ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«УНІВЕРСИТЕТ ЕКОНОМІКИ ТА ПРАВА «КРОК»

Кваліфікаційна наукова праця на правах рукопису

УДК 005.95/.96:005.5:004

Злобін Кирило Васильович

ДИСЕРТАЦІЯ

ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ОЦІНЮВАННЯ ЛОЯЛЬНОСТІ ПЕРСОНАЛУ В СИСТЕМІ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПРОМИСЛОВИХ ПІДПРИЄМСТВ

Спеціальність 073 – Менеджмент

Подається на здобуття ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання практичних матеріалів, ідей, результатів і текстів інших авторів мають посилання на відповідне джерело _____ К.В. Злобін

Науковий керівник: Літвін Наталія Миколаївна, кандидат економічних наук, професор, професор кафедри управлінських технологій, перший проректор, ВНЗ «Університет економіки та права «КРОК»

Київ-2026

АНОТАЦІЯ

Злобін К.В. **Інформаційно-аналітичне забезпечення оцінювання лояльності персоналу в системі економічної безпеки промислових підприємств.** – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 073 - Менеджмент. Вищий навчальний заклад «Університет економіки та права «КРОК». Київ, 2026.

Дисертаційне дослідження присвячене розробленню інформаційно-аналітичного забезпечення оцінювання лояльності персоналу, здатного інтерпретувати її результати як ранні сигнали впливу загроз на систему економічної безпеки промислових підприємств, що дозволить переводити аналітику в управлінські рішення.

Актуальність теми зумовлена тим, що традиційне використання кадрових показників і періодичної звітності часто має фрагментарний характер і не забезпечує своєчасного виявлення ризикових відхилень у поведінці персоналу. У роботі обґрунтовано, що лояльність персоналу може виступати раннім сигналом ризику, який передує операційним збоям, втратам якості, інцидентам охорони праці, порушенням регламентів і комплаєнс-вимог. Відтак у центрі уваги поставлено завдання переведення лояльності з площини «м'яких» описових характеристик у площину формалізованих індикаторів, порогів і регламентованих управлінських дій. Методологічна логіка дослідження ґрунтується на системному поєднанні даних, процедур, відповідальностей і правил інтерпретації результатів. Практичне спрямування роботи полягає у створенні керованого контуру, який забезпечує регулярне вимірювання лояльності, її аналітичну інтерпретацію, інтеграцію в індексну модель економічної безпеки та запуск управлінських інтервенцій із контролем ефекту.

Наукова новизна одержаних результатів полягає у формуванні авторської концепції інформаційно-аналітичного забезпечення оцінювання лояльності персоналу як елемента системи економічної безпеки промислового підприємства, що забезпечує перехід від розрізнених кадрових метрик до формалізованих індексів і регламентованих управлінських дій. Уперше запропоновано цілісну концепцію інформаційно-аналітичного забезпечення економічної безпеки промислового підприємства як інституціоналізованого соціотехнічного контуру даних, процесів і ролей, інтегрованого з ERM, BCM, ISMS та циклом «моніторинг – аналіз – рішення – дія – навчання». Такий підхід дозволяє трактувати інформаційно-аналітичне забезпечення не як описово-звітну функцію, а як механізм перетворення відомостей про загрози, вразливості та можливості на відтворювані управлінські дії з визначеною відповідальністю. У межах запропонованої концепції розроблено методику оцінювання стану економічної безпеки на основі відкритих джерел із прозорою формулою інтегрального індексу S, поєднанням кількісного та якісного блоків і дискретними порогами інтерпретації. Встановлено, що поєднання фінансових і нефінансових ознак уразливості підвищує управлінську придатність інтегральної оцінки, оскільки дозволяє раніше фіксувати ризикові зони ще до прояву проблем у фінансовій звітності. Доведено, що стандартизація показників, словників і правил агрегації забезпечує порівнюваність результатів у часі та між підрозділами, а також знижує ризик неоднакової інтерпретації даних.

Уперше запропоновано авторську соціотехнічну модель інтеграції результатів оцінювання лояльності персоналу в систему управління загрозами економічній безпеці як єдиний контур прийняття рішень. У моделі лояльність інтерпретується як багатовимірна характеристика, що включає афективний, нормативний та інструментальний виміри, і розглядається як ведучий індикатор для випереджального управління.

Формалізовано математичний механізм включення індексу лояльності до інтегрального індексу економічної безпеки через передатну функцію, агреговану чутливість і сценарні розрахунки. Це забезпечує відтворюваний зв’язок між поведінковими характеристиками персоналу та фінансовими, операційними і ризиковими метриками підприємства. Результати узагальнення показують, що інтеграція лояльності у контур економічної безпеки скорочує часовий лаг між появою слабких сигналів та управлінським реагуванням, підсилює превентивність рішень і підвищує керованість ризиків людського чинника. Обґрунтовано, що така інтеграція особливо важлива для промислових підприємств, де дисципліна виконання технологічних процедур і дотримання регламентів безпосередньо впливають на операційну надійність.

Удосконалено структурно-функціональну архітектуру інформаційно-аналітичного забезпечення економічної безпеки підприємства шляхом деталізації операційних функцій контуру. Відмінністю від наявних підходів є орієнтація не на описово-звітний супровід, а на регламентований управлінський цикл із визначеними процедурами стандартизації показників і словників, консолідації даних, формування ранніх попереджувальних індикаторів і ключових індикаторів ризику, пріоритизації загроз, сценарного моделювання, формування доказової бази та організаційного навчання. Це дозволяє забезпечити відтворюваність рішень, підзвітність відповідальностей і системне перетворення аналітики на керовані дії, а перехід до такого циклу змінює роль аналітики з фіксації стану на інструмент управління відхиленнями. Показано, що зворотний зв’язок через повторні вимірювання є критичним для оцінки ефективності інтервенцій і коригування порогів, ваг та правил ескалації. Уточнено, що без регламентованої архітектури результати вимірювань втрачають управлінську цінність, оскільки не формують чіткої логіки «виявлено –

пояснено – призначено відповідального – виконано дію – перевірено ефект».

Удосконалено методичний підхід до оцінювання економічної безпеки підприємства шляхом збалансування кількісних фінансових коефіцієнтів із якісними ознаками, зокрема через урахування характеру аудиторської думки, наявності ковенантів, юридичних і регуляторних ризиків та прозорості розкриття інформації. На відміну від традиційних методик, у яких домінують фінансові метрики й ретроспективна діагностика, запропонований підхід підвищує чутливість інтегральної оцінки до нефінансових джерел уразливостей. Це дозволяє точніше визначати критичні зони ризику і обирати адресні управлінські заходи залежно від природи відхилень. Встановлено, що для промислових підприємств нефінансові ознаки часто виступають першими сигналами деградації керованості процесів, яка згодом трансформується у фінансові втрати. Доведено, що поєднання кількісного та якісного блоків сприяє прийняттю рішень, орієнтованих на причини ризику, а не лише на наслідки.

Удосконалено інструментарій операціоналізації лояльності персоналу через поєднання опитувальних і поведінкових індикаторів, нормування показників до інтервалу [0;1], перевірку внутрішньої узгодженості та зважування за надійністю і стратегічною релевантністю для конкретної технологічної системи підприємства. На відміну від практик, де переважають разові анкети або фрагментарні показники без єдиної шкали та верифікації, запропонований інструментарій забезпечує порівнюваність результатів у часі та між підрозділами. Це дозволяє зменшити вплив суб’єктивних викривлень і підвищити придатність оцінювання лояльності для управління ризиками. Саме комбінація психометричних і поведінкових даних підвищує валідність вимірювання в промисловому середовищі, де лояльність проявляється через дисципліну, відповідальність, готовність дотримуватися процедур і підтримувати зміни. Обґрунтовано, що

регулярність вимірювань і чітка порогова інтерпретація є умовами, за яких лояльність може функціонувати як ранній сигнал ризику.

Удосконалено логіку інтеграції людського чинника в систему економічної безпеки шляхом регламентованого зв'язування результатів оцінювання лояльності з реєстром ризиків та набором управлінських інтервенцій. Відмінністю є наявність порогів, сценаріїв реагування, власників ризику та визначених горизонтів реагування, тоді як у багатьох підходах кадрові показники використовуються ізольовано від ризик-реєстру. Це дозволяє скоротити часовий лаг між появою слабких сигналів і втручанням, підвищити превентивність рішень і контролювати ефект інтервенцій через повторні вимірювання. Доповнено систематизацію внутрішніх і зовнішніх загроз, що реалізуються через персонал, та обґрунтуванно роль низької лояльності як фактора посилення ризиків. Встановлено, що формалізація загроз у межах реєстру ризиків з індикаторами й планами реагування переводить проблему лояльності з рівня загальних соціально-психологічних оцінок на рівень керованих ризикових категорій. Доведено, що така інтеграція посилює стійкість операційних процесів і знижує ймовірність втрат, пов'язаних із технологічними порушеннями та комплаєнс-відхиленнями.

Дістали подальшого розвитку понятійно-категоріальний апарат інформаційно-аналітичного забезпечення оцінювання лояльності персоналу в системі економічної безпеки промислових підприємств, зокрема уточнено зміст понять «економічна безпека промислового підприємства», «інформаційно-аналітичне забезпечення економічної безпеки», «лояльність персоналу», «індекс лояльності», «модель інтеграції результатів оцінювання лояльності персоналу в систему забезпечення економічної безпеки промислового підприємства». Це забезпечило узгоджений підхід до аналізу ризиків людського чинника та побудови алгоритмів оцінювання і моніторингу, які поєднують порогову

інтерпретацію результатів і їх перетворення у керовані тригери дій. Доведено, що саме формалізація понять дозволяє поєднувати якісні спостереження та кількісні індикатори в єдиній управлінській логіці.

Дістали подальшого розвитку підходи до сценарного управління в системі економічної безпеки через кількісне описання впливу лояльності персоналу на інтегральний рівень безпеки. Запропоновано використання чутливостей та еластичностей показників до змін лояльності, а також підхід до калібрування впливу на панельних даних із контролем зовнішніх факторів і можливістю врахування нелінійних ефектів у різних зонах шкали безпеки. Обґрунтовано, що сценарні розрахунки надають можливість оцінювати очікуваний ефект програм підвищення лояльності на ключові процесні та фінансові результати. Показано, що сценарний підхід посилює прогностичну спроможність управління, оскільки дозволяє порівнювати альтернативні інтервенції та пріоритизувати ресурси залежно від чутливості критичних процесів до людського чинника.

Отримані результати мають теоретичне і практичне значення для розвитку підходів до економічної безпеки промислових підприємств, оскільки пропонують формалізований спосіб включення людського чинника до системи управління ризиками. У дисертація доводить, що інформаційно-аналітичне забезпечення оцінювання лояльності персоналу є важливим інструментом управління загрозами економічній безпеці, який підтримує довгострокову стійкість виробничих процесів і конкурентоспроможність підприємства.

Ключові слова: економічна безпека підприємства; промислове підприємство; інформаційно-аналітичне забезпечення; лояльність персоналу; індекс лояльності; кадрова безпека; управління персоналом; управління ризиками; ранні попереджувальні індикатори; відкриті джерела даних; нефінансові індикатори; комплаєнс-ризики; управлінські інтервенції; етичні та правові вимоги; добробут працівників.

ABSTRACT

Zlobin K.V. **Information and analytical support for assessing personnel loyalty in the system of economic security of industrial enterprises**. Qualification scientific work as a manuscript.

Dissertation for the degree of Doctor of Philosophy in specialty 073 Management. Higher Educational Institution "KROK University". Kyiv, 2026.

The dissertation research is devoted to developing information and analytical support for assessing staff loyalty that can interpret its results as early warning signals of the impact of threats on the economic security system of industrial enterprises, thereby enabling the translation of analytics into managerial decisions.

The relevance of the topic is determined by the fact that the traditional use of personnel indicators and periodic reporting often has a fragmented nature and does not ensure timely identification of risk deviations in personnel behavior. The paper substantiates that personnel loyalty can act as an early risk signal that precedes operational disruptions, quality losses, occupational safety incidents, violations of regulations and compliance requirements. Therefore, the focus is on the task of transferring loyalty from the plane of "soft" descriptive characteristics to the plane of formalized indicators, thresholds, and regulated managerial actions. The methodological logic of the research is based on a systemic combination of data, procedures, responsibilities, and rules for interpreting results. The practical orientation of the work consists in creating a controlled contour that ensures regular measurement of loyalty, its analytical interpretation, integration into an index model of economic security, and the launch of managerial interventions with effect control.

The scientific novelty of the obtained results lies in the formation of an authorial concept of information and analytical support for assessing personnel loyalty as an element of the system of economic security of an industrial

enterprise, which ensures the transition from disparate HR metrics to formalized indices and regulated managerial actions. For the first time, a holistic concept of information and analytical support for the economic security of an industrial enterprise is proposed as an institutionalized sociotechnical contour of data, processes, and roles, integrated with ERM, BCM, ISMS, and the cycle "monitoring – analysis – decision – action – learning". This approach makes it possible to interpret information and analytical support not as a descriptive and reporting function, but as a mechanism for transforming information about threats, vulnerabilities, and opportunities into reproducible managerial actions with defined responsibility. Within the proposed concept, a methodology for assessing the state of economic security based on open sources has been developed, with a transparent formula of the integral index S, a combination of quantitative and qualitative blocks, and discrete interpretation thresholds. The conclusions of the study confirm that the combination of financial and non-financial signs of vulnerability increases the managerial applicability of the integral assessment, since it allows earlier identification of risk zones even before problems manifest in financial reporting. It has been proven that the standardization of indicators, glossaries, and data aggregation rules ensures comparability of results over time and across departments, and also reduces the risk of inconsistent data interpretation.

For the first time, an authorial sociotechnical model of integrating the results of assessing personnel loyalty into the system of managing threats to economic security is proposed as a unified decision-making contour. In the model, loyalty is interpreted as a multidimensional characteristic that includes affective, normative, and instrumental dimensions, and is considered a leading indicator for anticipatory management. A mathematical mechanism for incorporating the loyalty index into the integral index of economic security through a transfer function, aggregated sensitivity, and scenario calculations has been formalized. This provides a reproducible link between behavioral characteristics of personnel

and the enterprise’s financial, operational, and risk metrics. The results of generalization show that integrating loyalty into the contour of economic security reduces the time lag between the emergence of weak signals and managerial response, strengthens the preventive nature of decisions, and increases the controllability of human-factor risks. It is substantiated that such integration is especially important for industrial enterprises, where discipline in the execution of technological procedures and compliance with regulations directly affect operational reliability.

The structural and functional architecture of information and analytical support for the economic security of an enterprise has been improved by detailing the operational functions of the contour. The difference from existing approaches is the orientation not toward descriptive reporting support, but toward a regulated management cycle with defined procedures for standardizing indicators and glossaries, consolidating data, forming early warning indicators and key risk indicators, prioritizing threats, scenario modeling, forming an evidence base, and organizational learning. This makes it possible to ensure the reproducibility of decisions, accountability of responsibilities, and the systemic transformation of analytics into managed actions. The dissertation conclusions prove that the transition to such a cycle changes the role of analytics from recording the state to a tool for managing deviations. It is shown that feedback through repeated measurements is critical for assessing the effectiveness of interventions and adjusting thresholds, weights, and escalation rules. It is specified that without a regulated architecture, measurement results lose managerial value because they do not form a clear logic "identified – explained – assigned responsible party – action performed – effect verified".

The methodological approach to assessing the economic security of an enterprise has been improved by balancing quantitative financial coefficients with qualitative signs, in particular by taking into account the nature of the audit opinion, the presence of covenants, legal and regulatory risks, and the

transparency of information disclosure. Unlike traditional methods in which financial metrics and retrospective diagnostics dominate, the proposed approach increases the sensitivity of the integral assessment to non-financial sources of vulnerabilities. This makes it possible to more accurately identify critical risk zones and choose targeted managerial measures depending on the nature of deviations. The conclusions of the study confirm that for industrial enterprises, non-financial features often act as the first signals of degradation in process controllability, which later transforms into financial losses. It has been proven that the combination of quantitative and qualitative blocks contributes to decision-making focused on the causes of risk rather than only on the consequences.

The tools for operationalizing personnel loyalty have been improved through a combination of survey-based and behavioral indicators, normalization of indicators to the interval [0;1], verification of internal consistency, and weighting by reliability and strategic relevance for the specific technological system of the enterprise. Unlike practices where one-time surveys or fragmented indicators prevail without a single scale and verification, the proposed toolkit ensures comparability of results over time and across departments. This makes it possible to reduce the impact of subjective distortions and increase the suitability of loyalty assessment for risk management. The dissertation conclusions show that it is the combination of psychometric and behavioral data that increases measurement validity in the industrial environment, where loyalty is manifested through discipline, responsibility, readiness to follow procedures, and support change. It is substantiated that regularity of measurements and clear threshold interpretation are conditions under which loyalty can function as an early risk signal.

The logic of integrating the human factor into the system of economic security has been improved through regulated linking of loyalty assessment results with the risk register and a set of managerial interventions. The difference

is the presence of thresholds, response scenarios, risk owners, and defined response horizons, whereas in many approaches personnel indicators are used in isolation from the risk register. This makes it possible to reduce the time lag between the emergence of weak signals and intervention, increase the preventive nature of decisions, and control the effect of interventions through repeated measurements. The study conclusions complement this novelty by systematizing internal and external threats implemented through personnel and substantiating the role of low loyalty as a factor that amplifies risks. It is shown that formalizing threats within the risk register with indicators and response plans transfers the problem of loyalty from the level of general socio-psychological assessments to the level of managed risk categories. It has been proven that such integration strengthens the resilience of operational processes and reduces the likelihood of losses associated with technological violations and compliance deviations.

Further development was gained by the conceptual and categorical apparatus of information and analytical support for assessing personnel loyalty in the system of economic security of industrial enterprises, in particular, the content of the concepts "economic security of an industrial enterprise", "information and analytical support for economic security", "personnel loyalty", "loyalty index" has been уточнено. This ensured a coherent approach to analyzing human-factor risks and to building algorithms for assessment and monitoring that combine threshold interpretation of results and their transformation into managed action triggers. The dissertation conclusions confirm that without terminological coherence it is impossible to achieve uniform interpretation of data and correct escalation of deviations between departments. It is shown that уточнення of categories supports the formation of a single glossary of indicators and data aggregation rules, and also creates prerequisites for automating calculations and digital analytics. It has been proven that it is the formalization of concepts that makes it possible to combine qualitative observations and quantitative indicators into a unified managerial logic.

Further development was gained by approaches to scenario management in the system of economic security through a quantitative description of the impact of personnel loyalty on the integral level of security. The use of sensitivities and elasticities of indicators to changes in loyalty is proposed, as well as an approach to calibrating this impact on panel data with control of external factors and the possibility of taking into account nonlinear effects in different zones of the security scale. The study conclusions substantiate that scenario calculations provide an opportunity to assess the expected effect of loyalty improvement programs on key process and financial results. It is shown that the scenario approach strengthens the prognostic capacity of management because it allows comparing alternative interventions and prioritizing resources depending on the sensitivity of critical processes to the human factor. It has been proven that such logic supports the transition from reactive response to anticipatory management of threats to economic security.

The obtained results have theoretical and practical significance for the development of approaches to the economic security of industrial enterprises, as they propose a formalized way of incorporating the human factor into the risk management system. In conclusion, the work proves that information and analytical support for assessing personnel loyalty is an important tool for managing threats to economic security, which supports long-term stability of production processes and the competitiveness of the enterprise in an unstable business environment.

Keywords: enterprise economic security; industrial enterprise; information and analytical support; personnel loyalty; loyalty index; personnel security; human resource management; risk management; early warning indicators; open data sources; non-financial indicators; compliance risks; managerial interventions; ethical and legal requirements; employee wellbeing.

Публікації, в яких опубліковані основні наукові результати дисертації:

1. Злобін К. (2025). Сучасні підходи до оцінювання лояльності персоналу в контексті економічної безпеки. *Актуальні проблеми економіки*. № 10 (292), жовтень, 2025. DOI: 10.32752/1993-6788-2025-1-292-172-181 (Google Scholar, Dimensions) (0,8 др.арк.).

2. Zlobin, K. (2025). Model of Integration of Loyalty Assessment Results into the Threat Management System of the Economic Security of an Industrial Enterprise. In P. Kolisnichenko (Ed.), *Insider threats and security in corporations*. 274p. (pp. 181–203). Scientific Center of Innovative Research. DOI: https://doi.org/10.36690/ITSC-181-203 (Google Scholar, Dimensions) (1,5 др.арк.).

3. Злобін К. (2024). Вплив війни в Україні на лояльність персоналу підприємств до роботодавців. *Вчені записки Університету "КРОК"*. № 2(74), С. 217–227. DOI: https://doi.org/10.31732/2663-2209-2024-74-217-227 (Index Copernicus, Google Scholar, Dimensions, OpenAire) (0,8 др.арк.).

4. Zlobin K. (2024). Information and analytical support and tools for assessing employee loyalty in enterprises. *Economics, Finance and Management Review*. 2024. № 2(18), P. 60-72. DOI: https://doi.org/10.36690/2674-5208-2024-2-60-72 (Index Copernicus, Google Scholar, Dimensions, OpenAire) (0,8 др.арк.).

5. Злобін, К., Літвін, Н., & Бурлакова, І. (2023). Вплив програм wellbeing на продуктивність та лояльність персоналу. *Вчені записки Університету «КРОК»*, (1(69), 162–170. https://doi.org/10.31732/2663-2209-2022-69-162-170 (Index Copernicus, Google Scholar, Dimensions, OpenAire) (0,7 др.арк., в т.ч. автору належить 0,3 др. арк.).

Публікації, які засвідчують апробацію матеріалів дисертації:

1. Zlobin K. (2024). The impact of involving employees in decision-making on increasing the loyalty of the company's personnel. *International Conference on*

Corporation Management: book of abstract (April 26, 2024). Estonia, https://conf.scnchub.com/index.php/ICCM/ICCM-2024/paper/view/740/208 (Google Scholar, Dimensions) (0,3 др.арк.)

2. Злобін К.В. (2024). Ідентифікація ризиків економічної безпеки через персонал. *Держава, регіони, підприємництво: інформаційні, суспільно-правові, соціально-економічні аспекти розвитку: тези доповідей VI Міжнародної конференції* (грудень 5-6, 2024). Київ: Університет "КРОК". https://conf.krok.edu.ua/SRE/SRE-2024/paper/view/2638 (Google Scholar) (0,3 др.арк.)

3. Злобін К.В. (2024). Вплив лояльності персоналу на довгострокове стратегічне планування компанії. Сучасний менеджмент організації: витоки, реалії та перспективи розвитку: тези доповідей IV Наукової конференції (18 квітня 2024 р.). Київ: Університет "КРОК". https://conf.krok.edu.ua/MMO/MMO-2024/paper/view/2235 (Google Scholar) (0,3 др.арк.)

4. Zlobin K. (2023). Personnel well-being as a component of the social policy of the company. *Relationship between public administration and business entities management: book of abstract* (November 24, 2023). Estonia. https://conf.scnchub.com/index.php/RPABM/RPABM-2023/paper/view/600/83 (Google Scholar, Dimensions) (0,3 др.арк.)

ЗМІСТ

ВСТУП

Актуальність теми. Актуальність теми дисертації зумовлена тим, що промислові підприємства функціонують у середовищі високої невизначеності, де поєднуються цінова волатильність енергоресурсів, фрагментація ланцюгів постачання, геоекономічні обмеження, а також прискорена цифровізація виробництва й зростання кіберзагроз. За таких умов економічна безпека набуває характеру інтегральної здатності системи своєчасно ідентифікувати загрози, запобігати їх матеріалізації, витримувати вплив реалізованих ризиків і відновлювати цільові параметри функціонування без критичної втрати вартості та керованості.

Водночас у практиці управління безпекою досі домінує акцент на фінансових показниках і ретроспективній діагностиці, тоді як джерела ризиків дедалі частіше мають соціотехнічну природу та проявляються через поведінкові відхилення, збої в дисципліні процесів і деградацію організаційної культури. У цій логіці особливого значення набуває лояльність персоналу як характеристика, що впливає на комплаєнс, якість виконання процедур, стабільність виробничих режимів і готовність підтримувати зміни. Теоретична передумова авторської моделі полягає у визнанні лояльності ведучим індикатором, який передує змінам у ключових показниках ризику, операційних коефіцієнтах і фінансових результатах, а отже може бути основою для випереджального управління загрозами.

Саме тому проблема інформаційно-аналітичного забезпечення оцінювання лояльності персоналу в системі економічної безпеки промислових підприємств є науково та практично значущою, а її розв’язання потребує узгодження категоріального апарату, методів вимірювання, процедур інтеграції результатів у ризик-контур і вимог до якості даних.

Теоретичні основи вивчення економічної безпеки підприємств у своїх наукових працях досліджували Г. В. Козаченко, В. П. Пономарьов, О. М. Ляшенко, В.Г. Алькема, З.Б. Живко, М.І. Копитко, О.С. Кириченко, В.І. Франчук, С.І. Мельник, Н. П. Сисоліна, М. І. Небава, Ю. В. Міронова, Б. С. Дуб, Т. О. Меліхова, М. Шмалій, В. Шинкар, В. Орлик, В. Панченко, а також T. Primorac, T. Kozina, I. Turčić та інші. У їхніх роботах економічна безпека інтерпретується як поєднання стану захищеності та системи управлінських механізмів, що забезпечують стійкість підприємства в умовах загроз і потребують безперервного моніторингу та діагностики ризиків.

Питання оцінювання лояльності персоналу вивчали J.P. Meyer і N.J. Allen, D.W. Organ, N.P. Podsakoff, P.M. Blau, R. Eisenberger, J.A. Colquitt, а також І.П. Мігус, О.О. Наумова, О.П. Панченко та інші. Їхні напрацювання формують підґрунтя для трактування лояльності як багатовимірної організаційної прихильності та як поведінкового феномена, що проявляється у проорганізаційних діях і підтримується механізмами соціального обміну та справедливості.

Стан наукової розробленості проблематики засвідчує наявність окремих дослідницьких ліній, однак їхня інтеграція залишається недостатньою. У сучасній літературі інформаційно-аналітичне забезпечення економічної безпеки дедалі частіше трактується не як пасивний інформаційний супровід, а як соціотехнічний контур, що поєднує джерела даних, методи аналітики, правила доступу й підзвітності та процедури прийняття рішень за ризиками.

