УДК 004.056:174:004.9 DOI: 10.31673/2412-4338.2025.038722

Легомінова Світлана Володимирівна
Державний університет інформаційно-комунікаційних технологій, м. Київ
ORCID 0000-0002-4433-5123

Капелюшна Тетяна Вікторівна
Державний університет інформаційно-комунікаційних технологій, м. Київ
ORCID 0000-0001-7490-6751

Щавінський Юрій Віталійович
Державний університет інформаційно-комунікаційних технологій, м. Київ
ORCID 0000-0002-2319-8983

Мужанова Тетяна Михайлівна
Державний університет інформаційно-комунікаційних технологій, м. Київ
ORCID 0000-0002-7435-0287

МОДЕЛЬ ОЦІНЮВАННЯ ЕТИЧНОЇ ЗРІЛОСТІ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ

Анотація: *У статті представлено розроблену модель оцінювання етичної зрілості системи інформаційної безпеки організації, спрямовану на інтеграцію етичних принципів у процеси забезпечення інформаційної безпеки організації. На основі аналізу сучасних наукових досліджень, які підтверджують, що більшість інцидентів інформаційної безпеки пов'язані з діями співробітників, виявлено проблему оцінювання етичної зрілості систем інформаційної безпеки та обґрунтовано необхідність урахування людського фактора. Для вирішення проблеми запропоновано математичний опис моделі оцінювання етичної зрілості системи інформаційної безпеки організації, що базується на системі ключових показників ефективності, які відображають рівень впровадження етичних заходів у політиках, процедурах і практиках організації.*

Методологічною основою моделі виступає метод аналізу ієрархій, який дозволяє визначити ваги критеріїв через матриці попарних порівнянь та забезпечити узгодженість експертних оцінок. Для стандартизації показників застосовано нормалізацію на основі z-оцінок, що дає змогу привести різновимірні дані до уніфікованої шкали та дозволяє інтегрувати результати в єдиний індекс етичної зрілості, який відображає поточний стан системи інформаційної безпеки організації.

Запропонована модель формалізує зв'язок між етичними контрольними точками та вимогами міжнародних стандартів. Практичне значення моделі полягає у можливості її використання як інструменту підготовки до сертифікаційних аудитів, внутрішнього моніторингу та безперервного вдосконалення процесів управління інформаційною безпекою. Математична формалізація забезпечує прозорість оцінювання, об'єктивність результатів і можливість кількісного порівняння організацій за рівнем етичної зрілості. Запропонована модель також дозволяє системно розглядати процес внутрішнього інциденту з точки зору етапності та превентивних заходів.

Таким чином, розроблена модель поєднує науковий підхід до формалізації етичних аспектів інформаційної безпеки з практичною потребою бізнесу у відповідності до міжнародних стандартів та зменшенні ризиків, зумовлених внутрішнім людським фактором.

Ключові слова: *інформаційна безпека, етична зрілість систем кібербезпеки, модель етичної зрілості, кіберетика, ключові показники ефективності.*

Lehominova Svitlana
State university of information and communication technologies, Kyiv
ORCID 0000-0002-4433-5123

Kapeliushna Tetiana
State university of information and communication technologies, Kyiv
ORCID 0000-0001-7490-6751

Shchavinsky Yurii
State university of information and communication technologies, Kyiv
ORCID 0000-0002-2319-8983

Muzhanova Tetiana
State university of information and communication technologies, Kyiv
ORCID 0000-0002-7435-0287

MODEL FOR ASSESSING THE ETHICAL MATURITY OF AN ORGANIZATION'S INFORMATION SECURITY SYSTEM

Abstract: *This study presents a model for assessing the ethical maturity of an organization's information security system, designed to integrate ethical principles into the processes of safeguarding information security. Drawing on the analysis of contemporary scientific research, which demonstrates that the majority of information security incidents are linked to employee actions, the study identifies the problem of evaluating the ethical maturity of information security systems and substantiates the necessity of considering the human factor. To address this issue, a mathematical model for assessing ethical maturity is proposed, grounded in a system of key performance indicators (KPIs) that reflect the level of implementation of ethical measures across organizational policies, procedures, and practices.*

The methodological foundation of the model is the Analytic Hierarchy Process (AHP), which enables the determination of criterion weights through pairwise comparison matrices and ensures the consistency of expert judgments. To standardize the indicators, z-score normalization has been applied, allowing heterogeneous data to be transformed into a unified scale and integrated into a single Ethical Maturity Index. This index provides a quantifiable representation of the current state of an organization's information security system in terms of ethical maturity.

The proposed model establishes a formalized relationship between ethical control points and the requirements of international standards. Its practical significance lies in its applicability as a tool for certification audit preparation, internal monitoring, and continuous improvement of information security management processes. The mathematical formalization ensures transparency in assessment, objectivity of results, and the possibility of quantitative comparison of organizations by their ethical maturity level. Furthermore, the model provides a systematic perspective on the internal incident process, emphasizing its stages and corresponding preventive measures.

