безпеки.

Напрямком подальших досліджень буде розроблення показників запропонованих критеріїв та методу оцінювання етичної зрілості системи інформаційної безпеки організації.

Перелік посилань

1. Гапіченко , А., & Штанько , В. (2025). Етичні принципи як основа кібербезпеки в умовах цифрових загроз. Збірник наукових праць «ΛΌГОΣ» , (24 січня 2025 р.; Сеул, Південна Корея), 322–325. https://doi.org/10.36074/logos-24.01.2025.067.

2. Yaghmaei, E., van de Poel, I., Christen, M., Gordijn, B., Kleine, N., Loi, M., Morgan, G., & Weber, K. (2017). Canvas White Paper 1 Cybersecurity and Ethics. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3091909.

3. WEBER, K. (2022a). CYBERSECURITY AND ETHICAL, SOCIAL, AND POLITICAL CONSIDERATIONS: WHEN CYBERSECURITY FOR ALL IS NOT ON THE TABLE. Humanities and Social Sciences quarterly. https://doi.org/10.7862/rz.2022.hss.07.

4. WEBER, K. (2022b). CYBERSECURITY AND ETHICAL, SOCIAL, AND POLITICAL CONSIDERATIONS: WHEN CYBERSECURITY FOR ALL IS NOT ON THE TABLE. Humanities and Social Sciences quarterly. https://doi.org/10.7862/rz.2022.hss.07.

5. ПРОФЕСІЙНА ЕТИКА УПРАВЛІНСЬКОЇ ДІЯЛЬНОСТІ В КІБЕРБЕЗПЕЦІ. Навчальний посібник / С.В. Легомінова, Ю.В. Щавінський, Т.М. Мужанова, Ю.М. Якименко, Т.В. Капелюшна, Д.І. Рабчун, К. : ДУТ, 2023, 198 с.

6. Wright, D. (2011). A framework for the ethical impact assessment of information technology. Ethics and Information Technology. 13. 199-226. https://doi.org/10.1007/s10676-010-9242-6.

7. Halim, Z., Durya, N. P. M. A., Kraugusteeliana, K., Suherlan, S., & Alfisyahrin, A. L. (2023). Ethics-Based Leadership in Managing Information Security and Data Privacy. Jurnal Minfo Polgan, 12(2), 1819–1828. https://doi.org/10.33395/jmp.v12i2.13018.

8. Sharma, N. (2023). The Role of Ethics in Developing Secure Cyber-Security Policies. Tuijin Jishu/Journal of Propulsion Technology. 43. 250-254. https://doi.org/10.52783/tjjpt.v43.i4.2346.

9. Formosa, P., Wilson, M., & Richards, D. (2021). A principlist framework for cybersecurity ethics. Computers & Security, 109, 102382. https://doi.org/10.1016/j.cose.2021.102382.

10. Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., Luetge, C., Madelin, R., Pagallo, U., Rossi, F., Schafer, B., Valcke, P., & Vayena, E. (2018). AI4People – An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations. Minds and Machines, 28(4), 689–707. https://doi.org/10.1007/s11023-018-9482-5.

11. Fenech, J., Richards, D., & Formosa, P. (2024). Ethical principles shaping values-based cybersecurity decision-making. Computers & Security, 140, 103795. https://doi.org/10.1016/j.cose.2024.103795.

© Легомінова С.В., Капелюшна Т.В., Щавінський Ю.В., Мужанова Т.М. (2025) Концептуальні підходи інтеграції етичних норм у політику інформаційної безпеки. Сучасний захист інформації, 3(63), 90–98. https://doi.org/10.31673/2409-7292.2025.031152

12. Coates, Rebecca; Baruwal Chhetri, Mohan; Liu, Dongxi; Pieprzyk, Josef; Richelle, Regine; Kang, Wei; Kwashie, Selasi; Wu, Tina; Nepal, Surya. Risks of quantum computing to cybersecurity: Perspectives from experts and professionals. Brisbane: CSIRO; 2023. csiro:EP2022-5789. https://doi.org/10.25919/fv3w-6863.

13. Berestiana, T. (2024). Research in the Field of Quantum-Safe Cryptography. Сучасний захист інформації, 2(58), 109–116. https://doi.org/10.31673/2409-7292.2024.020013.

14. ACM. The Code affirms an obligation of computing professionals to use their skills for the benefit of society. 2018. Доступно за посиланням: https://www.acm.org/code-of-ethics . [Дата звернення: 24.06.2025].

15. Christen, M., Gordijn, B., & Loi, M. (2020). The Ethics of Cybersecurity. Springer International Publishing. https://doi.org/10.1007/978-3-030-29053-5.

16. Воронюк, Ю., та Сатушева, К. (2024). Світовий досвід впровадження етичних принципів в організації економічної безпеки підприємницької діяльності. Збірник наукових праць «Наукові записки», 34 (1), 6-15. http://doi.org/10.33111/vz_kneu.34.24.01.01.005.011.

Надійшла 04.07.2025