У межах цього підходу ключовими стають ранні попереджувальні індикатори та ключові індикатори ризику з порогами й наперед визначеними діями, а також інституціоналізація функцій стандартизації показників, консолідації даних, сценарного моделювання і формування доказової бази для рішень. Разом з тим кадровий вимір безпеки в промисловості часто подається фрагментарно, переважно через показники

плинності чи дисциплінарних інцидентів, без методично цілісного зв’язку з інтегральною оцінкою безпеки та без регламентованого використання результатів у системі управління загрозами. Запропоноване у дисертації бачення усуває цю роз’єднаність через побудову відтворюваного контуру, в якому валідоване вимірювання лояльності поєднується з формалізованим передатним механізмом у процесні та фінансові показники, пороговою інтерпретацією індексів і регламентованими управлінськими діями. Додатково актуалізується вимога до етичності й якості даних, оскільки робота з персоналом передбачає підвищені ризики неправомірного використання інформації, що потребує політик згоди, знеособлення, рольового доступу й журналів аудиту.

У сукупності це формує *наукове завдання*, яке полягає у розробленні інформаційно-аналітичного забезпечення оцінювання лояльності персоналу, здатного інтерпретувати її результати як ранні сигнали впливу деструктивних чинників на систему економічної безпеки промислових підприємств, що дозволить переводити аналітику в управлінські рішення.

Зв’язок роботи з науковими програмами, планами, темами. Дисертаційну роботу виконано відповідно до плану науково-дослідних робіт ВНЗ «Університет економіки та права «КРОК», зокрема в межах наукової теми «Науково-методичні засади реалізації сучасних концепцій та технологій управління підприємствами, установами та організаціями в умовах економічного відновлення і глобалізованого розвитку» (номер державної реєстрації 0122U201378). У межах зазначеної тематики автором здійснено комплексний аналіз інформаційно-аналітичного забезпечення як інструмента підтримки управлінських рішень у системі економічної безпеки промислових підприємств, з акцентом на оцінюванні лояльності персоналу як індикатора кадрових ризиків і стійкості виробничо-управлінських процесів. Це дало змогу обґрунтувати авторський підхід до організації збору, верифікації та інтерпретації даних про лояльність, а також

визначити механізми інтеграції результатів оцінювання у контур управління загрозами економічній безпеці та сформувати практико-орієнтовані рекомендації щодо впровадження відповідного інструментарію на промислових підприємствах.

Мета і завдання дослідження. Метою дисертаційної роботи є розроблення теоретико-методологічних засад та прикладного інструментарію інформаційно-аналітичного забезпечення оцінювання лояльності персоналу в системі економічної безпеки промислових підприємств з орієнтацією на випереджальне управління деструктивними чинниками.

Досягнення поставленої мети зумовило необхідність розв'язання взаємопов'язаних завдань, серед яких:

- вивчення теоретичних підходів до трактування поняття інформаційно-аналітичного забезпечення економічної безпеки суб'єктів господарювання;
- встановлення ролі та місця управління персоналом в системі економічної безпеки промислових підприємств;
- дослідження сучасних підходів до оцінювання лояльності персоналу в контексті економічної безпеки;
- вивчення сучасного стану економічної безпеки промислових підприємств;
- аналіз інструментів оцінювання лояльності персоналу та її впливу на економічну безпеку промислових підприємств;
- ідентифікація внутрішніх та зовнішніх загроз економічній безпеці промислових підприємств з боку персоналу;
- розробка моделі інтеграції результатів оцінювання лояльності в систему забезпечення економічної безпеки промислових підприємств;
- розробка процесної архітектури моделі інтеграції результатів оцінювання лояльності в систему забезпечення економічної безпеки промислових підприємств;

- визначення вимог до етичних, правових та організаційних аспектів використання результатів оцінювання лояльності персоналу для забезпечення економічної безпеки промислових підприємств.

Об'єктом дослідження є система економічної безпеки промислових підприємств у частині її інформаційно-аналітичного забезпечення оцінювання лояльності персоналу.

Предметом дослідження є методи, моделі та організаційно-технологічні процедури інформаційно-аналітичного забезпечення оцінювання лояльності персоналу.

Методи дослідження. Теоретико-методичною основою дослідження виступають положення системного підходу до управління економічною безпекою, концепції соціотехнічних систем і управління даними, підходи ризик-орієнтованого управління, а також методи композитного індексування та сценарної аналітики.

У роботі використано методи логічного узагальнення і систематизації для уточнення категоріального апарату (пп.1.1, 1.2 та 1.3); методи індексного моделювання для побудови інтегральних показників (пп.1.3, 2.1 та 2.2); методи нормування, зважування та порогової інтерпретації для забезпечення керованості результатів; статистичні та економетричні підходи для оцінювання зв'язків і підтвердження прогностичної функції індексів на основі подійних даних (пп.2.2 та 3.1); методи контролю якості даних для забезпечення повноти, узгодженості, недубльованості та коректної часової прив'язки показників (пп.3.2 та 3.3); метод узагальнення – для формулювання висновків.

Інформаційною базою дослідження є відкриті дані фінансової звітності промислових підприємств, аудиторські звіти та примітки до фінансової звітності, внутрішні HR метрики.

Наукова новизна дисертаційного дослідження. Наукова новизна одержаних результатів полягає у формуванні авторської концепції

інформаційно-аналітичного забезпечення оцінювання лояльності персоналу як складової системи економічної безпеки промислового підприємства, що забезпечує перехід від фрагментарних HR-метрик до формалізованих індексів і регламентованих управлінських дій. Основні результати дослідження відображають наступні аспекти:

уперше:

- запропоновано цілісну авторську концепцію інформаційно-аналітичного забезпечення економічної безпеки промислового підприємства як інституціоналізованого соціотехнічного контуру даних, процесів і ролей, інтегрованого з ERM, BCM, ISMS та циклом «моніторинг – аналіз – рішення – дія – навчання», у межах якого розроблено методику оцінювання стану економічної безпеки на основі відкритих джерел із прозорою формулою інтегрального індексу S, поєднанням кількісного та якісного блоків, дискретними порогами й відтворюваним дизайном розрахунків;
- запропоновано авторську соціотехнічну модель інтеграції результатів оцінювання лояльності персоналу в систему забезпечення економічної безпеки як єдиного контуру прийняття рішень, у якому лояльність інтерпретується як багатовимірна характеристика (афективний, нормативний, інструментальний виміри) і як ведучий індикатор для випереджального управління, та обґрунтовано і формалізовано математичний механізм включення індексу лояльності до інтегрального індексу економічної безпеки через передатну функцію, агреговану чутливість і сценарні розрахунки, що забезпечує відтворюваний зв’язок між поведінковими характеристиками персоналу та фінансовими, операційними і ризиковими метриками;

удосконалено:

- структурно-функціональну архітектуру інформаційно-аналітичного забезпечення економічної безпеки підприємства шляхом деталізації

операційних функцій контуру, що відрізняється від наявних підходів орієнтацією не на описово-звітний супровід, а на регламентований управлінський цикл із визначеними процедурами стандартизації показників і словників, консолідації даних, формування ранніх попереджувальних індикаторів і ключових індикаторів ризику, пріоритизації загроз, сценарного моделювання, формування доказової бази та організаційного навчання, що дозволяє забезпечити відтворюваність управлінських рішень, підзвітність відповідальностей і системне перетворення аналітики на керовані дії;

- методичний підхід до оцінювання економічної безпеки підприємства шляхом збалансування кількісних фінансових коефіцієнтів із якісними ознаками (характер аудиторської думки, наявність ковенантів, юридичні та регуляторні ризики, прозорість розкриття інформації), що відрізняється від традиційних методик домінуванням фінансових метрик та ретроспективної діагностики без врахування нефінансових джерел уразливостей, і дозволяє підвищити чутливість інтегральної оцінки до ранніх сигналів проблем, точніше визначати критичні зони ризику та обирати адресні управлінські заходи;

- інструментарій операціоналізації лояльності персоналу через поєднання опитувальних і поведінкових індикаторів, нормування показників до інтервалу [0;1], перевірку внутрішньої узгодженості та зважування за надійністю і стратегічною релевантністю для конкретної технологічної системи підприємства, що відрізняється від існуючих практик переважанням лише анкетних вимірювань або фрагментарних кадрових метрик без єдиної шкали, верифікації та прозорої вагової логіки, і дозволяє отримувати порівнювані в часі та між підрозділами результати, зменшувати вплив суб’єктивних викривлень і підвищувати придатність оцінки лояльності для управління ризиками;

- логіку інтеграції людського чинника в систему економічної безпеки шляхом регламентованого зв’язування результатів оцінювання лояльності з реєстром ризиків та набором управлінських інтервенцій, що відрізняється від наявних підходів, у яких кадрові показники використовуються ізольовано від ризик-реєстру та не мають визначених порогів і сценаріїв реагування, і дозволяє скоротити часовий лаг між появою слабких сигналів і управлінським втручанням, підвищити превентивність рішень та забезпечити контроль ефекту інтервенцій через повторні вимірювання;

дістали подальшого розвитку:

- понятійно-категоріальний апарат інформаційно-аналітичного забезпечення оцінювання лояльності персоналу в системі економічної безпеки промислових підприємств, зокрема уточнено зміст понять: «економічна безпека промислового підприємства»; «інформаційно-аналітичне забезпечення економічної безпеки»; «лояльність персоналу»; «індекс лояльності», «модель інтеграції результатів оцінювання лояльності персоналу в систему забезпечення економічної безпеки промислового підприємства», що сформувало узгоджений підхід до аналізу ризиків людського чинника та побудови алгоритмів оцінювання і моніторингу, які поєднують порогову інтерпретацію результатів та їх перетворення у керовані управлінські категорії і тригери дій, а також створюють передумови для автоматизації розрахунків і впровадження цифрової аналітики у форматі електронних таблиць та BI-панелей на основі відкритих джерел і формалізованих правил агрегації;
- систематизація інструментарію сценарного управління в системі економічної безпеки через кількісне описання впливу лояльності персоналу на інтегральний рівень безпеки, зокрема шляхом введення чутливостей та еластичностей показників до змін лояльності, а також через підхід до калібрування цього впливу на панельних даних із контролем зовнішніх

факторів і можливістю врахування нелінійних ефектів у різних зонах шкали безпеки.

Практичне значення отриманих результатів. Практичне значення результатів полягає у можливості впровадження розробленого інформаційно-аналітичного забезпечення як керованого контуру для промислових підприємств різних галузей, з орієнтацією на зменшення частоти інцидентів, стабілізацію випуску та підвищення резилієнтності в умовах невизначеності.

Результати дисертаційного дослідження використано в діяльності підприємств і консалтингової організації, що підтверджено відповідними довідками про впровадження, зокрема:

- ТОВ «ЕНЕРДЖІ ТРЕЙД ГРУП» (довідка N345/КП від 27.11.2025), де упроваджено методичні положення оцінювання стану економічної безпеки промислового підприємства на основі інтегрального індексу, сформованого як зважене поєднання кількісного та якісного блоків із використанням відкритих джерел даних, а саме фінансової звітності, аудиторського звіту та приміток, що підвищило відтворюваність розрахунків, порівнюваність результатів у часі та придатність висновків для управлінського моніторингу і визначення пріоритетів заходів.
- ТОВ «ПАУЕР ДЕВЕЛОПМЕНТ» (довідка №54 від 05.12.2025), де застосовано рекомендації щодо оцінювання лояльності персоналу як чинника стабільності операцій і зниження кадрових ризиків із поєднанням кількісних і якісних інструментів, зокрема стандартизованих опитувань, аналізу плинності кадрів і відсутностей, інтерв’ю та фокус-груп, контент-аналізу внутрішніх каналів зворотного зв’язку з відображенням результатів в аналітичних панелях, що посилило узгодженість рішень між функцією управління персоналом і функцією економічної безпеки та підтримало планування заходів утримання критичних компетенцій.

- ТОВ «РИЗИК КОНТРОЛЬ» (довідка №012/1-25 від 30.12.2025 р.), де підтверджено доцільність використання результатів дослідження для скринінгу, моніторингу та управлінського реагування в оцінюванні економічної безпеки підприємств, з акцентом на застосуванні інтегрального індексу економічної безпеки та врахуванні кадрового чинника через оцінювання лояльності персоналу як елемента ризикового профілю підприємства.

Запропоновані в дисертації методики та інструменти можуть бути використані службами управління персоналом, економічної безпеки, ризик менеджменту та внутрішнього контролю промислових підприємств, а також консалтинговими компаніями й науковцями. Вони забезпечують практично застосовне оцінювання економічної безпеки на основі відкритих даних і придатні для реалізації в електронних таблицях або BI панелях. Інтеграція оцінювання лояльності персоналу в контур управління загрозами дає змогу зменшувати ризики людського чинника та підвищувати стійкість виробничих процесів через порогову інтерпретацію, ескалацію та типові управлінські дії.

Особистий внесок здобувача. Дисертаційна робота є одноосібною науковою працею, у якій основні наукові положення, висновки та рекомендації, що виносяться на захист, одержані автором особисто. Внесок здобувача у працях, опублікованих у співавторстві, конкретизовано в переліку публікацій. Особистим внеском автора є комплексне обґрунтування та розроблення концептуальних і практичних засад інформаційно-аналітичного забезпечення оцінювання лояльності персоналу в системі економічної безпеки промислових підприємств, включно з уточненням понятійно-категоріального апарату, формуванням методики інтегрального оцінювання стану економічної безпеки на основі відкритих джерел, побудовою індексу лояльності та формалізацією

механізму його інтеграції в контур управління загрозами через сценарні розрахунки і порогову інтерпретацію результатів.

Апробація матеріалів дисертації. Основні направлення та положення проведених досліджень були апробовані на науково-практичних конференціях різного рівня, зокрема міжнародних: Міжнародна науково-практична конференція «4th International Conference on corporation management» (2024), «Relationship between public administration and business entities managemen» (2023), Держава, регіони, підприємництво: інформаційні, суспільно-правові, соціально-економічні аспекти розвитку (2024), International Conference on Corporation Management (2020), Сучасний менеджмент організації: витоки, реалії та перспективи розвитку (2024).

Публікації. Основні положення та результати дисертаційного дослідження опубліковані у 9 наукових працях загальним обсягом 4,72 др. арк., з яких особисто автору належить 4,32 друк. арк., у тому числі 4 статті, з яких 3 статті – у наукових фахових виданнях України, 1 - у виданнях іноземних держав, 1 одноосібний розділ у колективній монографії, виданій за кордоном, а також 4 – матеріали участі у науково-практичних конференціях різного рівня.

Структура та обсяг дисертації. Дисертація викладена на 288 сторінках та складається зі вступу, трьох розділів, висновків, списку використаних джерел та додатків. Обсяг основного тексту становить 247 сторінок, 4 додатки на 26 сторінках, список використаних джерел з 224 найменувань. Матеріали дисертації містять 45 таблиць та 32 рисунки.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ ОЦІНЮВАННЯ ЛОЯЛЬНОСТІ ПЕРСОНАЛУ В СИСТЕМІ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПРОМИСЛОВИХ ПІДПРИЄМСТВ

1.1. Теоретичні підходи до трактування поняття інформаційно-аналітичного забезпечення економічної безпеки суб'єктів господарювання

У ранніх дослідженнях «економічну безпеку підприємств» (ЕБП) переважно інтерпретували як стан захищеності від внутрішніх і зовнішніх загроз, з основним акцентом на мінімізації втрат та запобіганні деструктивним впливам. У 2000–2010-х роках у науково-практичний дискурс входять рамки Enterprise Risk Management (ERM) та стандарти ISO 31000, які зміщують фокус від реактивної охорони до проактивного управління ризиками, інтегрованого зі стратегією та результативністю. Паралельно розвивається підхід organizational resilience (Hollnagel та ін.), що підкреслює спроможність організації передбачати, моніторити, відповідати та навчатися; у менеджмент-практиках його підсилюють вимоги ISO 22301 щодо забезпечення безперервності бізнесу. Сукупність зазначених трансформацій формує сучасне бачення ЕБП як динамічної організаційної спроможності підтримувати цінність і цілісність компанії в умовах турбулентності, спираючись на дані, випереджальні індикатори й ключові ризик-показники (EWI/KRI) та замкнений цикл «моніторинг - аналіз - рішення - дія - навчання».

У вітчизняній та зарубіжній літературі економічну безпеку підприємства (ЕБП) трактують у кількох взаємодоповнювальних оптиках, що еволюціонують від «статичного стану» до «динамічної спроможності». Канонічно ЕБП подається як бінарна конструкція «стан + механізм

забезпечення», де інтегруються нормативно-правові, організаційні та економічні інструменти (Козаченко, Пономарьов, Ляшенко, 2003); подальші студії конкретизують її як керований управлінський цикл, зорієнтований на стійкість і розвиток (Сисоліна, 2014), або як управлінську підсистему з регламентами, ролями та інтегральною оцінкою рівня безпеки (Небава, Міронова, 2017). Освітньо-методичні підходи нормалізують понятійне поле, структуру загроз і принципи безпеки на мікрорівні (Дідик, 2020), тоді як узагальнювальні моделі наголошують на спроможності нейтралізації дестабілізаторів, зміщуючи акцент від «броні» до динамічної витривалості (Кургузенкова, 2015).

Системні й інституційні трактування фіксують принципи, функції, декомпозицію підсистем і маршрути взаємодії, підсилюючи легітимність та підзвітність безпекової функції (Дуб, 2016; Шульга, 2010). Фінансовоцентричні підходи висувають ядро ліквідності, платоспроможності та рентабельності з чіткими KPI для менеджменту й інвесторів, але ризикують редукціонізмом щодо людського й операційного вимірів (Орлик, 2017). Стейкхолдерсько-процесні рамки інтегрують ЕБП у системи менеджменту та стратегічні карти, формалізують ролі роботи з даними, SLA та пороги ескалації (Панченко, 2017). Концепція «комплексної здатності» зближує ЕБП із парадигмою резилієнс, але потребує галузевих KRI та стабільності інтегральних індексів (Шмалій, 2019). Контрольно-аудиторні підходи підвищують дисципліну рішень, однак без предиктивної аналітики ризикують запізненням реакцій (Меліхова, 2018). Історіографічні огляди фіксують еволюцію дефініцій, та цифрові ризики й вимоги XAI ще потребують глибшої операціоналізації (Архипенко, Іванова, 2021).

Подальші розробки деталізують методики оцінювання та індикаторні системи з урахуванням ERM-логіки (Шинкар, 2020; Андрієнко, 2014), галузевої специфіки (Пушак та ін., 2021), організаційно-економічних механізмів і інституціоналізації інформаційних потоків (Алькема, 2015–

2017; Лаптєв, 2017; Захаров, 2016, 2019; Кириченко, 2012). ESG- і сталий вимір додають трикутник «інтереси–загрози–ресурси», однак потребують кількісних KRI та сценарних матриць (Гривківська та ін., 2021). Оновлення канону через цифрову складову – кіберризики, залежність від IT-ланцюгів, OT/SCADA – відповідає викликам Industry 4.0, але потребує метрик і пояснюваних моделей (Самойленко та ін., 2023; Tereshchenko, 2021). Міжнародні підходи посилюють дефініційну ясність і композитні рамки «стану/спроможності», підкреслюючи ресурсно-ефективнісний і підприємницько-сталісний ракурси, однак часто бракує практичних ваг і порогів для впровадження (Primorac, Kozina, Turčić, 2018; Ianioglo, Polajeva, 2015–2017; Smelík, 2020; Rabotin, 2022; Kowalska, Matera, 2024; Stańczyk, 2020). Узагальнюючи, поле рухається від нормативно-дефініційних описів до даноцентричних, процесно- та ризик-орієнтованих моделей, що поєднують індикатори, KRI і цифрову аналітику в єдину керовану архітектуру ЕБП.

Підсумовуючи, економічну безпеку підприємства доцільно розуміти водночас як досягнутий стан захищеності та як спроможність підтримувати цю захищеність у динаміці, реагуючи на мінливі загрози. Систематизований перелік вищезазначених трактувань поняття «економічна безпека підприємства» представлено у таблиці В.1 Додатку В.

Розбіжності у літературі зводяться до різних підходів, систематизованих у таблиці 1.1. Узгодження окреслених ракурсів є можливим у межах інтеграційної рамки, у якій «стан» визначає ціль, а «спроможність» - механізм її досягнення та підтримання.

За результатами дослідження економічну безпеку промислового підприємства доцільно визначати як інституціоналізовану соціотехнічну здатність і водночас стан, що забезпечують стабільне досягнення стратегічних цілей і формування довгострокової цінності попри внутрішні та зовнішні загрози.

Таблиця 1.1

Основні підходи до трактування поняття

«економічна безпека підприємств»

Підхід	Характеристика	Основні автори
Охоронно-захисний	«Вільність від загроз», захист інтересів	Primorac et al., 2018; Козаченко et al., 2003.
Ресурсно-ефективнісний	Ефективне використання ресурсів → стійкість	Smelík, 2020; Ianioglo & Polajeva, 2016–2017.
Процесно-управлінський	Безперервний ERM-цикл моніторингу/рішень	Шинкар, 2020; Панченко, 2017.
Системний	Соціо-технічна система підсистем і ролей	Дуб, 2016; Небава & Міронова, 2017.
Результативно-цільовий	Досягнення цілей/розвитку/конкурентності	Ianioglo & Polajeva, 2016; Меліхова, 2018.
Фінансово-безпековий	Фінстійкість/прибуток як «ядро» ЕБП	Орлик, 2017; Rabotin, 2022.
Стейкхолдерсько-інституційний	Політики, культура даних, підзвітність	Шульга, 2010; Шмалій, 2019.
Резилієнс/BC	Передбачення–відповідь–навчання, безперервність	(узгодження з ISO 22301/Resilience)

Джерело: систематизовано автором на основі (Primorac et al., 2018; Козаченко et al., 2003; Smelík, 2020; Ianioglo & Polajeva, 2016–2017; Шинкар, 2020; Панченко, 2017; Дуб, 2016; Небава & Міронова, 2017; Ianioglo & Polajeva, 2016; Меліхова, 2018; Орлик, 2017; Rabotin, 2022; Шульга, 2010; Шмалій, 2019; ISO 22301/Resilience)

Операціоналізація цього поняття спирається на сучасне інформаційно-аналітичне забезпечення (ІАЗ), яке охоплює: стандартизоване управління даними й ризиками; систему випереджальних індикаторів та ключових ризик-показників (EWI/KRI) з визначеними порогами, процедурами ескалації та сценарними діями; пояснювану аналітику (XAI); політики безперервності та відновлюваності; етико-правові норми взаємодії зі стейкхолдерами.

Така конфігурація переводить категорію з декларативного рівня у площину керованої практики: забезпечується якість, доступність і трасованість даних; усувається ефект «чорної скриньки» у чутливих рішеннях; підтримується збереження критичних функцій і швидке відновлення; результати верифікуються за фінансово-операційними метриками (P&L/CF, продуктивність). Багаторівнева організація (мікро–

мезо-макро) та замкнений цикл «моніторинг - аналіз - рішення - дія - навчання» гарантують безперервне удосконалення. У підсумку економічна безпека постає не як статичний «щит», а як керована організаційна здібність, вимірювана, відтворювана та інтегрована у стратегію, операційну діяльність і культуру підприємства.

У сучасних умовах турбулентності ІАЗ ЕБ дедалі частіше розглядають не як пасивний «інформаційний супровід», а як соціо-технічний контур, що поєднує джерела даних, методи аналітики, правила доступу й підзвітності, а також процедури прийняття рішень за ризиками. Його зрілість визначається не лише переліком показників, а й якістю даних, пояснюваністю моделей, наявністю KRI/EWI із порогами та сценаріями, інтеграцією з виробничими/фінансовими системами та дотриманням етико-правових норм.

Інформаційно-аналітичне забезпечення економічної безпеки (ІАЗ ЕБ) у сучасній літературі трактується як цілісна, керована система, що поєднує дані, процеси та рішення. Концептуально ІАЗ подається як зв’язна архітектура збирання, оброблення й інтерпретації даних для ідентифікації загроз і підтримки управлінських рішень (Кавун, С., 2016) та як елемент організаційного устрою з чітко визначеними потоками, метриками, доступами й ролями (Воронюк, Є., 2021). Технологічний вимір підкреслює BI/DSS-характер ІАЗ, здатний перетворювати внутрішні й зовнішні дані на ранні сигнали ризику, підтримувати сценарний аналіз і дашборди керівників, із інтеграцією з ERP/SCM та вимогами актуальності даних (Крамаренко, К., 2024). Як управлінська підсистема моніторингу, діагностики й інтегральної оцінки ІАЗ спирається на структурно-рольовий дизайн і документування (Небава, М.; Міронова, Ю., 2017), системний розподіл відповідальності (risk owner, аналітик, аудитор) і матриці RACI (Дуб, Б., 2016). Фінансовий контур (KRI, LCR, DSCR) «зшиває» облік, аналіз і контроль, зокрема для казначейства та ковенантів (Онищенко, С.;

Глушко, А., 2023), тоді як обліково-аналітична база забезпечує показники, звітність і план-факт (Краєвський, В., 2020). Галузеві карти даних для гірничих підприємств (Міщук, І., та ін., 2021) і HR-вимір лояльності як ризик-фактора (Мігус, І., 2013; Єфіменко, А., 2024) розширюють предметну специфіку. Стандартизацію понять і критеріїв закладають навчально-методичні рамки та процесно-критеріальні конструкції з паспортами показників і галузевими індикаторами (Дідик, О., 2020; Шинкар, І., 2020; Пушак, Я., та ін., 2021; Гнилицька, Л., 2012, 2013).

Міжнародні рамки закріплюють вимоги до «нервової системи» ІАЗ: контур інформації-комунікації-звітності в ERM (COSO, 2017), структуровану підтримку процесів ризик-менеджменту (ISO 31000, 2018), контроль і безперервне поліпшення в управлінні інформаційними ризиками (ISO/IEC 27001, 2022) та засади data governance – якість, метадані, лінійку даних і рольові моделі (DAMA-DMBOK, 2017/2020). У підході resilience engineering ІАЗ виконує сенсорну функцію передбачення, моніторингу, реагування та навчання (Hollnagel, 2011/2017), а у SCM постає як мережеве «спостереження» за подіями й індикаторами вразливості (Jüttner, 2005).