In conclusion, the developed model bridges the scientific formalization of ethical aspects in information security with the practical demands of organizations to comply with international standards and mitigate risks arising from the internal human factor.

Keywords: *information security, ethical maturity of cybersecurity systems, ethical maturity model, cyberethics, key performance indicators.*

1. Вступ

У сучасному цифровому середовищі інформаційна безпека (ІБ) вже давно перестала бути лише технічним завданням, сьогодні вона включає соціальні, правові й етичні виміри.

Ключовими факторами, які підсилюють актуальність етичної зрілості є зростання ролі персональних даних, сучасні вимоги законодавства та стандартів, репутаційні ризики та етичні дилеми в ІБ. Організації збирають і обробляють величезні обсяги чутливої інформації. Будь-яке неетичне використання може призвести до втрати довіри клієнтів і регуляторних санкцій. Регламенти та міжнародні стандарти вимагають не лише технічних, але й організаційних та етичних заходів у сфері захисту даних. Скандали, пов'язані з порушенням конфіденційності або маніпуляціями з даними, показують, що навіть формальна відповідність закону не рятує від репутаційних втрат [1]. Баланс між правом користувача на приватність і необхідністю моніторингу для запобігання кіберзагрозам, використання штучного інтелекту для виявлення загроз без упереджень і дискримінації потребують впровадження етичних принципів в діяльність структурних підрозділів ІБ організацій. Разом з тим, у нормативних документах з інформаційної безпеки відсутні конкретні критерії та показники оцінювання етичної зрілості систем ІБ для проведення сертифікації, що потребує додаткових наукових досліджень.

2. Аналіз літературних даних і постановка проблеми

Конкретними дослідженнями визначення етичної зрілості систем ІБ організацій в Україні займались не так багато науковців. У статті [2] досліджено етичні аспекти інформаційного менеджменту у сфері захисту персональних даних. Особливу увагу приділено сучасним викликам у сфері ІБ, зокрема етичним аспектам використання алгоритмів та нормативно-правовим механізмам захисту даних.

У роботах [3-4] науковці акцентують увагу на ролі корпоративної етики у сфері інформаційних технологій (ІТ) та впливі цифрових технологій на ІБ, на захисті прав користувачів, аналізуючи механізми впровадження відповідальних стандартів управління персональними даними. Їх дослідження показують, що дотримання етичних норм у великих корпораціях знижує ризики витоків інформації та сприяє формуванню довіри з боку користувачів. Науковці також наголошують на необхідності розробки внутрішніх кодексів корпоративної поведінки, які визначатимуть відповідальність компаній за використання персональних даних.

У дослідженні [5] зроблена спроба порівняти найбільш використовувані моделі зрілості ІБ для аналізу їх відповідності цілям використання спільно із стандартом ISO 27001. Науковцями встановлено, що моделі зрілості ІБ ґрунтуються на оцінці ризиків, хоча і на різних рівнях глибини мають схожі рівні зрілості. Було відзначено, що кожна модель в силу своєї специфіки має різні сфери застосування.

Аналіз наукових публікацій дозволяє зробити висновок про те, що в Україні напряму робіт про етичну зрілість ІБ небагато. Частіше дослідження стосуються суміжних тем – цифрова кібернетика, політики захисту даних, моделі зрілості ІБ, які опосередковано інтегруються етичними категоріями.

Більшість зарубіжних досліджень зрілості ІБ були зосереджені також на розробці, удосконаленні та застосуванні технічних аспектів у системах ІБ [6-7]. Разом з тим, науковці відзначають потребу вирішення нових викликів, які пов’язані з людським впливом на стан захисту інформації в організаціях [8-10].

Наукова праця [11] містить ґрунтовні тематичні дослідження, що окреслюють етичні проблеми кібербезпеки, а також представляють рекомендації та інші заходи для вирішення цих проблем, обговорюються теорії, проблеми та рішення відповідних етичних питань, які охоплюють управління, корпоративне управління, аудит, дотримання вимог інформаційної політики безпеки та зрілість, остання з яких є предметом перспективних наукових досліджень.

У дослідженні [12] представлено стратегію вимірювання зрілості ІБ, яка також має на меті допомогти у застосуванні та визначенні пріоритетів безпечної обробки інформації в корпоративному середовищі. Для вимірювання стану процесу використовується набір метрик, які представляють собою певні характеристики але без чіткого визначення етичних питань. Оцінювання цих метрик за встановленою шкалою показує стан процесів, яке і буде характеризувати рівень їх зрілості.

Аналіз публікацій зарубіжних науковців свідчить про те, що застосування моделі зрілості для управління процесами ІБ значно поширене, але дослідження також не дозволяють визначити якість врахування етичних принципів в системах ІБ.