Технологічна платформа ІАЗ еволює до lakehouse-архітектури з уніфікованим сховищем та аналітикою, версіонуванням і ACID-гарантіями для масштабованих ризик-панелей (Armbrust та ін., 2021); практичні реалізації спираються на екосистеми Delta/Hudi/Iceberg (Jain та ін., 2023). Операційно ІАЗ поєднує методики побудови KRI (релевантність, валідація, частота, пороги) і GRC-оркестрацію ризиків, подій і контролів (AuditBoard, 2024; Thomson Reuters, 2025; MetricStream, 2025), індустріальні практики дашбордів і сценарного моделювання (Deloitte, 2020–2024) та кейс-аналітику інсайдерських загроз (CERT/SEI, Collins та ін., 2016/2020). Додаткові валідовані метрики організаційної прихильності (Meyer & Allen, 1991) можуть бути вхідними даними ІАЗ для оцінювання кадрових ризиків. У підсумку ІАЗ ЕБ постає як інтегрована, стандартизована й технологічно

підтримана система, що переводить різнорідні дані в відтворювані управлінські рішення.

Сукупно ці підходи формують багатовимірну оптику: ІАЗ ЕБ – це і процес, і система, і набір компетенцій, і інституційний режим. Порівняння трактувань поняття «» представлено у таблиці В.2 Додатку В.

За результатами проведеного дослідження, було систематизовано основні підходи до означення ІАЗ ЕБ та згруповано у таблиці 1.2).

Таблиця 1.2

Порівняльна таблиця теоретичних підходів до ІАЗ ЕБ

Підхід	Фокус визначення	Типові індикатори/артефакти	Сильні сторони	Обмеження
Функціональний	Перелік функцій ІАЗ (моніторинг, діагностика, прогноз, превенція)	KRI/EWI-набори, карти порогів, регламенти ескалації	Операційна чіткість, вимірюваність	Ризик редукціонізму (менше уваги до інституцій/культури)
Системний	ІАЗ як взаємодія підсистем «дані–процеси–люди–технології»	Карти процесів, RACI, SLA аналітичних сервісів	Цілісність, управління змінами	Вищі вимоги до координації
Ризик-орієнтований (ISO/COSO)	ІАЗ як інформаційна «оболонка» ERM	Реєстр ризиків, матриці ризику, звіти ERM	Зв’язок із стратегією, комплаєнс	Може зводитись до звітності без аналітики
Інституційний	Регламенти, політики, культура даних	Політики доступу, аудит-треки	Стійкість процесів, відповідальність	Повільність змін, «паперова» відповідність
Стейкхолдерський	Орієнтація на різні групи користувачів	Панелі для власників/менеджменту/HR/регулятора	Придатність до прийняття рішень	Підвищена складність комунікації
Ресурсно-компетентнісний	Дані й моделі як актив	Каталог моделей/даних, репозиторії	Конкурентна перевага	Ризик «lock-in» і залежності від кадрів
Цифрово-соціотехнічний	Пояснюваність, етика, Lakehouse/BI/ML	Каталог даних, лінійка даних, XAI-артефакти	Масштабованість, трасованість	Високі вимоги до зрілості даних

Джерело: систематизовано автором на основі [145-224]

Порівняльний аналіз засвідчує, що провідні підходи до інформаційно-аналітичного забезпечення економічної безпеки підприємства (ІАЗ ЕБ) є взаємодоповнювальними. Функціональний підхід забезпечує операційну визначеність вимірювань і реакцій; системний інтегрує «дані - процеси - людей - технології»; ризик-орієнтований (ISO/COSO) вмонтовує ІАЗ у стратегічний цикл ERM і комплаєнс; інституційний закріплює сталість правил і підзвітність; стейкхолдерський гарантує релевантність аналітики для різних груп; ресурсно-компетентнісний трактує дані та моделі як актив; цифрово-соціотехнічний додає масштабованість, трасованість і пояснюваність (XAI). У сукупності ці ракурси взаємно нівелюють типові обмеження (редукціонізм, «паперова відповідність») і формують спільне поле керованої практики.

У такій оптиці ІАЗ ЕБ доцільно тлумачити як інтегровану рамку, у якій «стан» безпеки визначає ціль, а «спроможність» – механізм її досягнення та підтримання.

Практична реалізація потребує багатошарової архітектури, що охоплює:

1) управління даними (якість, доступи, походження/лінійність, аудит);

2) платформу даних як «єдине джерело істини» для внутрішніх і зовнішніх потоків, зокрема OT/IoT та HR;

3) аналітичне ядро з EWI/KRI, порогами та сценаріями реагування, а також XAI для чутливих рішень;

4) механізми прийняття рішень – дашборди, журнали дій, SLA аналітичних сервісів, формалізовані правила ескалації;

5) компоненти резилієнсу й безперервності бізнесу (RTO/RPO, тренування сценаріїв, постінцидентне навчання).

Така конфігурація інтегрує сильні сторони окреслених підходів і мінімізує їхні обмеження.

Переходу від декларацій до керованої практики сприяє мінімальний тест зрілості ІАЗ ЕБ: наявність актуального реєстру ризиків і карти даних; валідованих EWI/KRI з визначеними власниками та порогами; дієвих правил ескалації; прозорих журналів перетворень і рішень; політик безперервності з перевіреними метриками відгуку/відновлення; етико-правових протоколів обробки персональних і комерційних даних. Критично, щоб усі ці елементи були безпосередньо пов'язані з фінансово-операційними результатами (P&L/CF, продуктивність, якість, простої), інакше ІАЗ редукується до формальної звітності.

Звідси випливають пріоритети розвитку: формування бібліотеки доменних EWI/KRI (зокрема для людського фактора та лояльності персоналу); стандартизація процедур пояснюваної аналітики та моніторингу «дрейфу» даних/моделей; інституціоналізація моделей зрілості ІАЗ як інструменту безперервного удосконалення. У підсумку економічна безпека постає не як статичний «щит», а як керована організаційна здібність, заснована на якісних даних, пояснюваній аналітиці та дисциплінованих процесах, інтегрованих у стратегію, операційну діяльність і культуру підприємства.

Враховуючи результати дослідження, поняття «*інформаційно-аналітичне забезпечення економічної безпеки підприємства*» пропонується визначати як інституціоналізований соціотехнічний контур даних, процесів і ролей, що перетворює інформацію про загрози, вразливості та можливості на своєчасні, відтворювані й підзвітні управлінські дії у сфері економічної безпеки. Воно реалізується через перелічені вище складові та підтримує цикл «моніторинг - аналіз - рішення - дія - навчання», будучи інтегрованим із ERM/BCM/ISMS і фінансово-операційними контурами підприємства з метою стійкого досягнення стратегічних цілей і довгострокової цінності.

Структурні складники інформаційно-аналітичного забезпечення економічної безпеки підприємства (ІАЗ ЕБ) утворюють взаємопов'язану

систему, у якій кожний блок виконує специфічну функцію, а їх узгодженість визначає зрілість усього контуру. Інформаційний блок формує «сировину» для аналітики, акумулюючи внутрішні джерела (ERP, MES/SCADA, CRM, HRIS, бухгалтерський облік, казначейство, виробнича телеметрія, системи якості) та зовнішні потоки (ринкові дані, масиви від постачальників і клієнтів, галузеві індикатори, новинні й регуляторні стрічки, відкриті дані). Для забезпечення інтероперабельності й відтворюваності запроваджуються стандарти опису – словники, довідники, класифікатори, логічні моделі даних, каталоги полів та ієрархії сутностей (контрагент, договір, актив, виробнича ділянка, інцидент). Окреме місце посідає таксономія ризикових атрибутів (ймовірність, вплив, швидкість настання, виявлюваність, контрольованість) і кодові книги ознак для EWI/KRI. Якість і лінійність даних підтримуються через політики повноти, точності, своєчасності, узгодженості й унікальності, доповнені угодами про рівень якості (SLA) та механізмами data lineage, що фіксують походження й перетворення. Інтеграція реалізується як для пакетних, так і для потокових сценаріїв: ETL/ELT-конвеєри, CDC (change data capture), подієві шини, API-шари й профілювання даних, а довідникова узгодженість забезпечується MDM. У підсумку формується стандартизований, інвентаризований і оцінений за якістю масив, придатний до побудови індикаторів ризику та аналітичних моделей.

Аналітичний блок перетворює дані на знання та керовані дії, поєднуючи описову й діагностичну аналітику (статистичні панелі, контрольні карти, кореляційно-каузальні аналізи, бенчмарки), предиктивні підходи (регресійні й класифікаційні моделі, моделі часових рядів, виявлення аномалій, баєсівські мережі, прогнози відтоку персоналу та збоїв обладнання) і прескриптивні інструменти (оптимізація, сценарне моделювання «what-if», симуляції Монте-Карло, теорія рішень). У цьому контексті конструюються випереджальні індикатори та ключові показники

ризику (EWI/KRI), калібруються пороги, гістерезиси та частоти вимірювання, визначаються власники індикаторів і реакційні карти. Валідність та надійність забезпечуються перехресною перевіркою, бек-тестуванням, оцінюванням стабільності у часі, моніторингом дрейфу даних і моделей; пояснюваність реалізується через інструменти XAI (зокрема feature importance, SHAP/LIME) із контролем упереджень та помилок I/II роду. Результатом є відтворювана, пояснювана аналітика, здатна транслювати сигнали у конкретні управлінські дії.

Організаційний блок інституціоналізує підзвітність та узгоджені рішення. Він визначає ролі й відповідальності (risk owners, data owners/stewards, аналітики, архітектори, CISO/CRO, DPO), закріплює RACI-матриці та права прийняття рішень. Процеси структуруються відповідно до «петлі» моніторинг → аналіз → рішення → дія → навчання, із чіткими регламентами ескалації та журналами рішень; підтримуються програми розвитку компетентностей (risk/data literacy) і професійна сертифікація. Нагляд здійснюють профільні комітети з ризиків і безпеки, що проводять циклічні перегляди індикаторів, аудити даних і моделей та керують змінами. Такий порядок забезпечує узгодженість дій по всьому життєвому циклу даних та ризиків.

Технологічний блок надає інфраструктурну основу. Архітектурно поєднуються сховище даних (Data Warehouse) і lakehouse-підхід для структурованих і напівструктурованих потоків; застосовуються шари зберігання bronze–silver–gold, feature stores та CI/CD для аналітики. Інструментарій охоплює BI/DSS, вітрини даних, системи оркестрації конвеєрів, каталоги (data catalog), SIEM/SOAR, платформи лог-менеджменту та виявлення аномалій. Інтеграції зі стандартними корпоративними системами (ERP/MES/SCM/HRIS/QMS) поєднуються з подієвими шинами та потоковою обробкою для ранніх попереджень. Надійність і безпека забезпечуються схемами високої доступності та

відновлення (HA/DR), резервуванням, шифруванням і токенізацією, політикою мінімальних привілеїв, а також захистом приватності через псевдонімізацію та контроль доступу. Усе це створює масштабовану, відмовостійку й керовану платформу для безперервної аналітики.

Нормативно-регламентний блок гарантує правову та етичну стійкість. Він включає політики і правила доступу (RBAC/ABAC), класифікацію й утримання даних, стандартизовані шаблони реагування на інциденти, журнали аудиту, вимоги до шифрування та журналювання дій. Додатково забезпечується відповідність внутрішнім стандартам, галузевим регламентаціям і чинному праву, зокрема в частині обробки персональних і комерційних даних. Завдяки цьому процедури залишаються легітимними та відтворюваними.

За результатами проведеного дослідження, у таблиці 1.3 було узагальнено основні структурни складники ІАЗ ЕБ.

Узгоджена робота перелічених блоків переводить ІАЗ ЕБ від ситуації фрагментарної звітності до безперервної аналітичної «петлі» з адаптивними порогами ризику та документованими управлінськими діями. Саме ступінь цієї узгодженості є надійним індикатором зрілості системи та її здатності підтримувати економічну безпеку підприємства на вимірюваному й стійкому рівні.

В процесі дослідження було встановлено, що ІАЗ працює на мікро-, мезо- та макро-рівнях. Таблиця 1.4 систематизує управлінські рівні інформаційно-аналітичного забезпечення економічної безпеки (ІАЗ ЕБ), фокус кожного рівня та характерні механізми контролю. Такий поділ дозволяє узгоджувати локальні сигнали з консолідованими рішеннями.

Таблиця 1.3

Основні структурні складники ІАЗ ЕБ

Назва блоку	Характеристика	Функції
Інформаційний	Формує «сировину» для аналітики з внутрішніх (ERP, MES/SCADA, CRM, HRIS, фіноблік, телеметрія, QMS) та зовнішніх джерел (ринкові/галузеві індикатори, постачальники/клієнти, регуляторика, open data); включає метадані, словники/класифікатори, таксономію ризик-атрибутів; забезпечує якість і лінійність (SLA якості, data lineage); підтримує інтеграцію (ETL/ELT, CDC, подієві шини, API) та MDM.	Агрегація та нормалізація даних; управління якістю (повнота, точність, своєчасність, узгодженість, унікальність); ведення метаданих і таксономій; інтеграція потоків (batch/stream) і довідників (MDM); забезпечення трасованості (data lineage) як основи для EWI/KRI та моделей.
Аналітичний	Охоплює описову/діагностичну, предиктивну й прескриптивну аналітику; проєктує EWI/KRI (leading/lagging), пороги, частоти; забезпечує валідацію та пояснюваність (бек-тести, стабільність, контроль дрейфу; SHAP/LIME, feature importance).	Побудова та калібрування EWI/KRI; виявлення аномалій і прогнозування ризиків; сценарне моделювання та оптимізація реагувань; валідація/моніторинг моделей і даних; трансляція сигналів у керовані дії (reaction maps).
Організаційний	Інституціоналізує ролі та відповідальність (risk/data owners, stewards, аналітики, CISO/CRO, DPO); фіксує RACI та права рішень; регламентує «петлю» моніторинг → аналіз → рішення → дія → навчання; забезпечує нагляд (комітети, аудити, change management) і розвиток компетентностей.	Розподіл підзвітності за ризики/дані; встановлення й підтримка процесів та ескалацій; координація рішень і ведення журналів дій; навчання (risk/data literacy) і сертифікація; періодичні рев'ю індикаторів, аудит даних/моделей.
Технологічний	Інфраструктурна основа: поєднання DWH і Lakehouse; шари bronze–silver–gold, feature store, CI/CD для аналітики; інструменти BI/DSS, data catalogs, оркестрація конвеєрів, SIEM/SOAR, лог-менеджмент; інтеграції з ERP/MES/SCM/HRIS/QMS; вимоги до надійності та безпеки (HA/DR, шифрування, токенізація, мінімальні привілеї).	Зберігання та обробка структурованих/потокових даних; забезпечення безперервної аналітики та попереджень; каталогізація і оркестрація даних/моделей; підтримка доступності/відмовостійкості та кіберзахисту; технічна підтримка XAI і швидкого розгортання (CI/CD).
Нормативно-регламентний	Політики доступу й контролю (RBAC/ABAC), класифікація/утримання даних, шаблони інцидент-респонсу, журнали аудиту, вимоги до шифрування/журналювання; відповідність внутрішнім стандартам, галузевим вимогам і праву (персональні/комерційні дані).	Встановлення правил data governance і комплаєнсу; контроль доступів і приватності; забезпечення доказовості та відтворюваності процедур (аудит, логування); уніфікація регламентів реагування; періодична актуалізація політик.

Джерело: систематизовано автором на основі [201-224]

Таблиця 1.4

Рівні інформаційно-аналітичного забезпечення економічної безпеки підприємств

Рівень	Опис управлінського фокусу	Типові об'єкти/приклади	Ключові індикатори/механізми
Мікрорівень	Операційні процеси/ділянки та щоденний контроль відхилень	Виробництво, техобслуговування, закупівлі, персонал, якість, охорона праці	Локальні KRI, оперативні ескалації, зміни режимів, карти інцидентів
Мезорівень	Узгодження ризиків на рівні бізнес-одиниць і ланцюгів	Філії, БО, постачання/збут, міжпроцесні залежності	Консолідовані карти ризиків, сценарії міжпідроздільних залежностей
Макрорівень	Вплив зовнішнього середовища та регуляторики	Галузеві/регіональні ризики, макроіндикатори, нагляд	Агреговані стрес-сценарії, міжфірмові/кластерні залежності

Джерело: систематизовано автором на основі [201-224]

Рівневий підхід забезпечує вертикальну узгодженість ІАЗ ЕБ: мікро-сигнали агрегуються на мезорівні та віддзеркалюються у макро-сценаріях. Критичною умовою є узгоджені KPI і пороги між рівнями.

За результатами проведеного дослідження були систематизовані основні контури ІАЗ ЕБП. Таблиця 1.5 відображає чотири контури, через які ІАЗ ЕБ перетворює дані на керовані дії: від раннього виявлення сигналів – до формалізованого прийняття рішень.

Поєднання контурів забезпечує безперервний цикл «моніторинг – аналіз - рішення - дія - навчання» та скорочує часовий лаг між сигналом і управлінським втручанням.

Таблиця 1.6 конкретизує операційні функції ІАЗ ЕБ, через які реалізуються стандартизація даних, побудова індикаторів ризику, сценарний аналіз і підзвітність рішень.

Таблиця 1.5

Основні контури, через які ІАЗ ЕБ перетворює дані на керовані дії

Контур	Призначення	Джерела сигналів	Механізм реагування / вихід
Раннє попередження (Early Warning)	Виявлення відхилень до настання події	Телеметрія, ринок, соц./новинні стрічки, події	Автоматичні алерти за порогами/аномаліями, тригери ескалації
Сканування середовища (Environmental Scanning)	Систематичний моніторинг зовнішніх драйверів ризику	Ціни, логістика, регуляторика, геополітика	Періодичні огляди ризиків, оновлення сценаріїв і порогів
Внутрішня «розвідка» (Internal Intelligence)	Контроль дисципліни процесів і поведінкових ризиків	KPI-відхилення, події комплаєнсу, HR-індикатори	Коригувальні дії, план наглядових перевірок, матриці контролів
Контур рішень (Decision Loop)	Трансляція аналітики в управлінські дії та ресурси	Узагальнені індикатори, сценарні оцінки	Зміни бюджетів/лімітів/політик, SLA, пост-оцінка ефективності

Джерело: систематизовано автором на основі [201-224]

Таблиця 1.6

Операційні функції інформаційно-аналітичного забезпечення економічної безпеки підприємств

№	Функція	Зміст	Типові артефакти / метрики
1	Стандартизація показників і словників	Єдині дефініції ризиків, класифікатори, таксономії	Каталог показників, довідники, дата-паспорт
2	Консолідація даних і усунення дублювань	Інтеграція джерел, MDM, узгодження ідентифікаторів	Карта даних, MDM-реєстри, звіти узгодженості
3	Побудова EWI/KRI та калібрування	Визначення leading/lagging, порогів, частот	Карти індикаторів, таблиці порогів, журнали спрацювань
4	Пріоритизація загроз	Оцінка ймовірності/впливу, ранжування ризиків	Матриці ризику, bow-tie, heat-maps
5	Сценарне моделювання і стрес-тестування	«What-if», Монте-Карло, шоки ланцюгів постачання	Звіти сценаріїв, stress-loss, чутливісний аналіз
6	Оцінювання ефективності контролів	Ex-ante/ex-post, співвідношення витрат і вигод	CBA, ROI контролів, KPI залишкового ризику
7	Формування доказової бази	Підзвітність менеджменту/наглядовим органам	Дашборди, аудиторські треки, протоколи рішень
8	«Замикання циклу» (learning loop)	Інкорпорація уроків у моделі, пороги, регламенти	Оновлені політики, версії моделей, дорожні карти поліпшень

Джерело: систематизовано автором на основі [201-224]

Повноцінна реалізація функцій переводить ІАЗ ЕБ із площини звітності у площину керованої практики: індикатори стають дієвими тригерами, а рішення – відтворюваними й підзвітними.

Інформаційно-аналітичне забезпечення економічної безпеки підприємства (ІАЗ ЕБ) функціонує на основі принципів, що формують нормативно-методологічну рамку узгодження даних, моделей і управлінських рішень.

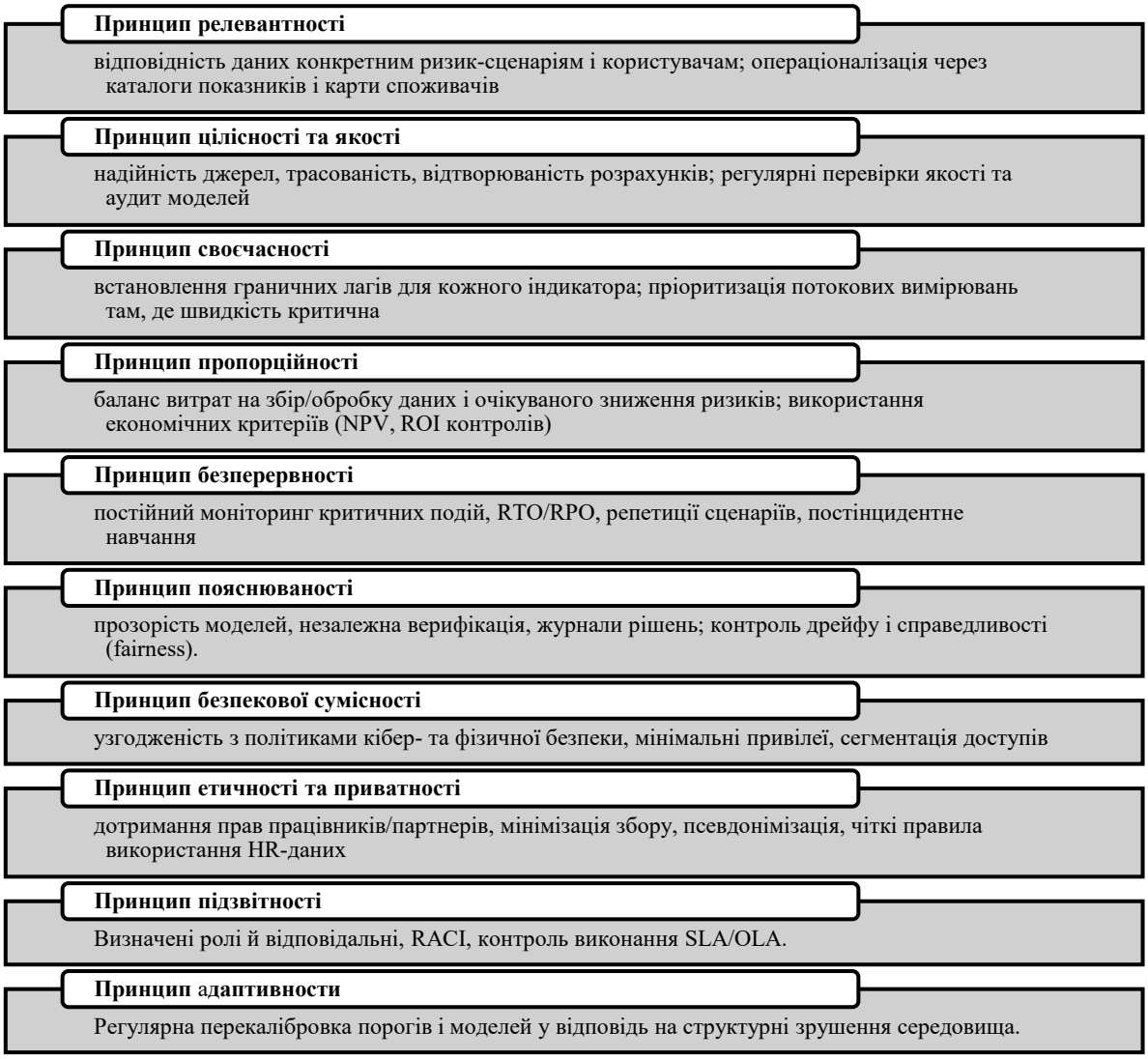

Рис. 1.1. Основні принципи інформаційно-аналітичного забезпечення економічної безпеки підприємства

Джерело: систематизовано автором на основі [201-224]

Практична імплікація полягає у формалізації цих засад у політиках управління даними, паспортах показників та регламентах ескалації з прив'язкою до фінансово-операційних результатів (P&L/CF, продуктивність, простої). Регулярна перекалібровка порогів, аудит моделей і перевірка готовності до інцидентів (RTO/RPO) завершують «петлю навчання», перетворюючи ІАЗ ЕБ на керовану, вимірювану та відтворювану складову системи економічної безпеки підприємства.

Операційно принципи втілюються через організаційні та технологічні механізми. На організаційному рівні функціонують профільні комітети з ризиків/безпеки, що затверджують паспорти показників, власників даних та порогові значення; впроваджуються цикли «моніторинг → аналіз → рішення → дія → навчання» з фіксацією підстав і наслідків втручань. На технологічному рівні застосовуються поєднання DWH і lakehouse-архітектур, каталоги даних і ознак (feature store), оркестрація конвеєрів, а для інцидентів – SIEM/SOAR і журнали подій, що підвищує відтворюваність ІАЗ і прискорює реакцію.

Перевірюваність дотримання принципів забезпечується системою індикаторів. Якість даних оцінюється через сукупний бал (data quality score) та частку записів із підтвердженим lineage; своєчасність – через середній лаг оновлення індикаторів і частку сигналів, що надійшли в межах SLA; результативність EWI/KRI – через точність/повноту спрацювань, частку хибнопозитивних/хибнонегативних сигналів та середній час до виявлення/реакції (MTTD/MTTR). Стабільність моделей фіксується показниками дрейфу (даних і моделей) та перехресною валідацією в часі; безперервність – результатами тестів RTO/RPO і частотою тренувань; підзвітність – відсутністю «сирітських» індикаторів і своєчасністю ведення журналів рішень. Етичність і приватність контролюються частотою інцидентів доступу, результатами аудитів, охопленням псевдонімізації та дотриманням правил ретенції.

Таким чином, застосування принципів ІАЗ ЕБ у їхній операціоналізованій формі забезпечує керовану, вимірювану та відтворювану практику економічної безпеки. Сукупність організаційних (ролі, підзвітність), технічних (архітектури, інструменти), нормативних (політики, комплаєнс) і аналітичних (EWI/KRI, XAI) компонентів створює умови для своєчасного виявлення й пріоритизації ризиків, коректного вибору контрзаходів і достовірної оцінки їхнього впливу на фінансово-операційні результати підприємства.

Отже, еволюція уявлень про економічну безпеку підприємства (ЕБП) рухається від охоронно-захисної оптики до ризик-орієнтованої та резилієнс-парадигми, інтегрованої з ERM/ISO 31000 та ISO 22301. ЕБП доцільно трактувати як бінарну категорію – досягнутий стан захищеності та спроможність підтримувати його в динаміці, що чітко розмежовує цілі й засоби. Взаємодоповнення провідних підходів (функціонального, системного, ризик-орієнтованого, інституційно-стейкхолдерського, ресурсно-компетентнісного, фінансово-безпекового, резилієнс/BC) мінімізує редукціонізм і «паперову відповідність», формуючи поле керованої практики. Ключовим інтегратором виступає інформаційно-аналітичне забезпечення ЕБ (ІАЗ ЕБ) як інституціоналізований соціотехнічний контур даних, процесів і ролей, що перетворює інформацію про загрози, вразливості та можливості на своєчасні дії. Його операціоналізація вимагає зрілого data governance, «єдиного джерела істини», системи EWI/KRI з порогами та сценаріями, пояснюваної аналітики (XAI), журналів рішень та інтеграції з ERM/BCM/ISMS, підтверджених мінімальним тестом зрілості. Вертикально-горизонтальна архітектура ІАЗ (мікро–мезо–макрорівні; контури від раннього попередження до ухвалення рішень) скорочує лаг між сигналом і втручанням та замикає цикл «моніторинг - аналіз - рішення - дія - навчання», закладаючи підґрунтя для подальшого аналізу ролі управління

персоналом як «першої лінії захисту» і сучасних підходів до оцінювання лояльності у ризик-панелях підприємства.

1.2. Роль та місце управління персоналом в системі економічної безпеки промислових підприємств

Управління персоналом (УП) є невід'ємною складовою системи економічної безпеки промислового підприємства, оскільки саме людський капітал одночасно виступає джерелом вартості (компетенції, організаційні знання, операційна надійність) і каналом ризиків (помилки, недобросовісна поведінка, інсайдерські загрози, порушення дисципліни безпеки). У межах інтегрованої рамки ризик-менеджменту (ERM) HR-функція виконує роль «першої лінії захисту», що забезпечує профілактику та раннє виявлення ризиків, а також формує організаційні умови для їх пом'якшення та ескалації.

У працях Л. В. Балабанової та О. В. Сардак (2011) управління персоналом (УП) трактується як специфічна функція менеджменту, що охоплює цілі, принципи та методи роботи з персоналом і вибудовується як система взаємопов'язаних підсистем (аналіз і планування, добір, оцінювання, навчання, використання кадрів). У О. В. Крушельницької та Д. П. Мельничука (2005) УП постає водночас як наукова дисципліна і практична технологія, що інтегрує політики, процедури та моделі кадрової роботи для досягнення організаційної результативності. Ф. І. Хміль (2006) акцентує на функціональній природі УП як управлінської діяльності, спрямованої на формування, розвиток і використання трудового потенціалу організації.

В. М. Данюк, А. М. Колот та ін. (2013) репрезентують УП як цілісну підсистему загального менеджменту, у межах якої регламенти, ролі та

процеси узгоджуються зі стратегією підприємства і його соціально-трудовою політикою. У працях В. Г. Никифоренка (2013) простежується перехід від класичних адміністративних підходів до процесної та модельованої організації кадрової роботи, що підсилює керованість і вимірність результатів. О. М. Шубалий та ін. (2018) подають УП як методологічно й процесно окреслену рамку: планування потреб у персоналі, формування та розвиток, рух і утримання, оцінювання, мотивація, організація умов праці – з фіксацією процедур і відповідальностей.

В аналітичній традиції С. У. Олійник (2013) розглядає УП як систему концептів, принципів і механізмів менеджменту «людського чинника», де ключовими є узгодженість політик і розвиток компетентностей. Дослідження Ю. Ю. Гурбика та О. С. Багунц (2018) репрезентують УП як складову загального менеджменту, виокремлюючи шість базових елементів (методологія, політика, залучення, оцінка, розміщення/мотивація, навчання). У М. Д. Виноградського (2009) домінує соціосистемний акцент із підвищеною увагою до суб'єктності персоналу й компетентнісної логіки управління. Нарешті, у працях колективу під керівництвом О. П. Дяківа (2018) УП визначається як організація кадрової роботи, спрямована на формування, розвиток, мотивацію, оцінювання та утримання персоналу із детальною процедурною регламентацією.

У західній літературі M. Armstrong (2014) визначає HRM як «стратегічний, інтегрований і узгоджений підхід до зайнятості, розвитку та добробуту людей в організаціях», акумулюючи функціональні модулі та архітектури HR. P. Boxall і J. Purcell (2003) фокусують увагу на управлінні трудовими відносинами у фірмі як на цілісному наборі практик, що формують продуктивну взаємодію сторін зайнятості. T.J. Watson (2010) підкреслює управлінське використання зусиль, знань, здібностей і відданої поведінки працівників у межах «обміну зайнятістю». G. Dessler (2005)

пропонує канонічну «процедурну» перспективу HRM як сукупності політик і практик щодо добору, навчання, винагород, оцінювання та трудових відносин.

Позиція R. L. Mathis та J. H. Jackson інтерпретує HRM як комплекс політик і процедур залучення, розвитку, оцінки й винагород, зорієнтований на результативність і відповідність законодавчим вимогам. J. Storey розрізняє «м'який» і «жорсткий» підходи, пов'язуючи HR із формуванням конкурентних переваг через залучення та компетентність. У стратегічній парадигмі P. M. Wright та G. C. McMahan (1992) формулюють зв'язок HR-практик зі стратегією організації в різних теоретичних перспективах (поведінковій, кібернетичній, агентській, ресурсно-орієнтованій тощо). Гарвардська модель (M. Beer, B. Spector, P. Lawrence, D. Q. Mills, R. E. Walton) розглядає HRM як поліцентричне поле політик і практик із балансом інтересів стейкхолдерів та коротко-/довгострокових наслідків. Нарешті, у працях N. Wilton (у співзвуччі з позиціями CIPD) HRM трактується як «парасольковий» термін управління трудовими відносинами, зі зсувом до бізнес-партнерства, вимірюваної цінності та аналітичної підтримки рішень.

Порівняння українського та зарубіжного корпусів дозволяє виокремити щонайменше сім взаємодоповнювальних підходів (Табл. 1.7).

Еволюція трактувань демонструє перехід від описово-процедурних визначень до стратегічно інтегрованої та дано-керованої парадигми HRM. У сучасному баченні «управління персоналом» – це інституціоналізована підсистема, що перетворює трудові відносини, компетентності й дані про людей на відтворювані управлінські рішення та вимірювану організаційну цінність, узгоджену зі стратегією, інституційними вимогами й показниками ефективності.

Таблиця 1.7

Узагальнювальна таблиця підходів до дефініювання «управління персоналом»

№	Підхід	Коротка характеристика	Ключові автори (APA, приклади)
1	Адміністративно-функціональний	УП як специфічна функція менеджменту з набором підсистем і процедур (планування, добір, оцінювання, навчання, мотивація).	Balabanova, L. V.; Sardak, O. V.; Khmil, F. I.; Dessler, G.
2	Системний / соціотехнічний	Інтеграція «дані – процеси – люди – технології»; УП як цілісна підсистема організації.	Shubalyi, O. M.; Oliinyk, S. U.; Armstrong, M.
3	Стратегічний (SHRM)	Узгодження УП зі стратегією; формування стійких конкурентних переваг через HR-практики.	Danyuk, V. M.; Kolot, A. M.; Wright, P. M.; McMahan, G. C.; Storey, J.; Boxall, P.; Purcell, J.
4	Компетентнісний / людський капітал	Акцент на вартості та розвитку компетентностей, перетворення людського капіталу на результативність.	Vynohradskyi, M. D.; Armstrong, M.
5	Стейкхолдерський / Employment Relations (ER)	Баланс інтересів сторін зайнятості; HR-політики як поліцентричне поле рішень.	Beer, M.; Spector, B.; Lawrence, P.; Mills, D. Q.; Walton, R. E.; Boxall, P.; Purcell, J.
6	Процесно-нормативний	Стандартизовані політики/процедури, комплаєнс, формалізація ролей і відповідальностей у HR-циклі.	(Узагальнення укр. навчально-методичних джерел); Dessler, G.
7	Аналітично-цифровий (data-driven)	HR-аналітика, KPI та дані як інфраструктура ухвалення рішень; вимірюваність внеску HR.	Dessler, G.; Armstrong, M.; Wilton, N.

Джерело: систематизовано автором на основі [1-44]

Управління персоналом (УП) задає цілі, політики й процеси роботи з людьми в організації (планування, добір, розвиток, оцінювання, винагороди, утримання), тоді як кадрова безпека є його спеціалізованою підсистемою, зосередженою на ідентифікації, попередженні та контролі ризиків, що виникають унаслідок дій або бездіяльності працівників і контрагентів. Іншими словами, УП формує архітектуру «людської» цінності, а кадрова безпека – архітектуру її захисту.

Результати вивчення наукових праць українських авторів дає підстави трактувати «кадрову безпеку» як інституціоналізований контур політик,

процесів і контрольних процедур, спрямованих на попередження та мінімізацію ризиків, що походять від персоналу, а також на підтримання надійності трудових відносин у межах системи економічної безпеки підприємства. В українському дослідницькому полі дефініції тяжіють до превентивно-процесної та системно-функціональної логіки. Так, В. І. Ткаченко (2018) визначає кадрову безпеку як процес запобігання негативним впливам на економічну безпеку через ризики й загрози, пов’язані з людським потенціалом і трудовими відносинами, роблячи акцент на превенції та зв’язку з ЕБП.

Г. В. Назарова (2012) інтерпретує її як підсистему економічної безпеки підприємства з окресленими загрозами, функціями та методами управління – від добору до контролю виконання. С. В. Кондратьєва (2015) підкреслює «комплекс дій», що зменшує вплив внутрішніх і зовнішніх чинників, забезпечуючи безпечну взаємодію працівників у кадрових процесах, а К. А. Шпакович (2014) структурує превентивний цикл «загроза – контроль – збереження». У дусі інтеграції з ЕБП Т. В. Ганущак (2014) наголошує на нормативних регламентах і профілактичних заходах у роботі з персоналом; методичні напрацювання авторського колективу КПІ систематизують сутність і складові кадрової безпеки та пропонують практичні рекомендації щодо її забезпечення.

У галузевому вимірі В. Г. Алькема та О. С. Кириченко (2016) конкретизують кадрову безпеку крізь призму логістичних процесів, підкреслюючи роль доступів, компетенцій і мотивації в операційній надійності, тоді як Н. Гавловська (2024) акцентує зростання значущості цього напряму в умовах війни й технологічних зрушень. Уточнюючи онтологію поняття, Р. І. Урдуханов (2023) обґрунтовує суб’єктно-об’єктну дуальність: персонал постає одночасно джерелом ризику та носієм контролю й захисту.

Закордонні джерела формують нормативно-методичну опору для практик кадрової безпеки. Так, NIST (2020) визначає personnel security як дисципліну оцінювання доброчесності, надійності та стабільності осіб для виконання довірених обов'язків (PS у SP 800-53), фіксуючи зв'язок між політиками, контрольними заходами та підтвердженням їх дієвості. Блок «personnel & people security» у NPSA/CPNI (UK, 2021–2022) інституціоналізує мінімізацію інсайдерського ризику через політики доступу, розвиток культури безпеки та протидію розвідувальним загрозам, що логічно кореспондує з організаційними настановами ProtectUK (2022). PSPF Австралії (2019–2025) деталізує вимоги до первинного скринінгу (vetting), надання кліренсів і безперервної оцінки благонадійності (continuous evaluation).

У площині інформаційної безпеки ISO/IEC 27001/27002 (2013/2022) кодифікують human resource security як набори контролів на етапах «до/під час/після найму» (розподіл ролей і відповідальностей, навчання, дисциплінарні процедури, припинення доступів). Ризик інсайдера докладно описують CISA (2021–2022) та посібники CERT (Collins, M., Cappelli, D., Moore, A., та ін., 2016), тоді як поведінкові та психосоціальні маркери (включно з неумисними інсайдерами) інтерпретуються у працях F. L. Greitzer та співавт. (2010–2019) і N. Khan та співавт. (2021), що підсилює важливість навчання, контексту та ранніх індикаторів ризику.

За результатами проведеного дослідження нами було систематизовано основні підходи до трактування поняття «кадрова безпека» (Табл. 1.8). Таблиця відображає логіку переходу від загальних визначень «управління персоналом» до спеціалізованого поля «кадрової безпеки», у якому HR-політики, процеси та дані трансформуються на керовану систему превенції та реагування.

Таблиця 1.8

Основні підходи до трактування поняття «кадрова безпека»

№	Підхід	Зміст / характеристика	Ключові інструменти та контролі	Інтеграція та метрики (EWI/KRI)
1	Ризик-превентивний	Структурує ідентифікацію загроз, оцінювання ризиків і добір контрзаходів з метою зменшення імовірності та наслідків інцидентів.	Реєстр загроз і ризиків, картування вразливостей, матриці «ймовірність×вплив», плани реагування, навчання.	Вбудування в ERM; KRI: частота інцидентів, частка резидуального ризику; EWI: тренди «near miss», зростання експозиції.
2	Системно-функціональний	Розглядає кадрову безпеку як підсистему ЕБП із чітко визначеними функціями, процесами та відповідальностями.	Політики, SOP, RACI-матриці, аудити відповідності, регламенти ескалації.	Узгодження з корпоративними політиками; KRI: виконання контрольних процедур, своєчасність ескалацій; EWI: збої процесів.
3	Життєвоцикловий (HR-security lifecycle)	Контролі «до/під час/після найму» для забезпечення безпеки на всіх етапах трудових відносин.	Background checks, onboarding/HSE/ІБ-тренінги, role-based access, SoD, періодичний перегляд доступів, offboarding/de-provisioning.	Інтеграція з ISMS/HRIS; KRI: частка несвоєчасних деактивацій, порушення SoD; EWI: прострочені тренінги, аномалії доступу.
4	Vetting/clearance та безперервна оцінка благонадійності	Забезпечує надійність і доброчесність персоналу через скринінг, кліренси та continuous evaluation.	Перевірки благонадійності, періодичне підтвердження кліренсів, моніторинг «червоних прапорців».	Узгодження з PSPF/NIST; KRI: прострочені перегляди, відсоток відмов; EWI: зміни ризик-профілю працівника.
5	Інсайдерський і культурний	Орієнтується на мінімізацію зловживання легітимним доступом та формування культури безпеки.	Insider-threat program, whistleblowing, захист викривачів, кампанії обізнаності, поведінкова аналітика.	Зв’язок із програмами security culture; KRI: інсайдерські інциденти; EWI: частота повідомлень, «near miss», сигнали поведінкового ризику.
6	Аналітично-цифровий (data-driven)	Ґрунтується на паспортованих EWI/KRI, журналізації рішень та інтеграції даних для своєчасних управлінських дій.	Дашборди, SIEM/SOAR, data lineage, моніторинг дрейфу даних/моделей, журнали рішень.	Інтеграція з ERM/ISMS/BCM; KRI: MTTD/MTTR, частка хибних спрацювань; EWI: падіння якості даних, дрейф моделей.
7	Суб’єкт-об’єктний	Балансує превенцію з підтримкою: персонал як джерело ризиків і водночас носій контролю та захисту.	Етичні кодекси, «just culture», канали підтримки, програми добробуту, лідерські практики.	Узгодження з HR-стратегією; KRI: дисциплінарні кейси, конфлікти інтересів; EWI: індекс залученості, абсентеїзм, ознаки вигорання.

Джерело: систематизовано автором на основі [125-224]

Для встановлення взаємозв'язку між поняттями «управління персоналом» та «кадрова безпека», було досліджено інтеграцію УП і кадрової безпеки за трьома комплементарними рівнями: нормативно-стратегічним, процесним (вздовж життєвого циклу працівника) та організаційним (ролі й підзвітність). Така стратифікація дає змогу, по-перше, закріпити правила й стандарти поведінки, по-друге, віддзеркалити HR-процеси в безпекових контролях, і, по-третє, забезпечити інституційний нагляд і відповідальність за виконання.

Таблиця 1.9

Рівні узгодження управління персоналом та кадрової безпеки

Рівень	Зміст (академічна характеристика)	Ключові механізми	Приклади контрольних дій/процедур
Нормативно-стратегічний	Узгодження кадрової політики, компетентнісних профілів і стандартів поведінки з режимами благонадійності, доступів та відповідальності; інтеграція з ERM/ISMS/BCM.	Політики та кодекси; матриці ролей/доступів; дисциплінарні регламенти; регламенти ескалації.	Screening і конфлікт інтересів; role-based access; сегрегація обов'язків (SoD); процедури дисциплінарного впливу.
Процесний (життєвий цикл працівника)	Дзеркальне відображення HR-процесів у безпекових контролях на етапах «до/під час/після найму».	Стандарти для добору, адаптації, розвитку/кар'єри, offboarding; SLA/OLA між HR та безпекою.	Добір: профілювання критичних посад, перевірки благонадійності; Адаптація: HSE/ІБ-тренінги, мінімальні привілеї; Розвиток: періодичний перегляд доступів, SoD; Завершення: своєчасна деактивація доступів, передача знань.
Організаційний	Інституціональний розподіл ролей і підзвітність між HR і безпекою.	Комітети з ризиків; RACI-матриці; регламенти взаємодії; нагляд (аудит/комплаєнс).	Визначення risk/data owners; періодичні огляди інцидентів; планові аудити дотримання політик.

Джерело: систематизовано автором на основі [125-224]

Узгодження на трьох рівнях – нормативно-стратегічному, процесному та організаційному – формує керовану рамку взаємодії HR і функції безпеки: від визначення змісту та цільового призначення («що» і «навіщо», політики), через способи реалізації («як», процеси та контролі), до

розподілу відповідальності й механізмів нагляду («хто відповідає», ролі та нагляд).

Таблиця 1.10 ілюструє, як вихідні показники HR (плинність, своєчасність навчання, графіки роботи, результати оцінювання) трансформуються у вхідні параметри контуру кадрової безпеки (EWI/KRI, порогові значення, правила ескалації) і, у зворотному напрямі, як безпекові сигнали (інциденти доступу, події типу *near miss*, результати аудитів) слугують підставою для калібрування політик добору, розвитку, мотивації та розподілу обов'язків. У підсумку забезпечується функціонування замкненого управлінського циклу «дані → рішення → дії → навчання».

Таблиця 1.10

Взаємозв'язок між інформаційними потоками в управлінні персоналом та кадровій безпеці

Напрям потоку	Дані/сигнали	Використання у контролях/рішеннях	Приклади EWI/KRI
З УП → у кадрову безпеку	Плинність у критичних ролях; відвідуваність тренінгів; понаднормові; абсентеїзм; результати оцінювання	Живлення ризик-панелей; налаштування порогів і ескалацій; таргетовані тренінги/ротації	EWI: індекс втоми; прострочені тренінги; дефіцит компетенцій. KRI:плинність у критичних ролях; незакриті зауваження аудиту.
З кадрової безпеки → в УП	Інциденти/аномалії доступу; «near miss»; висновки розслідувань; результати аудитів	Корекція добору, навчання, мотивації; перерозподіл обов'язків; оновлення профілів компетентностей	EWI: сигнали поведінкового ризику; зростання «near miss». KRI: частота інцидентів доступу; порушення SoD.

Джерело: систематизовано автором на основі [125-224]

Двоспрямований обмін даними між підсистемами управління персоналом і безпеки формує їхню взаємозалежність: перша забезпечує інформаційні «сенсори» людського фактора, тоді як друга повертає доказово обґрунтовані (evidence-based) корекції політик і практик. Наступною умовою ефективної інтеграції виступають культурно-поведінкові засади та метричне забезпечення підзвітності.

У таблиці 1.11 узагальнено відповідні культурні (лідерство, підвищення обізнаності, «just culture», механізми повідомлення про порушення) та метричні компоненти (паспорти показників, журнали рішень, SLA/OLA, аудит моделей і даних), які забезпечують відтворюваність, верифікованість і чітку прив'язку інтеграції HR і безпеки до бізнес-результатів.

Таблиця 1.11

Культурні та метричні компоненти в управлінні персоналом та кадровій безпеці

Блок	Інструменти та практики	Метрики підзвітності	Очікувані результати
Культура та поведінка	Лідерські наративи безпеки; програми обізнаності; whistleblowing і захист викривачів; тренування сценаріїв; «just culture»	Частота повідомлень; частка підтверджених кейсів; індекс залученості; показники вигорання/абсентеїзму	Зниження умисних і неумисних інсайдерських ризиків; підвищення дисципліни дотримання політик
Вимірюваність і підзвітність	Паспорти показників; журнали рішень; SLA/OLA для аналітичних сервісів; аудит моделей/даних	HR-KPI ↔ KRI/EWI мапа:плинність ↔ критичні ролі без наступника; своєчасність навчання ↔ прострочені тренінги; аномалії доступу; MTTD/MTTR	Відтворюваність і прозорість рішень; доведена ефективність контролів; прив'язка до бізнес-результатів (P&L/CF, простої, якість)

Джерело: систематизовано автором на основі [125-224]

Культурні механізми зменшують імовірність виникнення інцидентів, тоді як метричні забезпечують верифікованість результатів і підзвітність управлінських рішень. У поєднанні вони формують замкнутий контур практики: від узгоджених правил і процесів (табл. 1.9), через дані та аналітику (табл. 1.10), до стійкої організаційної культури та вимірюваної цінності (табл. 1.11).

Узагальнюючи, наведені таблиці репрезентують послідовний каркас «рівні узгодження → обмін даними → культура та вимірюваність». У межах цієї конфігурації управління персоналом і кадрова безпека функціонують як єдиний, керований даними та підзвітний контур, що знижує ризики,

зумовлені людським фактором, і підсилює економічну безпеку промислового підприємства.

Управління персоналом опосередковує економічну безпеку промислового підприємства через низку взаємопов'язаних каналів (Рис. 1.2), у межах яких кадрові політики, процедури та рішення трансформуються на вимірювані ефекти в продуктивності, витратах, безперервності операцій і регуляторній відповідності (Armstrong, 2014; Dessler, 2005). Узгодження цих каналів із бізнес-стратегією та контуром управління ризиками (ERM) підсилює їхню результативність і забезпечує підзвітність рішень, формуючи причинно-наслідкові зв'язки між HR-практиками та показниками економічної безпеки (COSO, 2017; Wright & McMahan, 1992).

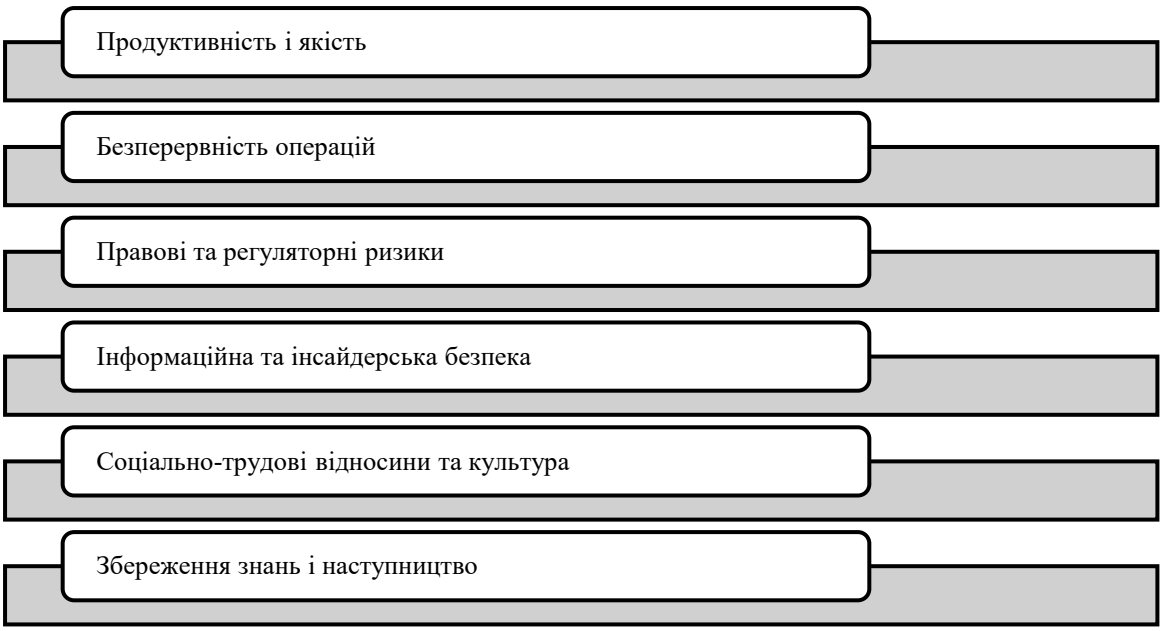

Рис. 1.2. Канали впливу управління персоналом на економічну безпеку промислового підприємства

Джерело: систематизовано автором на основі [125-224]

Перший канал пов'язаний із продуктивністю та якістю. Стан і динаміка компетенцій, дисципліна процесів та якість управління змінами

визначають втрати від браку, переробок, відхилень технологічних режимів і простоїв; на операційному рівні це відбивається у таких показниках, як загальна ефективність обладнання (OEE), частка браку (scrap rate), «перший прохід без дефектів» (first-pass yield) і «вартість низької якості» (cost of poor quality). Відповідні управлінські важелі – карти компетенцій для критичних операцій, стандарти навчання (SPC, lean), контроль версій технологічних карт і система допусків/сертифікацій (Balabanova & Sardak, 2011; Armstrong, 2014). У цій площині випереджальні індикатори (EWI) включають пропуски обов'язкових тренінгів, дрібні відхилення параметрів процесу й аномальне зростання понаднормових, тоді як ключові ризик-показники (KRI) – частку браку, години простою з кадрових причин і частку невідповідностей за підсумками внутрішніх аудитів (Hnylytska, 2012).