3. Мета і задачі дослідження

Метою дослідження є розробка моделі оцінювання етичної зрілості системи ІБ організації, яка дозволить кількісно та якісно вимірювати рівень дотримання етичних норм, забезпечити баланс між технологічними механізмами захисту та людським фактором, а також підвищити довіру користувачів і суспільства до інформаційних процесів організації.

Для досягнення поставленої мети вирішено такі завдання:

– аналіз наукових джерел та нормативних документів (GDPR, NIST, ISO/IEC 27001, ISO/IEC 27701) з метою визначення етичних вимог до систем ІБ;

– виявлення ролі етичних чинників у виникненні внутрішніх загроз ІБ організацій;

– формування критеріїв та ключових показників ефективності (KPI) для оцінювання етичної зрілості системи ІБ;

– розробка багаторівневої моделі оцінювання зрілості за аналогією з CMMI (Capability Maturity Model Integration), адаптованої до сфери ІБ та етичних стандартів, та створення математичного апарату та метрик для розрахунку індексу етичної зрілості (EMI - Ethical Maturity Index) організації.

4. Виклад основного матеріалу

4.1. Вимоги міжнародних регламентів та стандартів щодо організації етичних заходів інформаційної безпеки

Для того, щоб мати можливість оцінювати етичну зрілість систем ІБ організацій, необхідно проаналізувати вимоги нормативних документів та міжнародних стандартів, які включають етичні принципи.

У Загальному регламенті про захист даних (GDPR, англ. - General Data Protection Regulation) хоч і немає розділу, який прямо називається “етичні заходи”, але документ містить низку вимог, які по суті є етичними принципами обробки даних та організації роботи з персональною інформацією.

Вони зобов'язують організації діяти не лише формально законно, а й добросовісно та з повагою до прав людини. Організація повинна не лише дотримуватися норм, але й демонструвати, що вона це робить (документація, політики, внутрішні процедури). Це означає наявність етичної звітності перед клієнтами, партнерами та регуляторами.

У документах NIST (National Institute of Standards and Technology, США) прямо не використовується термін "етичні заходи" у сенсі GDPR, але в багатьох стандартах і рекомендаціях закладені принципи, які мають виразно етичний зміст. Вони стосуються прозорості, підзвітності, справедливості та поваги до прав користувачів під час організації інформаційної безпеки:

- прозорість (Transparency) – користувачі повинні знати, що, як і навіщо робиться з їхніми даними;
- мінімізація (Minimization) – збір лише необхідної інформації;
- підзвітність (Accountability) – організація документує та доводить, що дотримується безпечних і чесних практик;
- справедливість (Fairness) – відсутність упередженого чи дискримінаційного використання даних;
- довіра (Trustworthiness) – підтримання високої репутації системи безпеки;
- людиноцентричність (Human-Centric Security) – врахування впливу заходів безпеки на права та свободи людей.

У міжнародному стандарті ISO/IEC 27001 - Система управління інформаційною безпекою етичний аспект вбудований у принципи корпоративного управління ІБ, зокрема у політиці ІБ має бути зобов'язання доброчесної діяльності у відповідності до законодавства, персонал повинен знати не лише технічні, а й етичні норми роботи з інформацією, дії користувачів мають бути відслідковувані, щоб можна було виявити та розслідувати порушення, процедури мають враховувати не лише технічні, а й етичні наслідки (наприклад, шкоду репутації, порушення довіри).

Стандарт ISO/IEC 27701 – Система управління конфіденційністю інформації розширює ISO/IEC 27001 і робить акцент на захисті персональних даних. Етичні вимоги цього стандарту включають:

−прозорість обробки даних (користувачі мають бути поінформовані, як і з якою метою обробляються їхні дані);

−мінімізація даних (збір лише необхідної інформації, щоб не створювати зайвих ризиків);

−згода суб'єкта даних (дані можна обробляти лише після явної згоди або на законних підставах);

−обмеження доступу та передачі (передача даних третім сторонам лише за чітко визначених умов);

−відповідальність організації (документовані докази того, що компанія дотримується принципів доброчесності й конфіденційності);

−етична оцінка ризиків, врахування впливу на приватність і суспільну довіру під час проєктування систем.

Загальне порівняння етичних вимог перерахованих нормативних документів наведені у таблиці 1.