Другий канал стосується безперервності операцій. Плинність кадрів, дефіцит критичних навичок, абсентеїзм і дисбаланс графіків підвищують імовірність зупинок, порушення цільових часів відновлення/відновлення даних (RTO/RPO) і перенавантаження змін. Ефективними контрзаходами є планування потужностей робочої сили, матриці навичок, балансування змін, політики керування втомою та резервування персоналу для «вузьких місць» (Danyuk, Kolot, & Sukov, 2013; ISO 22301:2019). Відповідні EWI – «дірки» в графіках, сплески понаднормових у критичних змінах і падіння індексу покриття навичок; KRI – частка зупинок із кадрових причин, середній час закриття критичних вакансій (time-to-fill) та коефіцієнт абсентеїзму у вузлових підрозділах.

Третій канал охоплює правові та регуляторні ризики. Невиконання вимог охорони праці, промислової безпеки, трудового законодавства або колективних договорів породжує прямі санкції та непрямі втрати (репутаційні, часові, виробничі). HR-функція формалізує відповідність через обов'язкові навчання й допуски, медичні огляди, ведення персональних справ, облік робочого часу та процедурну справедливість

дисциплінарних практик (Khmil, 2006; ISO 45001:2018). Тут EWI – прострочені сертифікати/інструктажі й зростання «near miss» у підрозділах із дефіцитом навчання; KRI – кількість/сума штрафів і приписів, частка несвоєчасно закритих зауважень аудитів і відсоток працівників без чинних допусків.

Четвертий канал – інформаційна та інсайдерська безпека – виникає на перетині HR із OT/IT-середовищем і економічною безпекою. Від коректної реалізації процесів «прийшов-перемістився-звільнився» (joiner–mover–leaver), рольової моделі доступів (RBAC), сегрегації обов'язків (SoD) і своєчасної деактивації облікових записів залежить рівень інсайдерського ризику (ISO/IEC 27001:2022; NIST, 2020). Типові EWI – аномальні часові/географічні шаблони входів, затримки деактивації доступів і піки запитів на підвищення прав; KRI – кількість інсайдерських інцидентів, частота порушень SoD і частка запізнілих відключень доступів (CISA, 2021; Collins, Cappelli, & Moore, 2016).

П'ятий канал пов'язаний із соціально-трудовими відносинами та культурою. Ерозія довіри, токсичні практики, низька залученість і лояльність підвищують ризики страйків, саботажу, порушень правил HSE і «мовчазного опору» змінам. Через політики взаємодії, канали зворотного зв'язку, програми безпеки праці та «психологічної безпеки» HR формує культуру, що знижує імовірність як умисних, так і неумисних ризиків (Beer, Spector, Lawrence, Mills, & Walton, 1984; Ulrich & Brockbank, 2005). У цій площині EWI – падіння індексу залученості за пульс-опитуваннями, зростання частоти скарг/грієвенсів та ознак вигорання (комбінації понаднормових, абсентеїзму, просідання продуктивності); KRI – дні страйків/зупинок, частота порушень поведінкових кодексів і плинність у чутливих підрозділах (Pfeffer, 1998).

Нарешті, *шостий канал – збереження знань і наступництво*. Втрата носіїв критичних компетенцій (пенсії, міграція) знижує технологічну

надійність, ускладнює відновлення після інцидентів і створює «одиничні точки відмови». Практики картографування критичних знань, наставництво/shadowing, стандарти робочих інструкцій, ротації та формальні плани наступництва мінімізують ці ризики (Armstrong, 2014; Noe, Hollenbeck, Gerhart, & Wright, 2017). Відповідно, EWI – теплові карти ризику виходу ключових експертів, частка функцій із єдиним носієм знань і збільшення часу введення новачків у роль; KRI – частка критичних позицій із призначеними наступниками, середній час до набуття компетентності (mean time to competency) і показники ретенції знань після ротацій/звільнень.

Зазначені канали формують цілісну рамку, у межах якої HR-рішення конвертуються в керовані економічні ефекти через систему EWI/KRI, паспортовані процедури, журнали рішень та інтеграцію з ERM/BCM/ISMS (COSO, 2017; ISO, 2018; ISO 22301:2019; ISO/IEC 27001:2022). Практична реалізація цієї рамки потребує інституціоналізації ролей (risk/data owners), стандартизації даних і періодичної валідації метрик (DAMA International, 2017), формалізованих порогів і сценаріїв ескалації, а також прив’язки до фінансово-операційних результатів (P&L/CF, продуктивність, якість, простої) та вимірювання внеску HR у створення вартості (Becker & Huselid, 2001). За таких умов управління персоналом постає не допоміжною, а опорною функцією економічної безпеки, яка знижує імовірність і наслідки інцидентів та підвищує стійкість промислового підприємства.

У межах системи економічної безпеки промислового підприємства HR-функція виконує роль «першої лінії захисту», перетворюючи політики та процедури роботи з персоналом на відтворювані, підзвітні й вимірювані управлінські дії. Її інструментарій ґрунтується на ризик-орієнтованій логіці та життєвому циклі працівника (добір–розвиток–рух–вихід), інтегрований із контурами ERM/ISMS/BCM і підтриманий метричною базою EWI/KRI (COSO, 2017; ISO/IEC 27001:2022; ISO 22301:2019). У цьому контексті

добір і верифікація, керування компетенціями, управління графіками та втомою, система винагород, процедурна справедливість, етичні «speak-up» механізми, спільне з ІТ/ІБ управління доступами та планування наступництва формують цілісний соціотехнічний контур, що знижує імовірність і наслідки інцидентів і водночас підсилює продуктивність і відповідність (Armstrong, 2014; Noe, Hollenbeck, Gerhart, & Wright, 2017; NIST, 2020; Becker & Huselid, 2001; Beer, Spector, Lawrence, Mills, & Walton, 1984).

Кожен з цих механізмів розглядається з огляду на зміст, операційну реалізацію та індикатори контролю (Рис. 1.3). Їх призначення – перетворити політики й процедури HR на відтворювані та підзвітні управлінські дії з вимірюваним ефектом для ризик-профілю та результативності (COSO, 2017; Armstrong, 2014; Becker & Huselid, 2001). Нижче подано логічно взаємопов'язаний виклад ключових складників із фокусом на змісті, механізмах реалізації та індикаторах EWI/KRI.

По-перше, *добір і верифікація* забезпечують первинну фільтрацію ризиків, пов'язаних із благонадійністю, конфліктом інтересів та етичною сумісністю. Практично це передбачає профілювання критичних посад (risk-based job profiling), перевірки благонадійності й релевантні бекграунд-процедури, а також оцінювання відповідності кандидатів культурі безпеки (Armstrong, 2014; NIST, 2020). До випереджальних індикаторів (EWI) належать частка винятків із процедур скринінгу, затримки перевірок і відхилення від профілю ризику; ключові ризик-показники (KRI) – частота виявлених невідповідностей після найму та частка призупинених/скасованих допусків протягом випробувального терміну (NPSA, 2022).

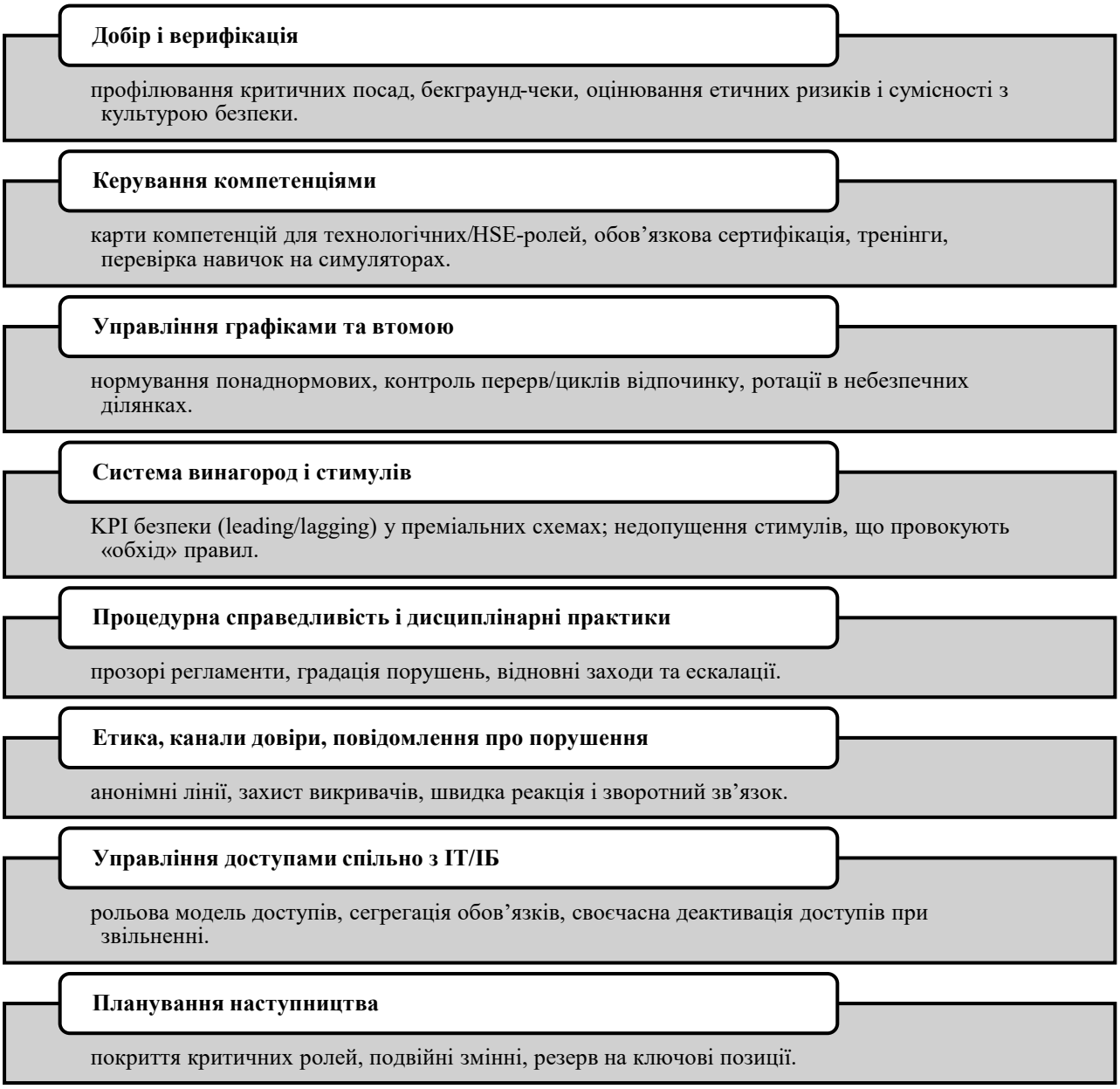

Рис. 1.3. HR-механізми як інструменти економічної безпеки промислового підприємства

Джерело: систематизовано автором на основі [125-224]

По-друге, *керування компетенціями* фокусується на формуванні, підтриманні та валідації знань і навичок для технологічних і HSE-ролей: карти компетенцій, обов'язкові сертифікації, планові та позапланові тренінги, перевірка навичок на полігонах і симуляторах (Noe, Hollenbeck, Gerhart, & Wright, 2017; ISO 45001:2018). Інформаційно-аналітичний вимір

включає паспорти показників навчання, контроль своєчасності сертифікацій та стабільність результатів перевірок. Типові EWI – прострочені навчальні модулі та «просідання» результатів тестування; KRI – питома вага інцидентів із ознаками дефіциту компетенцій і частка операційних відхилень, корельованих із людськими помилками (Hnylytska, 2012).

По-третє, *управління графіками та втомою* мінімізує ймовірність помилок і порушень режимів через перевтому: нормування понаднормових, контроль перерв і циклів відпочинку, ротації на небезпечних ділянках, балансування змін і покриття «вузьких місць» (ISO 45001:2018; Armstrong, 2014). Дані з табелювання, контролю доступу та OT-телеметрії дозволяють формувати індекси втоми як EWI; до KRI належать години простою з кадрових причин і частка дефектів, пов'язаних із порушенням графіків.

По-четверте, *система винагород і стимулів* закріплює безпекову поведінку через вбудовані показники у преміальні схеми: поєднання «leading» (EWI-типу) та «lagging» метрик, уникнення стимулів, що заохочують «обхід» правил, і узгодження з бізнес-цілями (Becker & Huselid, 2001; Pfeffer, 1998). Методично це оформлюється через HR-scorecard із причинно-наслідковою мапою «процес → поведінка → результат». Невідповідно сконструйовані KPI є самостійним джерелом ризику; EWI – ознаки «gaming the metrics», KRI – зростання інцидентів на тлі «поліпшення» формальних показників.

По-п'яте, *процедурна справедливість і дисциплінарні практики* забезпечують передбачуваність і легітимність реагування: прозорі регламенти, градація порушень, відновні заходи та формалізовані ескалації (Beer, Spector, Lawrence, Mills, & Walton, 1984; Colquitt, 2001). Емпірично справедливі процедури знижують девіантну поведінку і підвищують довіру до контролів. EWI – зростання частоти скарг і спорів; KRI – повторюваність порушень та частка оскаржених дисциплінарних рішень.

По-шосте, етика, *канали довіри та повідомлення про порушення* («speak-up») формують культурно-поведінковий бар'єр проти інсайдерських загроз: анонімні канали, захист викривачів, швидкий і прозорий зворотний зв'язок, навчальні кампанії (ISO 37002:2021; NPSA, 2022; CISA, 2021). Стійка «just culture» підвищує імовірність раннього сповіщення. До EWI належать зміни тону/обсягу повідомлень і «near miss»; до KRI – підтверджені інциденти з людським фактором і час реагування на звернення.

По-сьоме, *управління доступами спільно з ІТ/ІБ* інституціалізує принцип «мінімальних привілеїв» у процесах joiner–mover–leaver: рольова модель доступів (RBAC), сегрегація обов'язків (SoD), своєчасна деактивація при звільненні, журналізація змін прав (ISO/IEC 27001:2022; NIST, 2020). Аналітично це підтримується SIEM/SOAR та кореляцією подій доступу з HR-подіями. EWI – аномальні входи й відхилення у шаблонах доступу; KRI – кількість порушень SoD і частка запізнілих відключень облікових записів (Collins, Cappelli, & Moore, 2016).

По-восьме, *планування наступництва* знижує ризики «одиничних точок відмови» у знаннях і навичках: покриття критичних ролей, «подвійні зміни», резерв на ключові позиції, наставництво і формалізація передачі знань (Rothwell, 2010; Noe et al., 2017). До EWI належать теплові карти ризику втрати експертизи та зростання time-to-competency для нових працівників; до KRI – частка критичних позицій із призначеними наступниками і втрати продуктивності під час ротацій.

Крос-січно всі механізми спираються на дано-керовану інфраструктуру: паспорти показників (визначення, формули, власники, частота, пороги і сценарії дій), журнали рішень, аудит даних і моделей, а також узгодження з ERM/ISMS/BCM (DAMA International, 2017; ISO/IEC 27001:2022; ISO 22301:2019; COSO, 2017). Саме така конфігурація забезпечує вимірюваність (EWI/KRI), відтворюваність і підзвітність HR-

контролів, зменшуючи імовірність і наслідки інцидентів і водночас підсилюючи фінансово-операційні результати промислового підприємства (Becker & Huselid, 2001; Armstrong, 2014).

Інформаційно-аналітичний контур HR у системі економічної безпеки доцільно трактувати як стандартизовану соціотехнічну інфраструктуру, що інтегрує джерела даних про персонал, виробництво та безпеку й перетворює їх на своєчасні, пояснювані та підзвітні управлінські дії. Ядром цієї інфраструктури є «єдине джерело істини», сформоване шляхом консолідації HRIS/кадрового обліку, LMS (навчання), HSE-журналів, систем контролю доступу, табелів і пейролу, опитувань залученості/культури, а також OT/IT-телеметрії для кореляції поведінкових, виробничих і безпекових подій. Якість, цілісність і трасованість потоків забезпечуються політиками управління даними (визначення власників, контроль якості, управління метаданими, фіксація походження та аудит), які доцільно будувати відповідно до DAMA-DMBOK та вимог ISMS (DAMA International, 2017; ISO/IEC 27001:2022). Такий підхід створює методологічну основу для побудови, валідації та експлуатації ризик-індикаторів у HR-домені (Armstrong, 2014; Becker & Huselid, 2001).

Метричний дизайн спирається на зв’язку випереджальних індикаторів (EWI) і ключових ризик-показників (KRI). Перші сигналізують про зростання імовірності інцидентів і застосовуються для раннього втручання (наприклад, частка понаднормових у критичних змінах, пропуски або несвоєчасність обов’язкових тренінгів, частота «near miss», аномалії доступу – нічні входи чи відвідування нетипових зон, індекси втоми, отримані на перетині табелювання, змінності та перерв), тоді як другі фіксують рівень експозиції або фактичні наслідки (плинність у критичних ролях, абсентеїзм, коефіцієнт заповнення вакансій у «вузьких місцях», частота HSE-інцидентів на 200 тис. людино-годин, частка незакритих

зауважень аудиту, частка ролей без наступника) і використовуються для керування резидуальним ризиком (ISO 45001:2018; Hnylytska, 2012). Кожний індикатор має бути «паспортований»: наведено точне визначення та формулу розрахунку, указано джерела й власника даних, періодичність оновлення, пороги спрацювання (зокрема «жовті/червоні» зони) і заздалегідь визначені дії у разі перевищення (playbooks, ескалації). Одночасно необхідно дотримуватися етико-правових протоколів – принципів приватності, мінімізації та пропорційності обробки, доступів за ролями – узгоджених із ISO/IEC 27701:2019 і корпоративними політиками конфіденційності, а також вимог пояснюваності моделей (XAI) для будь-яких алгоритмічно підтриманих HR-рішень (від відбору до доступів і внутрішніх розслідувань), аби уникати «чорних скриньок» і забезпечувати недискримінаційне обґрунтування дій (NIST, 2020; ISO/IEC 27001:2022). Операційна експлуатація контуру передбачає дашборди, журнали рішень, моніторинг дрейфу даних/моделей та SLA/OLA для аналітичних сервісів (періодичність оновлення, цільовий час реакції на сигнали, правила позачергових переглядів) (COSO, 2017; DAMA International, 2017).

Щоб індикатори стабільно трансформувалися на своєчасні дії, HR має бути організаційно вбудований у контур безпеки. Директор з персоналу (CHRO) виступає співвласником людських ризиків поряд із виробництвом, інформаційною/економічною безпекою та фінансами; координація із директором з ризиків/службою економічної безпеки здійснюється через комітети з ризиків і регулярні огляди профілю HR-ризиків (Beer, Spector, Lawrence, Mills, & Walton, 1984; COSO, 2017). Для ключових процесів – добір і верифікація, навчання та сертифікації, управління доступами за логікою joiner–mover–leaver, розслідування інцидентів, offboarding/деактивація – встановлюються RACI-матриці, які однозначно визначають відповідальних (Responsible), погоджувачів (Accountable), консультантів (Consulted) і поінформованих (Informed); для аналітичних

сервісів фіксуються SLA/OLA (доступність звітів, частота оновлення, цільові пороги MTTD/MTTR за сигналами EWI/KRI).

Для промислових підприємств критичною є тристороння зв'язка HR–HSE–OT/SCADA, що дозволяє поєднувати поведінкові сигнали (залученість, втома, дисципліна навчання) з технологічними відхиленнями (нестабільність параметрів процесу, «near miss») та подіями доступу (RBAC/SoD), формуючи причинно-наслідкові карти й сценарії реагування. Такий підхід відповідає життєвоцикловій логіці контролів «до/під час/після найму», кодифікованій у ISO/IEC 27002 (людський фактор в інформаційній безпеці) та практиках personnel security (NIST SP 800-53, сімейство PS; NPSA/CPNI), із наголосом на screening/vetting, мінімальних привілеях, регулярному перегляді доступів, сегрегації обов'язків і своєчасній деактивації (NIST, 2020; NPSA, 2022; ISO/IEC 27002:2022).

Вимірюваність і підзвітність забезпечуються мапуванням HR-KPI на KRI/EWI кадрової безпеки (плинність у критичних ролях ↔ ризик втрати компетенцій; своєчасність навчання ↔ дефіцит допусків і HSE-ризики; рівень понаднормових ↔ індекс втоми; якість offboarding ↔ затримки деактивації облікових записів). Результати такого мапування інтегруються в процеси ERM – ідентифікацію, оцінювання, реагування та моніторинг – і BCM (планування безперервності/відновлюваності), що дає змогу обґрунтовано розподіляти ресурси безпеки та демонструвати вплив HR-контролів на виробничу й фінансову результативність (P&L/CF, простої, якість) (COSO, 2017; ISO 22301:2019; Becker & Huselid, 2001).

Отже, інформаційно-аналітичний контур HR постає як інституціоналізований механізм, який перетворює розрізнені кадрові та виробничі дані на керовані управлінські інтервенції з доведеною економічною віддачею. Його ефективність визначається не лише якістю метрик (EWI/KRI) й даних, а й організаційною архітектурою – розподілом ролей, дисципліною ескалацій, міжфункціональною координацією та

культурою безпеки – узгодженою з рамками ERM/ISMS/BCM (Armstrong, 2014; DAMA International, 2017; ISO/IEC 27001:2022; ISO 22301:2019). У такій конфігурації HR виходить за межі традиційної «кадрової» функції та виконує роль першої лінії захисту від ризиків людського чинника.

Проведений аналіз підтверджує, що управління персоналом (УП) є структурно й функціонально інтегрованою складовою системи економічної безпеки промислового підприємства. УП виконує роль «першої лінії захисту», поєднуючи превенцію, раннє виявлення та контроль ризиків людського чинника з вимірюваним впливом на операційну надійність, якість, безперервність і регуляторну відповідність. У межах ризик-орієнтованої парадигми (ERM) і комплементарних контурів ISMS/BCM воно перетворює кадрові політики та процедури на відтворювані, підзвітні управлінські дії, спираючись на стандартизоване управління даними й систему випереджальних індикаторів (EWI) і ключових ризик-показників (KRI).

Концептуальна «рамка узгодження» УП і безпеки вибудовується на трьох рівнях: (1) нормативно-стратегічному (політики, кодекси поведінки, матриці ролей/доступів і правила ескалації, узгоджені зі стратегією та вимогами ERM/ISMS/BCM); (2) процесному (дзеркальне накладання контролів на життєвий цикл працівника: добір–адаптація–розвиток–рух–вихід); (3) організаційному (розподіл відповідальності за моделлю RACI, регулярні огляди ризик-профілю, комітети з ризиків). Двоспрямований обмін даними між підсистемами УП і безпеки «замикає» цикл «дані → рішення → дії → навчання»: HR-показники живлять ризик-панелі та пороги реагування, а безпекові сигнали калібрують практики добору, розвитку, мотивації та розподілу обов’язків.

Емпірична придатність запропонованої рамки визначається дано-керованістю та культурою підзвітності. Мінімальний тест зрілості передбачає: актуальний реєстр ризиків і карту даних; паспортовані

EWI/KRI з власниками, порогами та сценаріями дій; прозорі журнали рішень і аудит даних/моделей; SLA/OLA для аналітичних сервісів; інтегрованість із OT/SCADA та HSE-даними; а також усталені механізми «speak-up» і «just culture». Ключовою умовою є пряма прив'язка до фінансово-операційних результатів (P&L/CF, простої, якість, продуктивність), що унеможливлює редукцію УП до формальної звітності та забезпечує верифіковану економічну віддачу.

Отже, у сучасному баченні УП виходить за межі традиційної «кадрової» функції й постає як інституціоналізований соціотехнічний механізм забезпечення економічної безпеки. Його цінність полягає у здатності системно знижувати імовірність і наслідки інцидентів людського походження та одночасно підсилювати стратегічну спроможність і стійкість промислового підприємства. Подальший розвиток має бути спрямований на стандартизацію доменних EWI/KRI (зокрема для критичних ролей і лояльності персоналу), удосконалення процедур пояснюваної аналітики (XAI) та інституціоналізацію моделей зрілості, що забезпечать безперервне поліпшення практик на стику УП і економічної безпеки.

1.3. Сучасні підходи до оцінювання лояльності персоналу в контексті економічної безпеки

Оцінювання персоналу в контексті економічної безпеки промислового підприємства постає не лише як інструмент HR-управління, а як елемент першої лінії захисту від ризиків, що генеруються людським чинником. У сучасних умовах технологічної складності та регуляторної турбулентності саме якість рішень щодо добору, розвитку, атестації та допусків до критичних операцій безпосередньо впливає на стабільність процесів,

витрати на брак і простої, дотримання вимог охорони праці й інформаційної безпеки. Відтак оцінювання має бути інтегрованим у контури ERM/BCM/ISMS, спиратися на валідні методики та породжувати керовані сигнали (EWI/KRI) для своєчасного управлінського втручання.

Попри значний масив напрацювань у сфері HRM, нинішні практики оцінювання часто залишаються фрагментарними, переважно процедурними та недостатньо «прив'язаними» до процесних і ризик-метрик. Поширеними є проблеми суб'єктивізму й низької психометричної якості інструментів, обмеженого зв'язку результатів оцінювання з операційними показниками (FPY, OEE, HSE-інциденти), а також слабка інтеграція з управлінням доступами та життєвим циклом працівника (joiner–mover–leaver). Додатковими викликами є вимоги пояснюваності моделей, приватності даних і етичної обґрунтованості рішень у чутливих HR-процесах.

За результатами проведеного дослідження було систематизовано сучасні підходи до оцінювання персоналу з позицій економічної безпеки (рис. 1.4), виявлено їхні сильні і слабкі сторони та обґрунтовано методологічні архітектури, здатні перетворювати результати оцінювання на вимірювані економічні й ризик-ефекти (Таблиця В.4 Додатку В).

1. Компетентнісний і результативний підхід до оцінювання персоналу в контексті економічної безпеки. Компетентнісний і результативний підхід (КіР) розміщує оцінювання персоналу на перетині моделювання компетентностей критичних ролей і перевірки їхнього впливу на процесні та ризик-метрики економічної безпеки (якість, стабільність режимів, дотримання регламентів). У стратегічному HRM це означає вимірювати те, що змінює продуктивність і ризик (Armstrong, 2014), операціоналізуючи компетентності через спостережувані поведінкові індикатори та зв'язуючи їх з результатами (Spencer & Spencer, 1993; Shippmann et al., 2000; Campion et al., 2011).

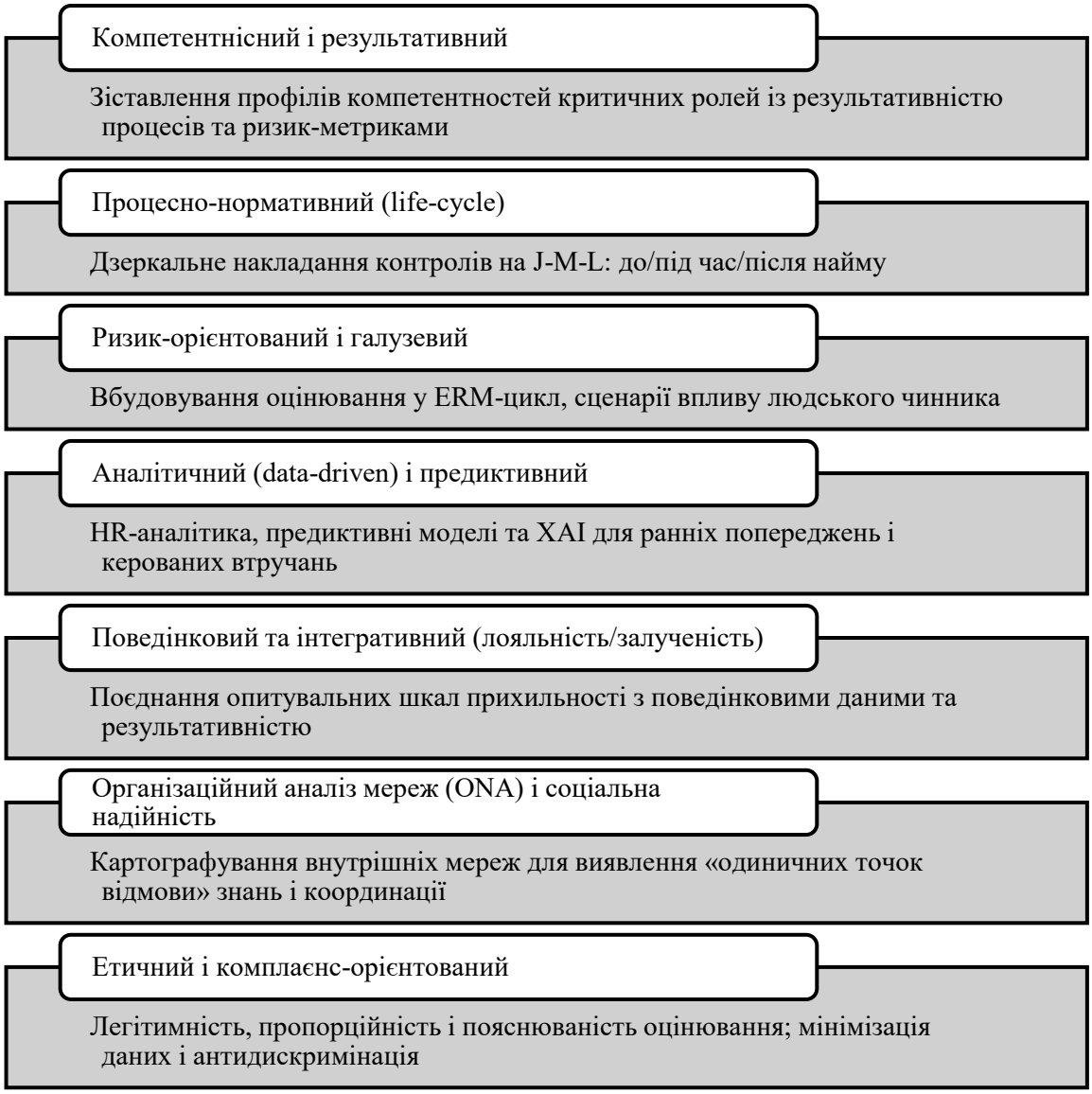

Рис. 1.4. Основні підходи до оцінювання персоналу в контексті економічної безпеки

Джерело: систематизовано автором на основі [125-224]

Причинно-наслідкова логіка HR Scorecard і BSC («HR-практики → поведінка → процеси → фінанси») природно доповнюється KRI/EWI (Becker & Huselid, 2001; Kaplan & Norton, 1996), а контроль варіації забезпечують SPC та Six Sigma у зв'язці з підходом до «організаційних бар'єрів» J. Reason (Harry & Schroeder, 2000; Montgomery, 2012; Reason, 1997). Українські джерела підкреслюють зв'язок компетентностей з браком, простоями і дисципліною виконання (Balabanova & Sardak, 2011; Hnylytska,

2012). Етичність, приватність і відтворюваність гарантують рамки data governance та privacy/XAI (DAMA International, 2017; ISO/IEC 27701:2019), а інтеграція з ERM/BCM/ISMS закріплює практичну керованість (ISO 45001:2018; ISO/IEC 27001:2022).

Методологічна архітектура підходу. Методологія компетентнісно-результативного підходу стисло зводиться до п’яти взаємопов’язаних кроків. По-перше, ідентифікуються критичні ролі та процеси з підвищеною ризик-експозицією через карти процесів і heat-maps відповідно до ISO 31000:2018 (OT/SCADA, енергетика, небезпечні дільниці, казначейство тощо).

По-друге, виконується системний job analysis із поєднанням DACUM, critical incident technique, gemba-спостережень та експертних інтерв’ю (Flanagan, 1954; Noe, Hollenbeck, Gerhart, & Wright, 2017), на основі якого конструюються компетентнісні профілі (core та role-specific) з багаторівневими поведінковими дескрипторами (Shippmann et al., 2000; Campion et al., 2011).

По-третє, кожна компетентність зв’язується з операційними проксі-метриками (наприклад, «керування режимами печі» ↔ варіативність температури, FPY, capability-індекси), а інструменти оцінювання добираються багатомодально: знаннєві тести із blueprint та аналізом дискримінативності, BARS і чек-листи спостережень для критичних операцій (Smith & Kendall, 1963), робочі проби/симуляції та assessment-center для складних ролей; 360° застосовується лише як допоміжний канал зі строгими протоколами мінімізації упередженості.

По-четверте, здійснюється психометрична перевірка: надійність (α-Кронбаха, ICC), валідність (контентна; конструктна – CFA; критерійна/прогнозна – кореляції з KPI/подіями), справедливість (DIF) та аудит упереджень (Nunnally & Bernstein, 1994; Lawshe, 1975).

По-п’яте, оцінки інтегруються з процесними показниками – контрольними картами SPC (X-bar/R, p-, c-), OEE, FPY, «вартістю низької якості» та індикаторами HSE/near-miss (ISO 45001:2018) – для проєктування паспортованих EWI/KRI (власник, формула, частота, пороги, сценарії дій). Причинно-наслідкові зв’язки верифікуються регресійними/логістичними моделями, HLM/SEM для ієрархії «працівник–зміна–дільниця», а також дизайнами interrupted time series і difference-in-differences; інтервенції (таргетоване навчання, супервізія, ротації, перегляд допусків, стандартизація інструкцій) оцінюються за ROI/CBA простоїв і браку (Becker & Huselid, 2001; Montgomery, 2012).

На підставі проведених досліджень були систематизовано основні методичні інструментарії компетентнісного і результативного підходів (1.12).

Таблиця 1.12

Основні методичні інструментарії компетентнісного і результативного підходів

Назва	Опис	Приклад
BARS (поведінково-якірні шкали)	П’яти–семибальні шкали з поведінковими дескрипторами для критичних операцій; підвищують об’єктивність спостережень і узгодженість оцінювачів.	BARS для «зарядження печі»: 5 рівнів із конкретними індикаторами дотримання температурного режиму; ICC між оцінювачами ≥ 0,75.
Структуровані спостереження	Стандартизовані чек-листи на робочому місці; фіксують виконання SOP, HSE та OT-процедур.	Чек-лист оператора преса: 20 пунктів із бінарною фіксацією, щозмінне вибіркове спостереження.
Робочі проби та симуляції	Практичні завдання/цифрові двійники для верифікації навичок у ризикових ролях (OT/SCADA).	Тренажер SCADA для аварійних сценаріїв: імітація відмов; фіксація часу реагування та помилок.
Assessment Center	Багатокомпонентна оцінка управлінських/координаційних компетентностей із кількома асесорами.	Центр оцінювання для майстрів змін: рольові ігри «аварійний простій», аналіз кейсу, групова дискусія.
360°-оцінювання	Багатоджерельний зворотний зв’язок про поведінкові індикатори; застосовується з обережністю через ризик упереджень.	360° для shift supervisor + кореляція з FPY/OEE; застосування валідованих шкал і анонімності.
Знаннєві/когнітивні тести	Перевірка знань регламентів, HSE та ІБ-процедур; потрібні еквівалентні форми й перевірена надійність.	Банки тестів з охорони праці: дві паралельні форми, α-Кронбаха ≥ 0,8.
Дизайн EWI (випереджальні індикатори)	Сигнали зростання імовірності інцидентів; прив’язка до джерел і порогів реагування.	«Індекс втоми» зі зшивки табелювання, доступів та OT-телеметрії; жовтий/червоний пороги.

Назва	Опис	Приклад
Дизайн KRI (ключові ризик-показники)	Метрики експозиції/наслідків ризику для контролю резидуального ризику.	Scrap rate, FPY, години простоїв з кадрових причин; поріг scrap > 2% = ескалація.
«Паспорти» індикаторів	Формалізація кожної метрики: формула, власник, частота, пороги, playbook дій.	Паспорт «прострочені сертифікації»: щотижневе оновлення, власник – HR/L&D, автоповідомлення керівнику зміни.
SPC та контрольні карти	Статистичний контроль процесів, відстеження стабільності виконання операцій.	X-bar/R-карти для температури печі; сигнал «3σ» → негайний перегляд допуску оператора.
ITS/DiD-дизайни	Квазіекспериментальні методи для оцінки ефектів інтервенцій «до/після» та «лікування/контроль».	Оцінка впливу переатестації операторів на зниження браку (DiD між двома дільницями).
HLM/SEM-моделювання	Багаторівневий/структурний аналіз зв'язків «компетентність → процес → результат».	Медіаційна модель: «BARS → стабільність режиму → FPY» із рівнями «працівник–зміна–дільниця».
Економічна оцінка (ROI/CBA)	Вимір віддачі контрзаходів: ROI, скорочення Cost of Poor Quality, уникнуті простої.	ROI від програми симуляцій = 3,2×; –28% простоїв, –35% браку за 6 міс.
Data governance (DAMA/MDM)	Каталоги даних, словники, управління якістю й лінійкою походження для довіри до аналітики.	Єдиний каталог показників HR/HSE/OT; MDM для ідентифікаторів працівника/ролі/дільниці.
Приватність та XAI	Пропорційність обробки даних, пояснюваність моделей, аудит упереджень.	DPIA для моделі ризику доступів; SHAP-графіки для пояснення рішень про допуски.
Типові помилки та пом'якшення	Переобтяжені профілі, «метрики без процесу», формалізм без психометрії.	Матриця «критичність×спостережуваність» (6–8 компетентностей/роль), тренування оцінювачів, журнали рішень.
Ілюстративний кейс (термічна дільниця)	Комплексна програма: job analysis → BARS/симуляції → EWI/KRI → інтервенції → перевірка ефектів.	–35% scrap, –28% простої, +0,4 Cp/Cpk за 6 місяців; ефекти підтверджені DiD.

Скорочення: SOP – стандартні операційні процедури; HSE – охорона праці та безпека; OT/SCADA – операційні технології/системи диспетчерського керування; FPY – first-pass yield; OEE – загальна ефективність обладнання; EWI – випереджальний індикатор; KRI – ключовий ризик-показник; MDM – master data management; DPIA – оцінка впливу на приватність; SHAP – пояснюваність вкладом ознак.
Джерело: систематизовано автором на основі [1-224]

У підсумку підхід забезпечує доказову трансляцію оцінювання у керовані економічні та ризик-наслідки, будучи вбудованим у контури ERM/BCM/ISMS і практики data governance та відповідаючи вимогам етики й приватності (Armstrong, 2014; ISO/IEC 27001:2022).

2. Процесно-нормативний підхід тлумачить взаємодію підприємства з працівником як керований життєвий цикл joiner–mover–leaver (J-M-L), у межах якого кожну фазу інституціоналізовано політиками, ролями, процедурами та метриками. Оцінювання персоналу тут вмонтовано у контури ERM/BCM/ISMS і спрямовано на зниження імовірності інцидентів

людського чинника та своєчасність управлінських реакцій. Теоретичний фундамент задають стандарти ISO/IEC 27001/27002 (людські контролі «до/під час/після найму» у логіці PDCA), рамки NIST SP 800-53/800-63 (vetting, clearance, continuous evaluation, керування електронною ідентичністю), емпіричні дослідження insider-risk (CERT/SEI) та практики people security NPSA/CPNI, що підкреслюють підвищені ризики на етапах переміщення і звільнення. Школа HRM/SHRM (Armstrong; Boxall & Purcell; Wright & McMahan) легітимізує процесну стандартизацію добору, розвитку, оцінювання й винагород у прив'язці до стратегії та результативності, тоді як підходи data governance і XAI (DAMA-DMBOK) забезпечують якість, трасованість і пояснюваність метрик, запобігаючи формальному «тикінню чек-боксів». У підсумку J-M-L-рамка з'єднує оцінювання з керованими діями: від скринінгу й навчання – до рольових доступів, своєчасної деактивації, журналів рішень і перевірюваних EWI/KRI, перетворюючи оцінювання на дієвий механізм економічної безпеки.

Методологічна архітектура підходу. Практична методологія life-cycle підходу починається з архітектури підзвітності (Табл. 1.13). На рівні управління встановлюються RACI-матриці, які однозначно визначають відповідальних і підзвітних за J-M-L-контролі: HR (скринінг, навчання, кадрові події), IT/ІБ (IAM, RBAC/ABAC, SIEM), лінійні керівники (схвалення доступів), функції ризиків і комплаєнсу (нагляд, аудити). Створюється комітет з людських ризиків, який на регулярній основі переглядає профіль HR-ризиків, показники KRI/EWI й уроки інцидентів. Політики screening/vetting, мінімальних привілеїв, сегрегації обов'язків (SoD), обов'язкових тренінгів HSE/ІБ і дисциплінарні процедури закріплюються в нормативних документах разом зі службовими угодами про рівень обслуговування (SLA/OLA), зокрема щодо часу деактивації доступів при звільненні.

Таблиця 1.13

Основні методичні інструментарії процесно-нормативного (life-cycle) підходу

Назва	Опис	Приклад
RACI та комітети	Закріплення відповідальності за J-M-L-контролі; регулярний нагляд за KRI/EWI та інцидентами.	Комітет з людських ризиків щокварталу переглядає профіль ризиків; RACI визначає HR як Responsible за скринінг, CISO – Accountable за IAM.
Політики та SLA/OLA	Формалізація screening/vetting, мінімальних привілеїв, SoD, навчань; часові зобов'язання.	SLA деактивації доступів ≤ 4 год із моменту offboarding; обов'язкові HSE/ІБ-курси для критичних ролей.
Журнали рішень та ескалацій	Протоколювання підстав доступів/змін і порогів ескалації.	«Червоний» прапорець, якщо деактивація > SLA; автоматичний тікет ескалації до ІБ.
Joiner (вхід)	Ризик-орієнтований скринінг, підтвердження кваліфікацій, стартові тренінги, надання мінімальних доступів.	Vetting для оператора SCADA; RBAC-роль «Оператор-Лінія-1» без фінансових прав.
Mover (переміщення)	Ресертифікація доступів, перевірка SoD, тимчасові привілеї з TTL, подієві access-review.	Під час переведення інженера – автоматична SoD-перевірка та 7-денний тимчасовий доступ до нової зони.
Leaver (вихід)	Повне de-provisioning, інвентаризація активів, блокування зовнішніх каналів, передача знань.	Автовідключення AD/VPN/SCADA за 2 год; чек-лист повернення бейджа/ноутбука; handover-нотатка.
RBAC/ABAC	Рольова й атрибутивна модель доступів із принципом мінімальних привілеїв.	Доступ до виробничої бази лише з цехових терміналів у робочі зміни (ABAC: локація/час/пристрій).
SoD-матриці	Заборонені комбінації обов'язків для зменшення шахрайських ризиків.	«Створити контрагента» ≠ «погодити оплату»; «внести рецепт» ≠ «затвердити зміну рецепта».
Періодичні access-review	Регулярні та позапланові огляди прав; ticket-треки змін.	Щомісячний рев'ю прав у фінансах; позаплановий рев'ю після масового переведення.
Data governance і паспорти метрик	Каталог джерел (HRIS/IAM/SIEM/LMS/OT), визначення показників, пороги, власники, частоти.	Паспорт KRI «Порушення SoD»: формула, дані SIEM+IAM, власник CISO, поріг = 0/місяць.
EWI (випереджальні індикатори)	Сигнали ймовірності інцидентів для раннього втручання.	Частка прострочених ІБ-тренінгів > 5%; «піки» понаднормових у критичних змінах; нічні входи поза графіком.
KRI (ключові ризик-показники)	Індикатори експозиції/наслідків ризиків.	Порушення SoD/міс.; частка запізнілих деактивацій; частота інсайдерських інцидентів/квартал.
SPC/контрольні карти	Статистичний контроль стабільності процесів доступів/навчань.	Контрольна карта часу деактивації: вихід точок за UCL – тригер на аналіз причин.
Предиктивна аналітика + XAI	Моделі ризику доступів/втоми з пояснюваністю і моніторингом дрейфу.	SHAP-аналіз показує, що комбінація «нічні зміни + понаднормові» підвищує ризик порушень на 30%.
Оцінювання ефектів інтервенцій	Квазіексперименти для перевірки впливу нових контролів.	DiD для впровадження SoD-матриці: −40% інцидентів проти контрольних підрозділів.
Ex-post CBA/ROI	Економічна верифікація результатів через уникнені втрати/вигоди.	ROI програми J-M-L = 3.2 завдяки зменшенню простоїв і штрафів.

Назва	Опис	Приклад
HSE/ІБ-тренінги та сценарні вправи	Рольово-адаптоване навчання, table-top/war-games, регулярні перевірки знань.	Щоквартальні вправи «інсайдер отримав зайві права» з планами ескалації.
Just culture & speak-up	Справедлива дисципліна, захист викривачів, етичні правила використання аналітики.	Анонімна лінія повідомлень; заборона карального застосування дашбордів продуктивності.
Приватність і пропорційність (DPIA/PIA)	Оцінка впливу на дані, мінімізація, псевдонімізація, політики ретенції.	DPIA для моделі «ризику втоми»; логування доступів до персональних даних; ретенція 12 міс.
Модель зрілості	Рівні розвитку від «паперових» політик до потоково-аналітичної інтеграції.	Рівень 1: чек-листи; Рівень 2: IAM+квартальні рев'ю; Рівень 3: HRIS–IAM–SIEM–OT інтеграція, XAI-моделі, playbooks.

Примітка: J-M-L – joiner–mover–leaver; RBAC/ABAC – рольова/атрибутивна модель доступів; SoD – сегрегація обов'язків; EWI/KRI – випереджальні індикатори/ключові ризик-показники; SPC – статистичний контроль процесів; SLA/OLA – угоди про рівень сервісу/взаємодії.
Джерело: систематизовано автором на основі [1-224]

Деталізація процесів J-M-L забезпечує операційну керованість. На фазі *joiner* критичними є risk-based vetting, верифікація кваліфікацій і culture-fit, обов'язкові тренінги HSE/ІБ та надання мінімально необхідних доступів у моделях RBAC/ABAC. На фазі *mover* відбувається повторна сертифікація прав, перевірка SoD на конфлікти обов'язків, надання тимчасових привілеїв із обмеженим часом дії та позапланові перегляди доступів у разі змін ролі. На фазі *leaver* процедура de-provisioning повинна забезпечувати повне та своєчасне відкликання доступів, інвентаризацію активів, блокування зовнішніх каналів і формалізовану передачу знань; затримки деактивації фіксуються як порушення SLA та підлягають ескалації.

Контроль доступів спирається на чітко визначені ролі (RBAC) та атрибутивні умови (ABAC) для чутливих операцій (географія, час, тип пристрою), а також на явні SoD-матриці із забороненими комбінаціями функцій. Періодичні огляди доступів (access reviews) – щомісячні й подієві – забезпечують своєчасне виявлення «зайвих» прав і «висячих» облікових записів. У частині даних застосовується повноцінне data governance: каталоги джерел (HRIS, IAM, SIEM, LMS, OT/SCADA), паспорти показників із визначеннями, формулами, власниками, періодичністю оновлення, порогами та сценаріями дій (playbooks). Випереджальні

індикатори (EWI) сигналізують про зростання імовірності інцидентів (прострочені тренінги, затримки деактивацій, «сплески» понаднормових у критичних змінах, аномальні входи, підвищення частоти «near-miss»), тоді як ключові ризик-показники (KRI) фіксують рівень експозиції або фактичні наслідки (порушення SoD, частка запізнілих de-provisioning, частота інсайдерських інцидентів, години простоїв з кадрових причин). Кожний індикатор має бути «паспортований», а механізми реагування – завчасно визначені й протестовані.

Аналітичний контур поєднує статистичний контроль процесів (SPC) для стабільності ключових показників (час деактивації, своєчасність тренінгів), предиктивні моделі ризику доступів і втоми персоналу із забезпеченням пояснюваності (SHAP/LIME) та моніторингу дрейфу даних і моделей. Ефективність інтервенцій оцінюється квазіекспериментальними підходами (interrupted time series, difference-in-differences) з подальшим економічним обґрунтуванням (ex-post CBA/ROI), що переводить судження про «корисність контролів» у площину доказовості. Навчання й культура безпеки підтримуються рольово адаптованими HSE/ІБ-програмами, сценарними тренуваннями (table-top/war-games), процедурами «just culture» і захисту викривачів, із чіткими гарантіями неприпустимості репресивного використання аналітики. Вимоги приватності та пропорційності реалізуються через DPIA/PIA, мінімізацію даних, псевдонімізацію та політики ретенції.

Життєздатність підходу вимірюється моделлю зрілості. На базовому рівні (рівень 1) переважають паперові політики й ручні чек-листи без SLA. Проміжний рівень (рівень 2) характеризується первинною автоматизацією IAM, каталогізацією метрик і квартальними оглядами доступів. Зрілий рівень (рівень 3) передбачає потокову інтеграцію HRIS–IAM–SIEM–OT, застосування XAI-моделей, сценарні playbooks, регулярні аудити та обов’язковий перерахунок економічного ефекту.

Отже, процесно-нормативний (life-cycle) підхід переводить оцінювання персоналу з площини разових атестацій у керовану інституційну практику, у якій кожна подія життєвого циклу працівника ініціює передбачені контролі, метрики та управлінські дії. Узгодження J-M-L-процедур з управлінням доступами (RBAC/ABAC, SoD), системою EWI/KRI та XAI-аналітикою, підкріплене SLA/OLA і журналами рішень, формує відтворюваний контур першої лінії захисту. У такій конфігурації оцінювання персоналу стає невід'ємною частиною економічної безпеки: воно знижує імовірність та наслідки інцидентів людського чинника, підсилює продуктивність і відповідність, а також забезпечує доказовий зв'язок між HR-інтервенціями та фінансово-операційними результатами підприємства.

3. Ризик-орієнтований і галузевий підхід до оцінювання персоналу в контексті економічної безпеки. Ризик-орієнтований і галузевий підхід трактує оцінювання персоналу як складову повного циклу ERM: від ідентифікації та аналізу ризиків людського чинника – до ранжування, реагування й безперервного моніторингу з явною ув'язкою з апетитом/толерантністю до ризику та критичними процесами (ISO, 2018; COSO, 2017). Теоретичну основу формують ISO 31000, ISO 22301 і ISO/IEC 27001/27002, доповнені парадигмою organizational resilience – «передбачати, моніторити, відповідати, навчатися» (Hollnagel, 2011/2017) – та мережевою логікою ризиків у ланцюгах постачання (Jüttner, 2005). На перетині з HRM/SHRM наголошується стратегічне узгодження кадрових політик зі стратегією фірми (Armstrong, 2014; Wright & McMahan, 1992), а в полі people security – скринінг, надійність і керованість доступів (NIST, 2020; ISO/IEC 27002, 2022). Українські студії конкретизують процесно-індикаторну рамку (Шинкар, 2020; Пушак та ін., 2021). Емпіричні роботи з insider risk підтверджують життєвоциклову природу інцидентів і потребу

інтегрувати поведінкові маркери з технічними журналами доступів (Collins, Cappelli, & Moore, 2016; NPSA/CPNI, 2022).

Застосування фокусується на ролях і процесах з високою експозицією: OT/SCADA, енергетичні диспетчери, «вузькі місця» виробництва, хімічно небезпечні дільниці, казначейство та платежі. Ціль – статистично підтверджуване зниження імовірності й тяжкості інцидентів через систематичну оцінку ризиків персоналу та таргетовані контрзаходи, узгоджені з ризик-апетитом підприємства.

*Методологічна архітектура підходу***.** Методологія впровадження розгортається низкою взаємопов'язаних етапів (Табл. 1.14).

Спершу окреслюють периметр (критичні процеси/ролі) та затверджують апетит/толерантність до ризику людського чинника на рівні ради/комітету (ISO, 2018; COSO, 2017). Далі проводять аудит даних і встановлюють data governance: інвентаризація джерел (HRIS, LMS, HSE, IAM, OT), призначення власників, уніфікація словників і метаданих за DAMA-DMBOK (DAMA International, 2017). Ідентифікацію ризиків здійснюють через HIRA/HAZOP/FMEA та мапування вразливостей уздовж joiner–mover–leaver (ISO/IEC 27002, 2022). Аналіз і пріоритизація базуються на bow-tie, «теплових» картах (ймовірність×вплив), швидкості настання/виявлюваності та сценаріях деградації (Jüttner, 2005; Шинкар, 2020).

Проєктують бібліотеку індикаторів із «паспортами»: EWI (динаміка near miss, індекси втоми, аномалії доступів, «розігрів» SPC) та KRI (TRIR, інциденти з людським фактором, порушення SoD, запізнілі деактивації, time-to-fill, час до компетентності, MTTR) (NIST, 2020; ISO 45001:2018; Пушак та ін., 2021). Паралельно виконують сценарне/стрес-тестування («what-if», Монте-Карло, RTO/RPO; ISO 22301:2019) і впроваджують контролі: RBAC/ABAC, SoD, SLA деактивації, керування втомою, рольові HSE/ІБ-тренінги, table-top/war-games (ISO/IEC 27001:2022; NPSA/CPNI,

2022). Аналітика поєднує SPC, предиктивні моделі з XAI та моніторинг дрейфу даних/моделей (Armstrong, 2014; NIST, 2020).