Таблиця 1

Порівняння етичних вимог у GDPR, NIST, ISO/IEC 27001, ISO/IEC 27701

Стандарт / Регламент	Етичні принципи	Вимоги до організації	Приклади заходів	Точки етичного контролю
GDPR (ЄС, 2016)	Прозорість, законність, справедливість, мінімізація даних, підзвітність	Призначення DPO, навчання персоналу, DPIA	Політика конфіденційності, регулярні тренінги з етики обробки даних	На етапі збору даних (отримання згоди), при передачі даних, під час аудиту обробки
NIST CSF 2.0 / SP 800-53 (США)	Відповідальність, прозорість, захист прав користувача, запобігання шкоді	Ідентифікація ризиків, політики безпеки, навчання з етичних норм	Кодекс поведінки, контроль доступу, аудит рішень AI	При розробці політик безпеки, при зміні доступу, під час реагування на інциденти
ISO/IEC 27001:2022	Постійне вдосконалення, відповідальність керівництва, прозорість	Управління ризиками, визначення ролей, політики етичного використання	Розмежування доступу, перевірка постачальників, моніторинг інцидентів	На етапі оцінки ризиків, при виборі постачальників, при моніторингу систем

Стандарт / Регламент	Етичні принципи	Вимоги до організації	Приклади заходів	Точки етичного контролю
ISO/IEC 27701:2019	Принципи конфіденційності, прозорість, згода суб'єкта даних	Інтеграція PIMS до ISMS, призначення відповідальних за конфіденційність	Реєстр обробки даних, механізми відкликання згоди, етичні процедури збору	На етапі отримання згоди, при оновленні реєстру обробки, під час запитів на видалення даних

Аналіз наведених вимог у таблиці 1 дозволяє зробити узагальнений висновок про те, що етичний вимір ІБ є інтегрованим, але по-різному акцентованим у міжнародних нормативних актах та стандартах. GDPR зосереджується на захисті прав і свобод суб'єктів даних, прозорості та доброчесності обробки, розглядаючи етичність переважно крізь призму захисту приватності. NIST підходить більш технічно та процесно, проте містить етичний компонент через вимоги до підзвітності, навчання персоналу, управління інсайдерськими загрозами та доброчесного використання технологій. ISO/IEC 27001 розглядає етичність як складову системи управління ІБ, закріплюючи вимоги до політик, ролей, відповідальності та культури безпеки. ISO/IEC 27701 доповнює 27001, розширюючи етичний фокус на приватність та відповідальність за обробку персональних даних. Усі документи передбачають етичні контрольні точки: навчання персоналу, обмеження доступу, аудит дій, прозорість, підзвітність і моніторинг.

Водночас GDPR і ISO/IEC 27701 надають більше вимог, пов'язаних безпосередньо з правами особи, тоді як NIST та ISO/IEC 27001 більше фокусуються на процесах та управлінні ризиками. Таким чином, ефективна етична модель зрілості ІБ має інтегрувати правові, організаційні та технічні аспекти, поєднуючи підходи усіх чотирьох стандартів і регламентів для комплексного управління людським фактором та підтримання довіри.