Таблиця 1.14

Основні етапи впровадження методології ризик-орієнтованого і галузевого підходу

Назва	Опис	Приклад
Етап 1 – Визначення периметра та апетиту до ризику	Виокремлення критичних процесів/ролей; встановлення risk appetite/tolerance для людського чинника на рівні ради/комітету.	Рада затверджує: допустимий TRIR із людським фактором ≤ 0.4/200 тис. людино-год; критичні ролі – оператори SCADA, диспетчери енергоцеху.
Етап 2 – Карта даних і governance	Аудит HRIS/LMS/HSE/IAM/OT-джерел; призначення data owners/stewards; уніфікація словників і метаданих.	Створено каталог даних: відвідуваність тренінгів, логи доступів, табелювання; призначено власників даних у HR та IT.
Етап 3 – Ідентифікація ризиків	HIRA/HAZOP/FMEA для техно-організаційних процесів; мапування критичності завдань; інвентаризація ризиків joiner–mover–leaver.	FMEA на дільниці змішування: найвищий RPN у помилках дозування; виявлено прогалини в перевірках при переміщенні персоналу.
Етап 4 – Аналіз і ранжування	Bow-tie, heat-maps (ймовірність×вплив), матриці швидкості настання/виявлюваності; визначення контрольних точок.	Heat-map показує піковий ризик у нічних змінах; контрольна точка – подвійна перевірка рецептур і підпис «других очей».
Етап 5 – Дизайн індикаторів	Проєктування EWI/KRI з «паспортами» (визначення, формула, джерела, власник, частота, пороги, дії).	EWI: індекс втоми > 0,7 тригерить ротацію; KRI: частка прострочених деактивацій доступів > 5% → позаплановий аудит IAM.
Етап 6 – Стрес-тестування та сценарії	What-if/Монте-Карло; перевірка RTO/RPO і кадрових «вузьких місць».	Моделювання відсутності 20% операторів: резервні графіки забезпечують RTO цеху ≤ 8 год.
Етап 7 – Впровадження контролів	RBAC/ABAC, матриці SoD; SLA деактивації; політики втоми; рольові HSE/ІБ-тренінги; table-top/war-games.	Казначейство: SoD для платежів; деактивація доступів при звільненні ≤ 4 год; щоквартальні вправи «war-game» з інсайдерського ризику.
Етап 8 – Аналітика та пояснюваність	SPC/контрольні карти; предиктивні моделі ризику з XAI; моніторинг дрейфу даних/моделей.	SHAP показує, що комбінація «нічні зміни + понаднормові» найбільше підвищує ризик інцидентів на пакувальній лінії.
Етап 9 – Управління та нагляд	Комітет людських ризиків; RACI; квартальні рев'ю карт ризиків; ув'язка контролів із бюджетами/BCM; журнали рішень.	Комітет перерозподіляє бюджет на додаткове тренування LOTO після зростання KRI у механічному цеху.
Етап 10 – Оцінювання ефектів і вдосконалення	DiD/ITS для перевірки причинності; ex-post CBA/ROI; оновлення порогів і playbooks; аудит даних/моделей.	DiD фіксує −30% інцидентів після введення політики втоми; ROI програми > 2; переглянуто «жовті/червоні» пороги EWI.

Джерело: систематизовано автором на основі [1-224]

Управління закріплюють через комітет людських ризиків, RACI-матриці, квартальні огляди карт ризиків, зв'язок контролів із

бюджетами/BCM і журнали рішень/ескалацій (COSO, 2017). Ефективність перевіряють квазіекспериментальними дизайнами (DiD, ITS) і ex-post CBA/ROI з періодичною перекалібровкою порогів та аудитами (Пушак та ін., 2021; DAMA, 2017). Галузева специфіка визначає джерела та пріоритети (енергетика/OT, хімія, гірничі роботи, логістика, фінанси). Запобіжники проти типових вад (агрегованість, ігнорування поведінкових драйверів, непрозорість, фрагментація даних) – «паспортовані» EWI/KRI з playbooks, «just culture», speak-up, XAI, DPIA/PIA та повний data lineage. Результат – доказовий, метризований контур першої лінії захисту, що знижує ймовірність/наслідки інцидентів і підсилює фінансово-операційну стійкість.

4.Аналітичний (data-driven) та предиктивний підхід. Аналітико-предиктивний підхід інтерпретує оцінювання персоналу як дано-керовану рамку, що поєднує управління даними, статистично-машинне моделювання, пояснювану аналітику та ризик-менеджмент, перетворюючи сигнали «людського чинника» на своєчасні й підзвітні дії. Теоретичний каркас спирається на ресурсо- та результатоорієнтовану логіку людського капіталу (Becker & Huselid, 2001; Becker, Huselid, & Ulrich, 2001; Boudreau & Ramstad, 2007), дисципліну people analytics з вимогами бізнес-релевантності, належного data governance і трансляції інсайтів у політики/процеси (Davenport, Harris, & Shapiro, 2010; Angrave et al., 2016; Marler & Boudreau, 2017; Levenson, 2018; Armstrong, 2014; Wilton, 2019), а також стандарти ERM/ISO щодо повного циклу ризик-менеджменту та контурів people/security (COSO, 2017; ISO, 2018; ISO/IEC, 2022; NIST, 2020). Парадигма organizational resilience («передбачати–моніторити–відповідати–навчатися») узгоджується з логікою EWI/KRI і «петлею навчання» (Hollnagel, 2011/2017). Українські напрацювання конкретизують індикаторно-процесну й обліково-аналітичну складові ІАЗ ЕБ (Шинкар, 2020; Пушак та ін., 2021; Гнилицька, 2012, 2013; Онищенко & Глушко,

2023; Єфіменко, 2024; Крамаренко, 2024; Дідик, 2020). Операціоналізацію забезпечують бібліотеки KRI/EWI з «паспортами», decision logs і MLOps-процедури (Deloitte; AuditBoard; MetricStream; Thomson Reuters). У підсумку підхід забезпечує доказову конверсію HR-сигналів у керовані втручання, зниження ризиків інсайдерства/помилок і вимірюваний вплив на P&L/CF та комплаєнс.

Методологічна архітектура підходу. Методологія аналітико-предиктивного підходу починається з бізнес-фреймінгу: визначення периметра (критичні процеси/ролі) та апетиту/толерантності до ризику людського чинника, із формалізацією таргетів моделей (інциденти, дефекти, простої, інсайдерські події, відтік) (COSO, 2017; ISO, 2018). Далі вибудовується контур data governance: інвентаризація джерел (HRIS, LMS, HSE, IAM/SIEM, OT-телеметрія, табелі/пейрол, опитування), уніфікація словників та ідентифікаторів, призначення власників даних, політики якості, lineage, RBAC/ABAC і аудит (DAMA International, 2017/2020; ISO/IEC, 2022). Формування датасетів включає коректний лейблінг у часових вікнах, інженерію ознак (графіки, сертифікації, поведінка, доступи, SPC-сигнали), контроль leakage та роботу з дисбалансом.

Моделювання охоплює GLM/логістичну регресію, ансамблі (GBM, RF), survival-аналіз для відтоку, виявлення аномалій (IForest, one-class SVM, автоенкодери), часові ряди (ARIMAX/Prophet) і каузальні дизайни (DiD, ITS, propensity) з оцінкою AUROC/PR-AUC і калібруванням (Davenport et al., 2010; Marler & Boudreau, 2017). Пояснюваність і справедливість забезпечують SHAP/LIME, model cards та DPIA/PIA з human-in-the-loop (Lundberg & Lee, 2017; Ribeiro et al., 2016; Molnar, 2019; NIST, 2020).

Скорами керують через «паспортовані» EWI/KRI (власник, формула, частота, пороги, playbooks): індекс втоми → ліміти змін/ротації; ризик доступів → блокування та перевірка SoD; ризик відтоку → індивідуальні плани утримання (ISO 22301:2019; COSO, 2017). Експлуатація спирається

на DWH/Lakehouse, MLOps (CI/CD, дрейф), журнали рішень, SLA/OLA та інтеграцію з ERM/BCM/ISMS; ефекти перевіряються DiD/ITS і CBA/ROI (AuditBoard, 2024; Deloitte, 2020–2024).

Таблиця 1.15

Основні етапи впровадження аналітичного (data-driven) та предиктивного підходу

Назва етапу	Опис (стисло)	Приклад застосування
Бізнес-фреймінг і ризик-апетит	Визначення критичних процесів/ролей; формулювання цілей і толерантностей до ризику; вибір таргетів (інцидент, дефект, простій, інсайдерська подія, відтік).	Для OT/SCADA-операторів встановлено нульову толерантність до LOTO-порушень; таргет – «інцидент безпеки = 1/0».
Управління даними (data governance)	Інвентаризація HRIS/LMS/HSE/IAM/OT-джерел; призначення data owners/stewards; уніфікація словників та ідентифікаторів; політики якості; lineage; RBAC/ABAC і аудит.	Консолідація HRIS, SCADA і SIEM у lakehouse; DQ-score ≥ 95%; запроваджено ролі доступу й журнали аудиту.
Формування датасетів і ознак	Лейблінг подій у часових вікнах; інженерія ознак (графіки, компетенції, поведінка, доступи, SPC); боротьба з дисбалансом; feature store.	Індекс втоми з табелювання й перерв; SMOTE для рідкісних інцидентів; ознаки JML з IAM.
Моделювання	Класифікація/скоринг (GLM, бустинг, RF), anomaly detection (IForest, one-class SVM), часові ряди (ARIMAX/Prophet), каузальні оцінки (DiD/ITS). Оцінювання AUROC/PR-AUC і калібрування.	XGBoost для ризику інцидентів; ARIMAX для дефектів; Cox-модель для відтоку критичних ролей.
Пояснюваність і справедливість (XAI & fairness)	SHAP/LIME, PDP/ICE; тестування упередженості; model cards/data sheets; DPIA/PIA; політика human-in-the-loop.	SHAP показує, що нічні зміни та прострочені тренінги – топ-фактори ризику; вилучено проксі-ознаки.
Пороги, тригери, playbooks	Перетворення скорів у EWI/KRI з паспортами (формула, джерела, власник, частота, жовті/червоні пороги, сценарії дій).	Індекс втоми > 0,70 → ротація та обмеження нічних змін; аномалія доступу → тимчасове блокування + розслідування SoD.
Впровадження та MLOps	CI/CD для моделей, версіонування артефактів, моніторинг дрейфу (PSI/KS), decision logs, інтеграція з ERM/BCM/ISMS, SLA/OLA на сигнали/реакції.	Автовідкат моделі при PSI > 0,2; журнал рішень у ServiceNow; SLA: ескалація «червоного» EWI – ≤2 години.
Моніторинг і ефективність	Технічний моніторинг (стабільність даних/моделей, MTTD/MTTR, хибні спрацювання) і бізнес-ефекти (DiD/ITS, CBA/ROI).	Після впровадження: −15% простоїв і −12% дефектів; ROI контролів = 2,4; MTTD скорочено з 3 днів до 6 годин.

Джерело: систематизовано автором на основі [1-224]

Така конфігурація перетворює аналітику на відтворювану «першу лінію захисту», що знижує імовірність і тяжкість інцидентів та підсилює фінансово-операційну стійкість.

5.Поведенковий та інтегративний підхід. Поведенковий та інтегративний підхід трактує лояльність як багатовимірну конструкцію й поєднує «м'які» психологічні стани з «твердими» операційними даними. В його ядрі – компонентні моделі організаційної прихильності (афективна, нормативна, інструментальна), де низька афективна складова пов'язана з відтоком, девіаціями та «мовчазним опором», а домінування інструментальної вказує на крихку транзакційну лояльність (Meyer & Allen, 1991). Друга опора – дослідження залученості, що стабільно корелює з продуктивністю, якістю та безпекою праці, отже її спад підвищує ризики помилок і порушень (Kahn, 1990; Harter, Schmidt, & Hayes, 2002; Christian, Garza, & Slaughter, 2011). Третій блок – модель «вимоги–ресурси роботи» (JD-R), яка пояснює переходи від перевтоми до HSE-інцидентів і збоїв режимів (Bakker & Demerouti, 2007; Maslach, Schaufeli, & Leiter, 2001). Четвертий – клімат/культура безпеки та «just culture», що підсилюють раннє повідомлення й покращують якість даних для ІАЗ ЕБ (Zohar, 1980; Neal & Griffin, 2006; Reason, 1997). Нарешті, people analytics у зв'язці з ERM/ISO задає вимоги до якості, трасованості й підзвітності рішень, забезпечуючи трансляцію інсайтів у керовані дії (Davenport, Harris, & Shapiro, 2010; COSO, 2017; ISO 31000:2018). Українські роботи конкретизують інтеграцію опитувальних і поведінкових даних та метрик прихильності у ризик-профіль (Mihus, 2013; Гнилицька, 2012, 2013; Yefimenko, 2024).

Методологічна архітектура підходу. Методологія поведенково-інтегративного підходу (Табл. 1.16) починається з визначення фокусів ризику (вигорання, ерозія «safety climate», девіантна/інсайдерська поведінка) та таргетів моделей (інциденти HSE/SoD, hazard відтоку, дефектність/простої). Далі вибудовується data governance: інвентаризація джерел (HRIS, LMS, HSE-журнали, IAM/SIEM, OT-телеметрія, табелі, опитування), уніфікація словників і метаданих, призначення власників даних, контроль доступів і аудит.

Таблиця 1.16

Методологія поведенково-інтегративного підходу: від постановки завдання до операційної експлуатації та вимірювання ефектів.

Назва	Опис	Приклад
Концептуалізація та фокус ризику	Визначення ключових людських ризиків і бізнес-наслідків.	«Втома у нічних змінах підвищує HSE-інциденти й простої».
Цільові змінні	Формалізація залежних змінних: бінарні, часові, безперервні.	Бінарна: факт порушення SoD; часова: hazard відтоку; безперервна: scrap rate.
Гіпотези	Перевірювані твердження про зв'язки між предикторами та ризиками.	↓ афективної прихильності + ↑ понаднормових → ↑ HSE-подій у «гарячих» цехах.
Опитувальні шкали	Вимірювання прихильності, залученості, клімату/культури безпеки.	UWES + шкала Meyer–Allen + блок Zohar для safety climate.
Поведінкові дані	Збір цифрових слідів із HRIS/LMS/HSE/IAM/OT-телеметрії.	Табелювання, «near miss», прострочені допуски, аномальні входи.
Психометрична валідність	Оцінка надійності/валідності опитувань; інваріантність між змінами.	α-Кронбаха ≥0,80; CFA; інваріантність metric/scalar для підрозділів.
Етика та приватність	PIA/DPIA, псевдонімізація, доступ за ролями, «just culture».	Відокремлення ідентифікаторів; канали «speak-up» без каральності.
Data governance	Каталог показників, словники, data lineage, SLA своєчасності.	Паспорт метрики «індекс втоми»: формула, джерела, власник, частота.
Вікна подій	Прив'язка ознак до періодів до/після події для причинності.	28-денне «вікно» до HSE-інциденту для фіч із графіків/навчань.
Інженерія ознак	Конструювання графікових, компетенційних, поведінкових, доступових і опитувальних фіч.	Частка 12-годинних змін; прострочені HSE-модулі; порушення SoD.
Класифікація/скоринг	Прогноз імовірності подій/кейсів; калібрування й метрики якості.	Логістична регресія + бустинг; AUROC/PR-AUC; Brier score.
Виявлення аномалій	Нестандартні патерни в доступах і поведінці.	Isolation Forest для нічних входів поза графіком у критичні зони.
Часові/каузальні моделі	Прогноз трендів і оцінка впливу інтервенцій.	ARIMAX для scrap rate; DiD для ефекту ротацій у нічних змінах.
Пояснюваність/ справедливість (XAI)	Інтерпретація внеску ознак, перевірка упередженості.	SHAP: «понаднормові» та «пропуски HSE» як топ-фактори ризику.
Паспорт EWI/KRI	Опис індикаторів, порогів і дій; власники та частота.	EWI: індекс втоми >0,70 (жовтий), >0,85 (червоний); KRI: інциденти на 100 FTE.
Playbooks реагування	Формалізовані сценарії дій на спрацювання індикаторів.	Втома: ротації, мікропаузи, лідерські «safety-talks», додаткове наставництво.
Аналітична інфраструктура	DWH/Lakehouse, feature store, CI/CD, SIEM/SOAR, каталоги.	Потокове оновлення панелей ризиків; журнал рішень (decision log).
Моніторинг дрейфу та SLA/OLA	Стабільність даних/моделей; норми часу «сигнал→реакція».	PSI/KS-тести щомісяця; MTTD≤24 год, MTTR≤72 год за SLA.
Оцінювання ефектів	Технічні та бізнес-метрики, CBA/ROI, пост-аудит.	−30% HSE-порушень і −12% дефектів за 2 міс.; ROI програми >2.
Human-in-the-loop і нагляд	Комітети з ризиків, RACI, ескалації, аудит моделей/даних.	CHRO/CRO-рев'ю KRI, квартальні ревізії порогів і playbooks.

Джерело: систематизовано автором на основі [1-224]

Опитувальний блок охоплює валідовані шкали прихильності/залученості та клімату безпеки; поведінковий – табелювання, «near miss», дисципліну навчань/допусків, події JML та аномалії доступів. Психометрична якість перевіряється (α Кронбаха, CFA/IRT), етичність забезпечують DPIA/PIA, псевдонімізація, RBAC/ABAC і «just culture».

Формуються фічі (графікові, компетенційні, поведінкові, доступові, опитувальні) із жорстким time-stamping для уникнення leakage. Моделювання поєднує регуляризовані GLM/логіти й ансамблі для подій, survival-аналіз для відтоку, ARIMAX/Prophet для трендів, а також виявлення аномалій (isolation forest/one-class SVM/автоенкодери); якість оцінюється за PR-AUC/AUROC і калібруванням. Пояснюваність та справедливість гарантують XAI (SHAP/LIME), тести bias і policy human-in-the-loop.

Кожен індикатор паспортується (визначення, формула, джерело, власник, частота, пороги, playbook). Типові EWI – падіння афективної прихильності в «гарячих» змінах, сплески понаднормових/абсентеїзму, ріст «near miss», прострочені HSE/LMS, аномалії входів; типові KRI – частота HSE-подій і SoD-порушень, відтік у критичних ролях, дні простоїв, дисциплінарні кейси на 100 FTE. Експлуатація спирається на DWH/Lakehouse, feature store, CI/CD, моніторинг дрейфу, decision logs і SLA «сигнал-реакція» з інтеграцією в ERM/BCM/ISMS; ефекти перевіряються DiD/ITS та CBA/ROI. У підсумку «м’які» конструкти перетворюються на керовані EWI/KRI й відтворювані дії, що знижують імовірність/тяжкість інцидентів і підсилюють стійкість підприємства.

6. Підхід організаційного аналізу мереж (Organizational Network Analysis, ONA) у поєднанні з логікою соціальної надійності для оцінювання персоналу в інтересах економічної безпеки промислового підприємства. Підхід організаційного аналізу мереж (ONA) розглядає взаємодії людей, ролей і підрозділів як мережу вузлів і зв’язків, що

передають знання, координують реагування та підтримують впровадження змін, тим самим виявляючи «одиничні точки відмови», розриви координації та зони потенційної колузії у чутливих процесах (Cross & Parker, 2004; Rothwell, 2010). Його теоретичну основу становлять метрики центральності й посередництва (Freeman, 1979), формальна теорія соціальних мереж (Wasserman & Faust, 1994) та моделі «ключових гравців» і «потокової» центральності (Borgatti, 2005; Borgatti & Everett, 2006). Пояснювальні механізми спираються на «слабкі зв'язки», що пришвидшують дифузію новацій, і «сіммеліанські» трикутники довіри, які підсилюють здатність до змін (Granovetter, 1973; Krackhardt, 1992), а також на концепцію «структурних дір», що показує ризики концентрації інформаційного контролю у брокерів (Burt, 1992, 2004). Баланс когезії та брокерства визначає якість і швидкість передачі знань і, відповідно, операційну надійність (Hansen, 1999; Reagans & Zuckerman, 2001), тоді як «приховані» неформальні мережі часто суттєво відрізняються від формальної ієрархії (Ibarra, 1993, 1995). Теорія складних мереж пояснює вразливість «масштабно-інваріантних» структур до цільових відмов «хабів», що критично для залежності від «зіркових» експертів у виробництві (Barabási, 2002; Newman, 2003); додаткові показники мережевої ефективності та вагові центральності дають інструменти для моделювання затримок і «опору» шляхів знань (Latora & Marchiori, 2001; Opsahl, Agneessens, & Skvoretz, 2010). Інтеграція ONA з логікою соціальної надійності – здатністю системи зберігати функції, відновлюватися та навчатися після відхилень – поєднує аналіз структури взаємодій із управлінням людськими помилками й організаційними аваріями (Reason, 1997; Hollnagel, 2011). Для контуру економічної безпеки це означає раннє виявлення патернів доступів/довіри, що передують інсайдерським інцидентам, а також обґрунтоване планування дублювання компетенцій і наступництва (Collins, Cappelli, & Moore, 2016; Rothwell, 2010).

Методологічна архітектура підходу. Методична архітектура ONA в інтересах економічної безпеки починається з формулювання ризик-гіпотез для критичних процесів (OT/SCADA, ремонт, закупівлі, казначейство, IT-адміністрування). Дані збирають із опитувальних мереж (name generator/roster з тестами інваріантності) та цифрових метаданих без доступу до контенту: календарі, тікети й сервіс-деск, лічильники звернень у пошті/месенджерах, бейдж-входи, події IAM (joiner–mover–leaver), матриці компетенцій, доступів і SoD (Табл. 1.17). Далі будують багатошарову мережу (поради, розв'язання інцидентів, передача змін, спільні розслідування, перетин доступів) із вагами за частотою/тривалістю/критичністю та рухомими «вікнами» 30/60/90 днів; сезонні шуми очищають, приватність забезпечують псевдонімізацією, DPIA/PIA і RBAC/ABAC відповідно до ISO/IEC 27001/27701.

Аналітика охоплює локальні показники (degree/strength, betweenness, closeness, eigenvector, брокерство/constraint, k-core/k-shell, локальні мости, індекс дублювання навичок, мережева ефективність), «мезо»-рівень (ключові гравці, стійкість до фрагментації, спільноти Louvain/Infomap, кліки між конфліктними функціями) та динаміку (edge churn, часова центральність, черги на консультації, траєкторії «перепідключення» після вибуття експерта) (Freeman, 1979; Burt, 1992; Latora & Marchiori, 2001; Barabási, 2002; Newman, 2003).

Результати транслюють у EWI/KRI з «паспортами»: EWI – екстремальна betweenness у потоці змін, спад дублювання навичок у нічних змінах, зростання черг до «хабів», поява «клік» між ролями з SoD-конфліктом, позаграфікові контакти в «червоних зонах»; KRI – час до набуття компетентності, частка ролей без резерву, інциденти через втрату експертизи/затримку змін, MTTR/простої з людських причин, порушення SoD.

Таблиця 1.17

Методологія підходу організаційного аналізу мереж (Organizational Network Analysis, ONA) у поєднанні з логікою соціальної надійності

Назва	Опис	Приклад
Постановка завдання та гіпотез	Визначення критичних процесів і формулювання ризик-гіпотез щодо мережевих уразливостей.	H1: надмірна betweenness одного фахівця у передачі змін → зростання MTTR після аварій.
Опитувальні мережі	Збір даних про неформальні взаємодії (поради, вирішення інцидентів, передача змін) валідованими анкетами.	Name-generator: «До кого звертаєтесь, коли лінія дає збій?» (шкала частоти/важливості).
Цифрові метадані (без контенту)	Агреговані лічильники комунікацій і подій процесів як проксі потоків знань.	Тікети CMMS, звернення в сервіс-деск, календарі, бейдж-доступи, IAM (joiner–mover–leaver).
Карти компетенцій і допуски	Опис та підтвердження критичних навичок, сертифікацій і часу до компетентності.	Матриця навичок HSE/електробезпеки; MTTC для операторів печі випалу.
Нормативна модель SoD/RBAC	«Як має бути»: розподіл доступів і сегрегація обов'язків для виявлення тіньових шляхів.	Заборона суміщати закупівлі-приймання-оплату; рольова модель доступів у ERP.
Побудова мультишарових мереж	Конструювання шарів «порада/інциденти/зміна/доступи», зважування за частотою/критичністю.	Окремі шари для ко-участі в ремонтах і для передачі змін (30/60/90-денні вікна).
Локальна критичність	Оцінка вузлів: degree/strength, betweenness, closeness, eigenvector; брокерство (constraint).	Інженер з найвищою betweenness у нічних змінах → SPOF у відновленні лінії.
Глобальна вразливість і спільноти	Аналіз фрагментації, виявлення «клік» та міжфункціональних мотивів із SoD-конфліктами.	Щільна кліка «закупівлі–склад–облік» без належного SoD → ризик колузії.
Динаміка мереж	Плинність зв'язків, часові центральності, черги на консультації, «перепідключення» після вибуття експертів.	Після звільнення майстра маршрути передачі змін «зависають» на одному новачку.
Конструювання EWI (leading)	Ранні індикатори мережевих ризиків з порогами та правилами ескалації.	Ріст черг на консультації до «хаба» > 80-го перцентиля протягом 2 тижнів.
Конструювання KRI (lagging)	Експозиційні/запізнілі показники для контролю резидуального ризику.	Частка ролей без резерву у нічних змінах; MTTR із людських причин.
Playbooks (керовані дії)	Стандартизовані реакції на мережеві сигнали з відповідальними та SLA.	Ввести «другий номер» на критичну зміну; тимчасовий war-room; ревізія RBAC/SoD.
Перевірка ефектів	Каузальна та квазіекспериментальна оцінка впливу інтервенцій.	DiD/Interrupted Time Series для MTTR, OEE, scrap, HSE-порушень.
Врядування даними та етика	DPIA/PIA, псевдонімізація, RBAC/ABAC, «just culture», заборона контент-моніторингу.	Працюємо лише з метаданими, інформуємо персонал про цілі та межі ONA.
План впровадження (90 днів)	Етапи 0–30/31–60/61–90: від гіпотез і збору даних до пілот-інтервенцій і моніторингу.	0–30: каталог показників; 31–60: EWI/KRI; 61–90: розвантаження хабів, оцінка ефектів.
Обмеження та пом'якшення	Ризики неповноти, плутанини причинності, стигматизації; способи мінімізації.	Комбінування опитувань і цифрових шарів; каузальні дизайни; незалежний нагляд.
Ілюстративний кейс	Стислий приклад практичного результату впровадження.	−33% MTTR, −14% scrap, −28% HSE-порушень після дублювання «хабів» і ревізії SoD.