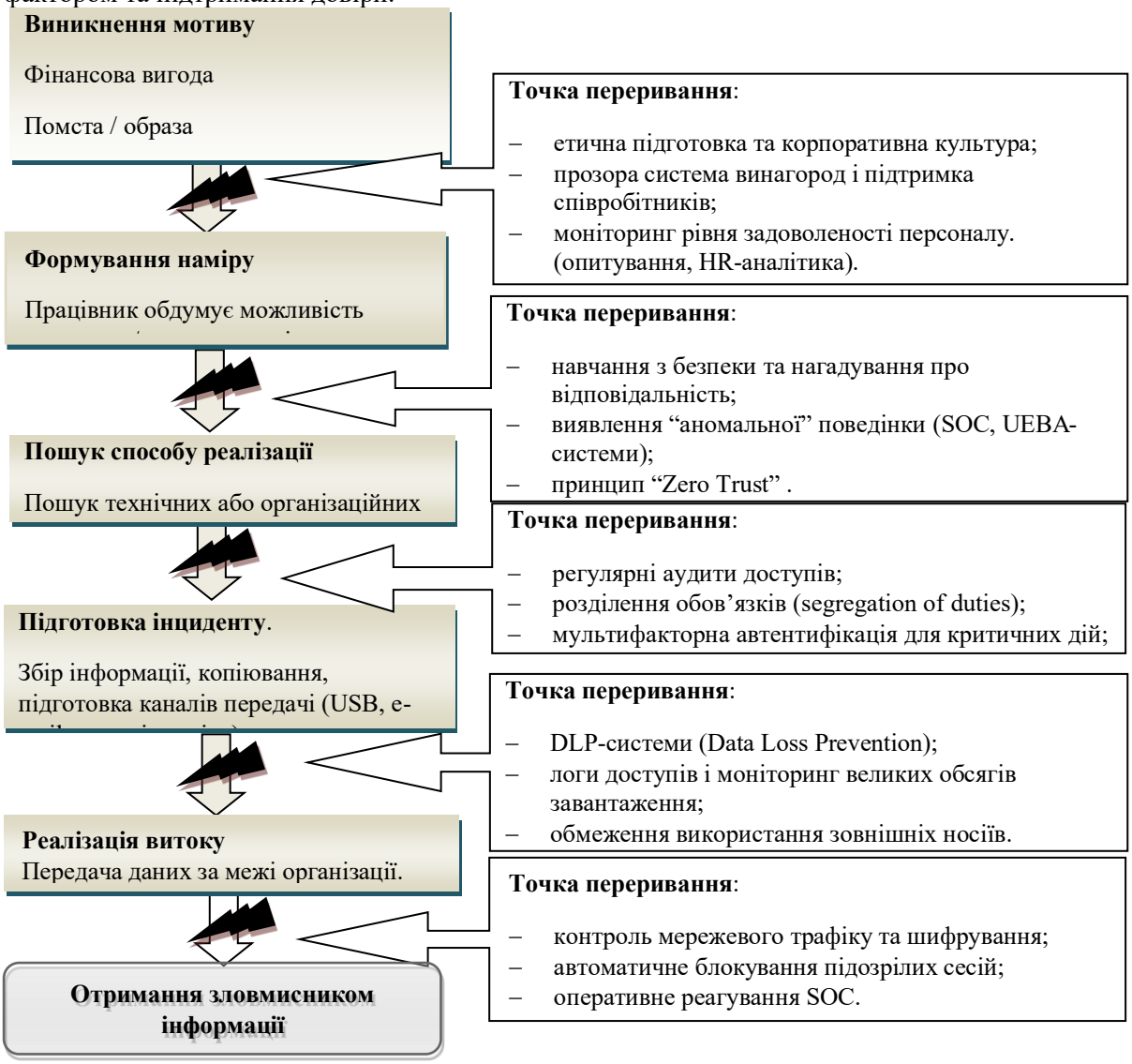

Рис. 1. Блок-схема етичних точок переривання дій порушника

4.2. Формування моделі оцінювання етичної зрілості системи інформаційної безпеки

Очевидно, що перед організацією, що здійснює діяльність з управління ІБ, рано чи пізно постає питання про те, як виконувати вимоги нормативних документів, в якому обсязі та на якому рівні деталізації і т. п. Відповісти на ці та інші питання може допомогти модель етичної зрілості з позначенням етичних контрольних точок, визначених в таблиці 1, які наочно показують де саме в процесах ІБ розташовуються ці точки (рис. 1).

Наведені на рисунку 1 точки переривання дозволяють: візуалізувати, де саме у процесах ІБ проявляються етичні ризики (наприклад, доступ до даних, моніторинг співробітників, прозорість політик); сформувати цілісне уявлення про етичний вимір у безпеці від нормативних вимог (GDPR, ISO, NIST) до внутрішніх практик та забезпечити узгодженість між технічними, організаційними та етичними аспектами; визначити метрики зрілості (наприклад, «рівень прозорості політики моніторингу» або «ступінь залученості співробітників у етичне навчання»); визначити організаційні етичні заходи для зупинення подальшого розвитку загроз. З практичної точки зору блок-схема (рис. 1) є інструментом для оцінювання та впровадження етичних заходів в організації.

Аналіз публікацій наукових досліджень зрілості ІБ [2-4, 6, 11] дозволяє зробити висновок, що ключовими напрямами оцінювання етичної зрілості мають бути: наявність політик і кодексів етики ІБ; інтеграція етичних норм у процеси (реагування на інциденти, управління доступом, аудит); освітні та культурні заходи (тренінги, симуляції етичних дилем); вимірюваність (ключові показники ефективності, індикатори етичної поведінки); рівень відповідальності (санкції, захист викривачів); вплив на зовнішнє середовище (участь у розробці стандартів, відкритість до спільноти).

Перераховані напрямки оцінювання дають можливість перетворити абстрактні етичні категорії у вимірювані показники критеріїв. Основні блоки критеріїв, які можуть бути застосовані при розрахунку рівня етичної зрілості системи ІБ, згруповані в таблиці 2.

Таблиця 2

Основні блоки критеріїв

Блок	Приклади критеріїв
Етична документація	Наявність кодексу етики, політик, декларацій
Навчання і обізнаність	Курси, тренінги, інтеграція в систему ІБ
Механізми звітності	Анонімні канали, захист викривачів, реагування на скарги
Етичне керівництво	Наявність комітету, лідерства, призначених осіб
Вбудованість у процеси ІБ	Врахування етики у прийнятті рішень, оцінці ризиків
Вимірювання та аудит	Наявність індикаторів, метрик, внутрішній аудит
Культура та поведінка	Рівень довіри, сприйняття працівниками, кейси практики

Таким чином, для вирішення проблеми оцінювання етичної зрілості системи ІБ потрібна модель оцінювання. Створення моделі оцінювання етичної зрілості системи ІБ організації є складним, але дуже перспективним напрямком наукових досліджень. Така модель дозволить не лише формально перевірити наявність документів і процесів, а й оцінити етичну відповідність, культуру та поведінку в організації.

Загальна ідея при створенні моделі оцінювання етичної зрілості системи ІБ організації полягає у визначенні інтегрального індексу етичної зрілості (Ethical Maturity Index, EMI)

$$EMI = \sum_{i=1}^{n} w_i * m_i \quad (1)$$

де m_i – нормалізоване значення i-того ключового показника ефективності, $m_i \in [0,1]$;
w_i – ваги (сума яких дорівнює 1);
n – кількість КПІ.

Рекомендована мін-макс нормалізація для KPI, де «більше = краще» [17]

$$m_i = \frac{x_i - \min(x_i)}{\max(x_i) - \min(x_i)} \quad , \tag{2}$$

де x_i – фактичне значення KPI_i
$\max(x_i), \min(x_i)$ – верхня та нижня межі очікувань (фіксуються експертно або статистично)

Для KPI, де «менше = краще» (наприклад, кількість етичних інцидентів) [17]

$$m_i = \frac{\max(x_i) - x_i}{\max(x_i) - \min(x_i)} \quad , \tag{3}$$

Примітка: якщо $\max(x_i) = \min(x_i)$ - встановити $m_i=1$ коли $x_i = \max(x_i)$ і 0 в іншому випадку.

У випадку нормального розподілу кількості значень окремого КПІ, з метою приведення показників до єдиного діапазону для коректного порівняння чи об'єднання (наприклад, у інтегральний індекс), нормалізацію для таких КПІ необхідно провести через z-оцінки [17]

$$z_i = \frac{x_i - \mu}{\sigma} \quad , \tag{4}$$

де μ – середнє арифметичне значень окремого КПІ;
σ – середнє квадратичне розподілу значень окремого КПІ, розраховується за формулою [18]

$$\sigma = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(x_i - \mu)^2} \tag{5}$$

Найбільш ймовірними кандидатами на нормальний розподіл серед KPI з етики та ІБ є: узагальнені рейтинги; середні часові показники (MTTR - Mean Time To Repair - Середній час відновлення; MTBF - Mean Time Between Failures - середній час між відмовами); оцінки за анкетуванням (рівень обізнаності, довіра, задоволеність).

Тоді нормалізація через z-оцінки (якщо розподіл нормальний) перетворює z в інтервал (0,1) через кумулятивну нормальну функцію

$$m_i = \frac{1}{2}\left(1 + \operatorname{erf}\left(\frac{z_i}{\sqrt{2}}\right)\right) \quad , \tag{6}$$

де **erf** — функція помилки (error function) [18], яка використовується в теорії ймовірностей.

Для пропонованої моделі оцінювання етичної зрілості це важливо тому, що дає можливість перетворювати KPI у порівнювані бали незалежно від масштабу.

З метою визначення інтегральної оцінки етичної зрілості за формулою (1) ваги кожного КПІ можна задати експертно або отримати методом аналізу ієрархій (MAI) попарним порівнянням КПІ між собою за шкалою Сааті (табл. 3) [19].

Таблиця 3

Коефіцієнти попарних порівнянь

Значення	Інтерпретація
1	Рівна важливість
3	Помірна перевага одного над іншим
5	Суттєва перевага
7	Дуже велика перевага
9	Абсолютна перевага

При цьому ваги кожного КПІ розраховуються методом геометричного середнього [20]

$$w_i = \frac{(\prod_{j=1}^{n} a_{ij})^{\frac{1}{n}}}{\sum_{k=1}^{n}(\prod_{j=1}^{n} a_{ij})^{\frac{1}{n}}} \quad , \quad i,j = 1,\dots,n\,, \qquad k = 1,\dots,n \tag{7}$$

де $\prod_{j=1}^{n} a_{ij}$ – добуток елементів у рядку *i;*

$(\prod_{j=1}^{n} a_{ij})^{\frac{1}{n}}$ - геометричне середнє;

i - KPI, вага якого обчислюється (рядок);

j - всі порівняння цього KPI з іншими (колонки);

k - кількість KPI для розрахунку суми для нормалізації.

Розрахований створеною моделлю інтегральний показник EMI (формула 1) дозволяє за аналогією CMMI (Capability Maturity Model Integration - Інтеграція моделі зрілості можливостей) [21] встановити рівні етичної зрілості системи ІБ (табл. 4).

Таблиця 4

Рівні етичної зрілості системи інформаційної безпеки

EMI	Рівень зрілості	Коротка характеристика
0.00–0.10	0 – Відсутність	Етика не враховується в ІБ
0.11–0.30	1 – Початковий	Ініціативи несистемні, реактивний підхід, процеси хаотичні, залежать від окремих людей, немає стандартизації
0.31–0.50	2 – Повторюваний	Деякі політики існують, але впровадження нерівномірне
0.51–0.70	3 – Визначений	Етика вбудована в процеси, є політики та навчання, процеси формалізовані, задокументовані й виконуються послідовно
0.71–0.85	4 – Кількісно керований	Проводиться моніторинг, аналіз, етичний аудит, процеси вимірюються, використовуються метрики для моніторингу та контролю
0.86–1.00	5 – Оптимізований	Етика – частина стратегічного управління, постійне вдосконалення процесів на основі аналізу даних та інновацій.

Створений математичний опис моделі дозволяє перевести етичні аспекти ІБ у кількісну форму, узгодити їх з вимогами міжнародних стандартів, забезпечити прозорий, відтворюваний і перевірений інструмент для сертифікації ІБ. Вхідними даними моделі при визначенні етичної зрілості системи ІБ організації будуть наступні, але не вичерпні КПІ:

- рівень формалізації етичних норм в політиці ІБ;
- наявність і зрілість етичної інфраструктури (кодексів, політик, каналів звітності);
- знання, ставлення й поведінка персоналу;
- вбудованість етики в процеси прийняття рішень щодо ІБ;
- дотримання принципів прозорості, справедливості, недискримінації тощо.

5. Обговорення результатів

Запропонована модель оцінювання етичної зрілості системи ІБ дозволяє:

- визначити, на якому етапі перебуває компанія у впровадженні етичних принципів під час оцінювання;
- побудувати дорожню карту переходу на вищі рівні;
- формувати стандарти та показники, за якими можна об’єктивно оцінювати прогрес.

Сформований математичний опис моделі має не лише академічну цінність, а й практичне значення у сфері сертифікації:

−модель з її математичним апаратом, визначеними КПІ, дозволяє уникнути суб’єктивності, властивої суто експертним оцінкам. При цьому сертифікаційний аудитор отримує числові результати, які можна перевірити;

−модель може бути «прив’язана» до вимог ISO/IEC 27001, 27701, NIST та GDPR, що робить її

придатною для використання як частини процесу підготовки до сертифікації;

– кожен KPI має визначену вагу й нормалізоване значення, що дозволяє чітко визначити, чому організація отримала саме такий рівень «етичної зрілості». Встановлення KPI, пов'язаних з етичною поведінкою, порушеннями даних та дотриманням вимог, може допомогти відстежувати прогрес та вимірювати ефективність етичних ініціатив. Це знижує ризик спорів з боку сертифікаційних органів чи внутрішніх аудиторів;

– модель допомагає виявити які етичні контрольні точки (наприклад, прозорість у використанні персональних даних, політика доступу) є слабкими, що дозволяє цілеспрямовано підготувати організацію до зовнішнього аудиту.

6. Висновки

Таким чином, ефективність системи ІБ організації прямо залежить не лише від технологічних та організаційних заходів, а й від рівня її етичної зрілості. Впровадження розробленої моделі оцінювання етичної зрілості дозволить своєчасно виявляти слабкі місця, пов’язані з людським фактором. Модель інтегрує етичні аспекти у процеси інформаційного захисту шляхом формалізації ключових показників ефективності, їх нормалізації та зважування за допомогою методу аналізу ієрархій. Вона забезпечує побудову інтегрального індексу етичної зрілості системи ІБ, що дозволяє кількісно оцінювати рівень відповідності організації міжнародним стандартам інформаційної безпеки (GDPR, NIST, ISO/IEC 27001, ISO/IEC 27701).

Практичне значення моделі полягає у можливості використання її як інструменту для внутрішнього аудиту, моніторингу рівня ІБ та підготовки до сертифікаційних перевірок. Запропонований підхід сприяє зменшенню ризиків, пов’язаних із людським фактором, та підвищує прозорість і об’єктивність прийняття управлінських рішень у сфері захисту інформації.

Розроблена модель може стати ефективною основою для побудови системи безперервного вдосконалення етичних практик ІБ, що є критично важливим у сучасних умовах зростання кіберзагроз і підвищених вимог до відповідності міжнародним регуляторним нормам. Зростання рівня етичної зрілості у довгостроковій перспективі сприятиме зменшенню частки внутрішніх інцидентів (витоків, зловживань, порушень доступу).

Наступним етапом дослідження на основі пропонованих математичних залежностях буде розробка інструментального прототипу (Python/Flask-системи) для практичного застосування моделі в організаціях та формування методики побудови матриці відповідності, що відображає узгодженість політик ІБ з етичними нормами.

Список використаної літератури

1. Журавльова І. Контекст і еволюція європейського права щодо захисту персональних даних. Часопис Київського університету права,. 2022. № 2-4. С. 113–123. URL: https://doi.org/10.36695/2219-5521.2-4.2022.21 (дата звернення: 15.05.2025).

2. Pokhidnia B. Ethics in information management: personal data protection. Economic scope. 2025. No. 197. P. 212–216. URL: https://doi.org/10.30838/ep.197.212-216 (дата звернення: 15.05.2025).

3. Осмятченко В. О., Згурська О. М., Мартиненко М. О. Вплив ділової етики на безпеку даних в IT- секторі в системі корпоративної культури. Проблеми сучасних трансформацій. Серія: економіка та управління. 2024. № 15. URL: https://doi.org/10.54929/2786-5738-2024-15-04-03 (дата звернення: 17.05.2025).

4. Скибун О.Ж. (2022). Сучасна етика як практична філософія кібербезпеки. Сучасний захист інформації, № 4. С. 66-70. DOI: https://doi.org/10.31673/2409-7292.2022.040011(дата звернення: 17.05.2025).

5. Коломицев М. В., Носок С. О., Тоцький Р. О. Порівняльний аналіз моделей оцінки зрілості інформаційної безпеки. Ukrainian Information Security Research Journal. 2019. Т. 21, № 4. С. 224–232. URL: https://doi.org/10.18372/2410-7840.21.14337 (дата звернення: 14.06.2025).

6. Gliner Dias Alencar, Hermano Perrelli de Moura, Ivaldir Honório de Farias Júnior, José Gilson de Almeida Teixeira Filho. An Adaptable Maturity Strategy for Information Security. Journal of Convergence Information Technology (JCIT), Volume 13, Number 2, Jun. 2018, p. 1-12 https://doi.org/10.48550/arXiv.1807.06184 (дата звернення: 14.06.2025).

7. Wang L., Liu F. A trusted measurement model based on dynamic policy and privacy protection in IaaS security domain. EURASIP Journal on Information Security. 2018. Vol. 2018, no. 1. URL: https://doi.org/10.1186/s13635-018-0071-1 (дата звернення: 25.06.2025).

8. Warkentin M., Willison R. Behavioral and policy issues in information systems security: the insider

threat. European Journal of Information Systems. 2009. Vol. 18, no. 2. P. 101–105. URL: https://doi.org/10.1057/ejis.2009.12 (дата звернення: 25.06.2025).

9. Choo K.-K. R. The cyber threat landscape: Challenges and future research directions. Computers & Security. 2011. Vol. 30, no. 8. P. 719–731. URL: https://doi.org/10.1016/j.cose.2011.08.004 (дата звернення: 16.07.2025).

10.Posey C., Bennett R. J., Roberts T. L. Understanding the mindset of the abusive insider: An examination of insiders' causal reasoning following internal security changes. Computers & Security. 2011. Vol. 30, no. 6-7. P. 486–497. URL: https://doi.org/10.1016/j.cose.2011.05.002 (дата звернення: 16.07.2025).

11.The Ethics of Cybersecurity / ed. by M. Christen, B. Gordijn, M. Loi. Cham : Springer International Publishing, 2020. URL: https://doi.org/10.1007/978-3-030-29053-5 (дата звернення: 24.07.2025).

12.Alencar, Gliner & Moura, Hermano & Junior, Ivaldir & Teixeira Filho, José. (2018). An Adaptable Maturity Strategy for Information Security. Journal of Convergence of Information Technology (JCIT), Volume 13, Number 2, June 2018, pp. 1-12. https://doi.org/10.48550/arXiv.1807.06184 (дата звернення: 24.07.2025).

13.Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) // Official Journal of the European Union. – 2016. – L 119. – P. 1–88. kmu.gov.ua/storage/app/media/uploaded-files/es-2016679.pdf (дата звернення: 24.07.2025).

14.NIST. Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. – Gaithersburg: National Institute of Standards and Technology, 2018. – 55 p. https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf (дата звернення: 24.07.2025).

15.ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. – Geneva : International Organization for Standardization, 2022. – 35 p. https://www.iso.org/standard/27001 (дата звернення: 24.07.2025).

16.ISO/IEC 27701:2019. Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines. – Geneva : International Organization for Standardization, 2019. – 79 p. https://www.iso.org/standard/71670.html (дата звернення: 24.07.2025).

17.Singh D., Singh B. Investigating the impact of data normalization on classification performance. Applied Soft Computing. 2020. Vol. 97. P. 105524. URL: https://doi.org/10.1016/j.asoc.2019.105524 (дата звернення: 19.08.2025).

18.Гнєденко Б.В. Курс теорії ймовірностей : підручник. Київ : Видавничо-полігр. центр "Київ. ун-т", 2009. 464 с.

19.Nisfoian S., Sysolina N., Savelenko H. Improving the Efficiency of Investment Project Selection Mechanisms at the Enterprise. Central Ukrainian Scientific Bulletin. Economic Sciences. 2020. No. 5(38). P. 228–237. URL: https://doi.org/10.32515/2663-1636.2020.5(38).228-237 (дата звернення: 19.08.2025).

20.Kułakowski K. On the Geometric Mean Method for Incomplete Pairwise Comparisons. Mathematics. 2020. Vol. 8, no. 11. P. 1873. URL: https://doi.org/10.3390/math8111873 (дата звернення: 19.08.2025).

21.Capability Maturity Model Integration, CMMI. Software Engineering Institute (SEI) Carnegie Mellon. URL: http://www.sei.cmu.edu/cmmi (дата звернення: 19.08.2025)