Джерело: систематизовано автором на основі [1-224]

Playbooks передбачають розвантаження «хабів» (наставництво, «другі номери»), кероване «re-wiring» (war rooms), корекцію RBAC/SoD та тренування відмов «хабів»; ефекти перевіряють до/після, DiD, перерваними часовими рядами, survival-аналізом і мережевими стрес-тестами з XAI-поясненнями внеску ознак. Дотримання пропорційності, прозорої мети й нагляду запобігає стигматизації та «соціальному скорингу» (Reason, 1997; Collins, Cappelli, & Moore, 2016). У підсумку ONA, поєднана з логікою соціальної надійності, забезпечує керовані EWI/KRI, сценарні реакції та поліпшення MTTR, OEE, scrap, HSE і P&L/CF.

7.Етичний та комплаєнс-орієнтований підхід до оцінювання персоналу (далі – ЕКОП) у контексті економічної безпеки промислового підприємства. Етичний і комплаєнс-орієнтований підхід (ЕКОП) трактує оцінювання персоналу як зону правових, репутаційних і операційних ризиків, тому процеси мають бути легітимними (правомірними й пропорційними), пояснюваними та підзвітними з повним аудитним слідом і механізмами оскарження.

У площині приватності застосовується «контекстуальна цілісність» і принципи privacy by design: мінімізація даних, псевдонімізація, контроль доступів (RBAC/ABAC) і документований перенос даних між контекстами (Nissenbaum, 2010; Solove, 2021). Щодо недискримінації ЕКОП визнає ризик відтворення упереджень та неминучі компроміси між «безпекою» і «рівністю»; отже, вибір метрик справедливості має бути заздалегідь нормативно закріплений і прозорий для стейкхолдерів (Barocas & Selbst, 2016; Hardt et al., 2016; Corbett-Davies & Goel, 2018). Пояснюваність забезпечується розмежуванням інтерпретованості та explainability, використанням Model Cards і Datasheets, а також незалежними алгоритмічними аудитами (Lipton, 2018; Mitchell et al., 2019; Raji et al., 2020). У people security діє принцип пропорційності контролів і чіткі, публічні дисциплінарні правила (Collins, Cappelli, & Moore, 2016).

Операційне підґрунтя формують стандарти ISO/IEC 27001, 27701, 37301, 37002, 31000, 23894, рамка NIST AI RMF та настанови «Trustworthy AI» HLEG EU, які визначають спільну мову політик, артефактів і контрольних процедур. У підсумку ЕКОП вбудовує оцінювання персоналу в ERM як керовану, відтворювану й аудитовану практику, що знижує регуляторні та етичні ризики й підвищує легітимність управлінських рішень.

Методологічна архітектура підходу. Методологічно ЕКОП – це інтегрований із ERM/ISMS/BCM соціотехнічний контур, що послідовно проходить шість етапів (Табл. 1.18):

1) врядування й підзвітність (RACI, комітети, кодекси, DPIA/PIA);

2) управління даними (каталоги й метадані, RBAC/ABAC, lineage, політики якості та ретенції);

3) ризик-оцінка й вимоги до privacy/fairness/explainability з моделюванням сценаріїв;

4) проєктування контролів (screening, SoD, access reviews, model cards, decision logs);

5) моніторинг і аудит (контрольні карти, XAI-профілі внеску ознак, незалежні аудити моделей, контроль SLA);

6) безперервне поліпшення (DiD/ITS, CBA/ROI, оновлення політик і порогів).

Метрична система двошарова: EWI як ранні сигнали (збої fairness-метрик, сплеск апеляцій, порушення SLA журналів рішень, інциденти приватності, аномалії XAI-профілів) і KRI як фактична експозиція/наслідки (скасовані дисциплінарні кейси, регуляторні претензії, прострочені аудити моделей, повільні DSAR). Кожен індикатор має «паспорт» (визначення, формула, власник, частота, пороги, playbook). У підсумку ЕКОП робить оцінювання персоналу легітимним, пояснюваним і підзвітним, знижує

правову й репутаційну експозицію, підсилює довіру та забезпечує верифіковані фінансово-операційні ефекти.

Таблиця 1.18

Методологія етичного та комплаєнс-орієнтованого підходу

Назва	Опис	Приклад
Етап 1. Правова основа та дизайн приватності	Визначення правової підстави обробки, проведення LIA/DPIA, опис операцій (ROPA), мінімізація/псевдонімізація даних, встановлення RBAC/ABAC.	Проведення DPIA для моделі пріоритизації навчання операторів OT/SCADA; створення ROPA; впровадження рольових доступів до тренувальних наборів.
Етап 2. Етичний дизайн та критерії справедливості	Нормативний вибір метрик fairness, визначення захищених груп, аудит упереджень (representation, reweighing, калібрування порогів) і фіксація правил у політиках.	Закріплення в політиці критерію *equalized odds* для рішень про допуски; контролі дисбалансу вибірок; протокол відбору атрибутів без прихованих проксі.
Етап 3. Дані, моделі, пояснюваність	Забезпечення якості та lineage, добір інтерпретованих або XAI-підтриманих моделей, документація через Model Cards і Datasheets; тести стабільності пояснень.	Каталог даних і моделей; SHAP-аудит градієнтного бустингу; Model Card із межами застосовності та ризиками; моніторинг дрейфу.
Етап 4. Управлінські процедури, апеляції, «людина в контурі»	Формалізація апеляцій (терміни, канали), ведення decision logs, обов'язковий human-in-the-loop для високоризикових рішень; канали speak-up/whistleblowing.	SLA на апеляцію 10 днів; журнали рішень у кейс-менеджменті; обов'язкова людська перевірка рішень щодо доступів до SCADA; політика ISO 37002.
Етап 5. Моніторинг, аудит, ретенція та видалення	Побудова EWI/KRI, встановлення порогів і MTTD/MTTR, періодичні (внутр./зовн.) аудити моделей і процесів, правила зберігання/видалення даних.	EWI: spike апеляцій; KRI: частка рішень без пояснень; квартальний аудит дрейфу; автоматизована ретенція 12 місяців із журналами доступів.
Етап 6. Врядування та ролі	Наглядові органи (комітет з етики даних/AI, комітет з ризиків), ролі DPO/CISO/CRO, призначення risk/data/model owners, RACI та програми data/ethics literacy.	Створення AI-етичного комітету; затвердження RACI для добору/оцінки/доступів; щорічне навчання керівників з етики даних і алгоритмів.

Джерело: систематизовано автором на основі [1-224]

За результатами проведеного дослідження було узагальнено сильні та слабкі сторони семи підходів до оцінювання персоналу в контексті економічної безпеки підприємств (Табл. 1.19).

Досліджені підходи є взаємодоповнюваними: процесно-нормативний і етичний забезпечують легітимність та контроль, компетентнісний і ризик-орієнтований – операційне фокусування, аналітичний і ONA – ранні сигнали та системний огляд, а поведінковий – культурний вимір.

Оптимальна конфігурація поєднує їх у єдиний контур EWI/KRI, data governance та керованих інтервенцій.

Таблиця 1.19

Сильні та слабкі сторони семи підходів до оцінювання персоналу в контексті економічної безпеки

Підхід	Сильні сторони	Слабкі сторони
1) Компетентнісний і результативний	Прямий зв'язок із процесними та якісними KPI (OEE, FPY, scrap); прозорі вимоги до ролей і допусків (HSE/ІБ); висока придатність до аудиту та переатестації; профілактика «людських» відхилень.	Ризик формалізму («галочки»); суб'єктивність поведінкових індикаторів; «знімковість» оцінок без потокових даних; можливий «розрив» HR від виробничих контурів.
2) Процесно-нормативний (life-cycle)	Повне покриття життєвого циклу працівника (joiner–mover–leaver); зниження інсайдерських ризиків через RBAC/SoD; висока відтворюваність і підзвітність; сумісність із ISMS/BCM.	«Паперова відповідність» без реальних SLA; фрагментація між HR/IT/ІБ; адміністративна трудомісткість; обмежена чутливість до культурно-поведінкових чинників.
3) Ризик-орієнтований і галузевий	Вбудованість у ERM і risk appetite; пріоритизація високої експозиції; сумісність зі стрес-тестами та BCM; фокус на причинно-наслідкових сценаріях.	Надмірна агрегованість heat-maps; вимогливість до якості даних; недооцінка поведінкових драйверів (втома, культура); значні витрати моделювання.
4) Аналітичний (data-driven) і предиктивний	Ранні попередження (EWI); масштабованість і інтеграція різнорідних джерел (HRIS/HSE/OT/IT-логи); вимірний ROI; XAI підвищує довіру до моделей.	Спуріозні кореляції й дрейф; ризики упередженості/проксі-дискримінації; залежність від зрілості data governance/MLOps; хибні спрацювання та перевантаження ескалаціями.
5) Поведенковий та інтегративний (лояльність/залученість)	Виявлення «м'яких» ризиків (вигорання, ерозія культури безпеки); поєднання опитувань і поведінкових даних; таргетування лідерських і організаційних інтервенцій.	Соціальна бажаність відповідей; «втома від опитувань»; складність каузальної атрибуції; ризик репресивного використання результатів.
6) Організаційний аналіз мереж (ONA) та соціальна надійність	Виявлення «одиничних точок відмови» знань; прозорість неформальних потоків; підтримка планів наступництва й дублювання навичок; зниження операційної уразливості.	Чутливість до приватності; ризик хибних висновків через неповні дані; стигматизація «вузлових» осіб; мережі швидко змінюються – потрібен постійний моніторинг.
7) Етичний і комплаєнс-орієнтований	Легітимність і довіра до рішень; зменшення правових ризиків; прозорість та пояснюваність (XAI), формалізовані апеляції; узгодженість із приватністю/антидискримінацією.	«Гіпер-комплаєнс» і сповільнення рішень; ресурсомісткість аудитів і навчання; ризик декларативності без реального нагляду та метрик ефективності.

Джерело: систематизовано автором на основі [1-224]

Отже, досліджені підходи утворюють комплементарну рамку: компетентності та результативність «прив'язують» оцінювання до процесів; life-cycle-контролі гарантують дисципліну доступів; ризик-

орієнтація забезпечує пріоритизацію; аналітика й XAI – раннє попередження та доказовість; поведінково-культурний шар знижує «м'які» ризики; ONA зберігає знання й надійність; етичний/комплаєнс-контур легітимує рішення. Саме їх зшивка через EWI/KRI, паспорти метрик, RACI та журнали рішень перетворює оцінювання персоналу на повноцінну першу лінію захисту економічної безпеки.

Узагальнюючи сучасні інтерпретації, лояльність персоналу доцільно розглядати як багатовимірну конструкцію, що поєднує ставлення працівника до організації, сталі поведінкові патерни та інституційні умови їх підтримки. Базовий атитюдний підхід трактує лояльність як організаційну прихильність трьох компонентів – афективної, нормативної та інструментальної (continuance), що фіксує стійкий психологічний зв'язок працівника з організацією (Meyer & Allen, 1991, 1997; Mowday, Porter, & Steers, 1982). Саме він забезпечує концептуальне «ядро» для операціоналізації опитувальниками (OCQ тощо) і виступає раннім індикатором змін у ризик-профілі людського чинника.

Поведінково-адміністративний ракурс переносить фокус із декларацій на спостережувані дії: дотримання процедур, участь у навчанні/сертифікаціях, дисципліну та позаобов'язкову проорганізаційну поведінку (OCB), що корелює з продуктивністю та надійністю процесів (Organ, 1988; Podsakoff, Whiting, Podsakoff, & Blume, 2009). Таке трактування напряму «прив'язує» лояльність до операційної керованості й метрик економічної безпеки.

У межах теорії соціального обміну лояльність постає як наслідок взаємності між працівником і організацією: сприйнята підтримка, справедливість процедур і дотримання психологічного контракту формують готовність до кооперації та дотримання правил (Blau, 1964; Rousseau, 1995; Eisenberger, Armeli, Rexwinkel, Lynch, & Rhoades, 2001;

Colquitt, 2001). Порушення цих умов прискорює ерозію лояльності й підвищує ризики девіантної поведінки та плинності.

Ідентифікаційно-ціннісний підхід інтерпретує лояльність як ототожнення працівника з цілями, нормами й символами організації; висока ідентифікація підвищує кооперацію й стійкість до стресу, хоча за надмірної конформності можливе «групове мислення» (Mael & Ashforth, 1992; Pratt, 1998; Riketta, 2005). Цей вимір пояснює, чому однакові формальні стимули по-різному впливають на поведінку в різних культурних контекстах.

Калькулятивна (side-bet) логіка розглядає лояльність як функцію накопичених «ставок» – сертифікацій, внутрішнього капіталу, пільг і спеціалізованих навичок, що збільшують витрати виходу і тим самим утримують працівника в організації (Becker, 1960). Вона корисна для прогнозування утримання критичних ролей, але слабше віддзеркалює афективні мотиви.

Парадигма залучення трактує лояльність як енергетично-когнітивну включеність у роботу та організацію («операційна лояльність»), що безпосередньо пов’язана з якістю, безпекою праці й результативністю підрозділів (Kahn, 1990; Harter, Schmidt, & Hayes, 2002; Saks, 2006; Schaufeli & Bakker, 2010). За умови коректної валідизації показників (на кшталт UWES) вона забезпечує практичний місток між «м’якими» станами і «жорсткими» бізнес-метриками.

Мультифокусний і безпековий підхід підкреслює, що лояльність адресована не лише організації загалом, а й керівнику, команді, професії та нормам безпеки; у вимірі кадрової/інформаційної безпеки вона збігається з благонадійністю: дотриманням правил доступу, принципу «мінімальних привілеїв» і готовністю повідомляти про порушення (Meyer & Herscovitch, 2001; NIST, 2020; ISO/IEC 27002, 2022). Відтак лояльність набуває прямого значення для управління інсайдерськими ризиками.

На рівні створення цінності сервіс-профіт логіка показує ланцюг від лояльності та залучення працівників – через якість і задоволеність клієнтів – до фінансових результатів, що дозволяє інтегрувати людський чинник у економіку ЕБП-рішень (Heskett, Sasser, & Schlesinger, 1997). Етичний/критичний ракурс водночас застерігає від ототожнення лояльності зі «сліпою відданістю»: зріла лояльність включає доброчесність і готовність до «speak-up» з належним захистом викривачів (Near & Miceli, 1985; ISO 37002, 2021).

Культурно-інституційне бачення пояснює, що стійка лояльність формується в середовищах із психологічною безпекою, прозорою справедливістю та навчальною орієнтацією, де помилки використовують для вдосконалення, а не для каральної реакції (Schein, 2010; Edmondson, 1999). Такі умови одночасно знижують імовірність інцидентів і підсилюють здатність до відновлення.

Нарешті, індексно-композитні підходи пропонують агрегувати атитюдні, поведінкові та мережеві показники у єдиний індекс лояльності для панелей ризику з прозорою ваговою схемою та звітністю про людський капітал (ISO 30414, 2018; методично: AHP/entropy-weighting). Це забезпечує сумісність з ERM/BCM/ISMS та дозволяє вводити порогові значення і сценарії ескалації. Українська прикладна традиція посилює цей інструментарій через інтеграцію HR-даних (навчання, плинність, дисципліна доступів) у контур економічної безпеки та формування релевантних EWI/KRI для людського чинника (Balabanova & Sardak, 2011; Migus, 2013; Yefimenko, 2024).

У сукупності ці ракурси не взаємовиключні, а комплементарні: атитюди дають ранні сигнали, поведінкові сліди – операційну керованість, соціальний обмін і культура – механізми підтримки, мультифокус і норми безпеки – зв’язок із інсайдерськими ризиками, а композитні індекси – керованість і підзвітність у межах інтегрованої рамки економічної безпеки

(Meyer & Allen, 1991; Organ, 1988; Blau, 1964; Mael & Ashforth, 1992; Becker, 1960; Kahn, 1990; NIST, 2020; ISO/IEC 27002, 2022; ISO 30414, 2018). Така інтеграція переводить управління лояльністю з декларацій у вимірювану, відтворювану та стратегічно узгоджену практику.

За результатами проведеного дослідження, були узагальнені сучасні підходи до трактування поняття «лояльність персоналу» та представлені у табл. В.4 Додатку В.

Вважаємо, що лояльність персоналу доцільно розглядати як багатовимірну конструкцію, що поєднує ставлення працівника до організації, його стійкі поведінкові прояви та організаційні умови, у яких ці стани і дії виникають і підтримуються.

У контексті ЕБП така оптика важлива, оскільки лояльність корелює з імовірністю помилок, інцидентів доступу, дотриманням процедур HSE/ІБ і стабільністю критичних знань. Теоретично й методично ідентифікуємо сім головних ракурсів оцінювання лояльності та водночас підходи до її трактування (таблиця В.6 Додатку В).

Узагальнюючи сучасні ракурси вимірювання лояльності персоналу в контексті економічної безпеки, її доцільно розглядати як багатовимірний конструкт із взаємодоповнювальними операціями вимірювання.

Атитюдний підхід трактує лояльність як організаційну прихильність – афективну, нормативну та інструментальну – і спирається на валідовані опитувальники (OCQ, а також шкали TCM; інколи – UWES, Q12, eNPS), що надають ранні сигнали ризиків поведінкової ненадійності, водночас вимагаючи контролю соціально бажаних відповідей (Meyer & Allen, 1991, 1997; Mowday, Porter, & Steers, 1982).

Поведінково-адміністративний підхід фіксує лояльність у стабільних патернах виконання правил і проорганізаційних дій, перетворюючи цифрові сліди з HRIS/LMS/HSE/OT/IT на EWI/KRI, що забезпечує високу операційну керованість, але ставить вимоги до якості даних і етики

моніторингу (Organ, 1988; Podsakoff, Whiting, Podsakoff, & Blume, 2009). Парадигма соціального обміну пояснює лояльність через взаємність між працівником і організацією – підтримку, справедливість і дотримання психологічного контракту; її ерозія підвищує ймовірність плинності та девіантної поведінки (Blau, 1964; Rousseau, 1995; Eisenberger, Armeli, Rexwinkel, Lynch, & Rhoades, 2001; Colquitt, 2001).

Ідентифікаційно-ціннісний підхід пов'язує лояльність з організаційною ідентифікацією та ціннісною конгруентністю, що посилюють кооперацію та стресостійкість, але можуть породжувати «groupthink» і приглушувати критичний speak-up (Mael & Ashforth, 1992; Pratt, 1998; Riketta, 2005).

Калькулятивний (side-bet) підхід інтерпретує лояльність як наслідок зростання «вартості виходу» завдяки специфічним інвестиціям у кар'єру та пільги; він корисний для моделей утримання, хоча слабко охоплює афективний вимір (Becker, 1960). Рамка залучення (engagement) пропонує операційний сурогат лояльності, що виразно корелює з результативністю та безпекою, однак потребує чіткої валідизації, аби уникнути підміни понять (Kahn, 1990; Harter, Schmidt, & Hayes, 2002; Saks, 2006; Schaufeli & Bakker, 2010). Нарешті, мультифокусна та безпекова лояльність інтегрує прив'язаність до різних «цілей» (організація, керівник, команда, професія) з вимогами благонадійності та дотримання режимів доступу, програмами speak-up і «just culture», що безпосередньо знижує інсайдерські ризики та узгоджується зі стандартами ISMS/NIST (Meyer & Herscovitch, 2001; NIST, 2020; ISO/IEC 27001/27002, 2022).

У сукупності ці підходи формують надійний вимірювальний контур: атитюдні індикатори дають ранню діагностику намірів, поведінкові – забезпечують керованість і аудитовність, а обмінні, ідентифікаційні та безпекові – задають механізми інтервенцій, що критично важливо для EWI/KRI у системі економічної безпеки. Це мінімізує вади кожного підходу

та переводить управління лояльністю з декларацій у керовану, вимірювану й підзвітну практику економічної безпеки.

Таблиця 1.20

Сильні та слабкі сторони основних підходів до оцінювання лояльності персоналу в контексті економічної безпеки підприємства

Підхід	Сильні сторони	Слабкі сторони
Атитюдний (commitment-based)	Теоретично обґрунтований (TCM); валідовані шкали (OCQ/ACS/NCS/CCS); ранні сигнали плинності; придатний для порівнянь і трекінгу динаміки.	Самозвіт і соціальна бажаність; інваріантність між культурами не завжди гарантована; «повільна» метрика; опосередкований зв'язок з ІБ/ЕБ-контролями.
Поведінково-адміністративний (behavioral trace)	Об'єктивні цифрові сліди (HRIS/LMS/HSE/OT/IT); висока операційна керованість; легко мапується в EWI/KRI; аудитовність, близькість до причин інцидентів.	Вимоги до даних і governance; конфаундинг контекстом; ризик хибних спрацювань/Goodhart; питання приватності/етики.
Обмінний/довіри (social exchange)	Пояснює механізми (POS, справедливість, психоконтракт); чіткі інтервенції HR/ERM; передбачає девіації та плинність.	Складність вимірювання (SEM, медіації); часові лаги; висока «вартість» змін у практиках; культурна чутливість.
Ідентифікаційно-ціннісний	Стабільна орієнтація на місію/норми; пов'язаний із OCB, кооперацією, резилієнс-поведінкою.	Ризик конформізму/«groupthink» і пригнічення speak-up; абстрактність метрик; повільна реакція на зміни.
Калькулятивний (side-bet)	Квантифікує «вартість виходу»; простий у моделюванні утримання; легко інтегрується з HRIS/фінданими.	Ігнорує афективні/етичні виміри; може стимулювати «застійну» лояльність («золоті наручники»); не знижує інсайдерський ризик.
Залучення як «операційна лояльність» (engagement)	Сильні кореляції з продуктивністю/якістю/HSE; бенчмарки (UWES, Gallup); чутливий до програм покращення.	Перекриття з commitment; сезонність/«ефект кампаній»; ризик «геймінгу» індексів; залежність від якості інструментів.
Мультифокусна та безпекова лояльність	Пряма інтеграція з ERM/ISMS/BCM; операціоналізація через JML, RBAC/SoD, speak-up; дає дієві EWI/KRI для інсайдерських ризиків.	Високі вимоги до міжфункціональної координації й комплаєнсу; ризик «surveillance creep»; небезпека «паперової» відповідності.

Джерело: систематизовано автором на основі [1-224]

Отже, жоден з досліджених підходів до оцінювання лояльності персоналу в контексті економічної безпеки не є вичерпним. Для надійного управління ризиками людського чинника в системі економічної безпеки

варто поєднувати атитюдні метрики (ранні сигнали) з поведінковими індикаторами (операційна керованість), підсилюючи їх рамками соціального обміну та мультифокусної/безпекової лояльності (EWI/KRI, JML, RBAC). Це забезпечує і прогностичність, і дієвість управлінських рішень.

Висновки до першого розділу

За результатами проведеного дослідження доцільно зробити наступні висновки.

1. Проведений порівняльний аналіз засвідчив, що провідні підходи до ІАЗ ЕБ (функціональний, системний, ризик-орієнтований ISO/COSO, інституційний, стейкхолдерський, ресурсно-компетентнісний та цифрово-соціотехнічний) не взаємовиключні, а взаємодоповнювані. ІАЗ ЕБ доцільно тлумачити як інтегровану соціотехнічну рамку, у якій «стан» безпеки задає ціль, а «спроможність» – механізм її досягнення й підтримання. Практична конфігурація такої рамки охоплює п’ять узгоджених блоків: інформаційний (стандартизовані дані та data lineage), аналітичний (EWI/KRI, сценарне моделювання, XAI), організаційний (ролі, RACI, журнали рішень), технологічний (DWH/Lakehouse, SIEM/SOAR, CI/CD аналітики) та нормативно-регламентний (RBAC/ABAC, комплаєнс, аудит). Мінімальний «тест зрілості» ІАЗ ЕБ включає: актуальний реєстр ризиків і карту даних; паспортовані EWI/KRI з порогами та власниками; формалізовані ескалації; журнали трансформацій і рішень; політики безперервності (RTO/RPO) та етико-правові протоколи обробки персональних і комерційних даних. За таких умов ІАЗ виходить за межі «звітності» й перетворюється на керовану практику, прив’язану до фінансово-операційних результатів (P&L/CF, продуктивність, якість, простої).

2. Управління персоналом є «першою лінією захисту» системи економічної безпеки, оскільки саме через HR-процеси реалізуються профілактика, раннє виявлення та стримування ризиків людського чинника. Доведено наявність щонайменше шести причинно-наслідкових каналів впливу HR на ЕБ: (1) продуктивність і якість (OEE, FPY, scrap rate); (2) безперервність операцій (кадрова спроможність, баланс змін, time-to-fill критичних позицій); (3) правові та регуляторні ризики (HSE, трудове право, комплаєнс); (4) інформаційна та інсайдерська безпека (RBAC/SoD, joiner–mover–leaver, своєчасна деактивація доступів); (5) соціально-трудові відносини та культура (залученість, «just culture», дисципліна дотримання правил); (6) збереження знань і наступництво (усунення «одиничних точок відмови»). Ефективність цих каналів забезпечує двобічний обмін даними між HR і контуром безпеки: HR-KPI трансформуються у вхідні EWI/KRI для кадрової безпеки, а сигнали безпеки калібрують політики добору, навчання, мотивації та доступів. Ключовими умовами дієвості є інтеграція HR-даних з HSE та OT/SCADA, паспортовані індикатори (EWI/KRI), формалізовані ескалації, наглядові механізми (комітети з ризиків) та постійна валідація метрик. У такій конфігурації HR переходить від допоміжної функції до опорного елементу економічної безпеки.

3. Досліджено й систематизовано підходи до оцінювання персоналу в контексті економічної безпеки (компетентнісний і результативний; процесно-нормативний / J-M-L; ризик-орієнтований і галузевий; аналітико-предиктивний / data-driven; поведінково-інтегративний; мережевий / ONA з логікою соціальної надійності; етично-комплаєнсний) та, окремо, підходи до оцінювання лояльності персоналу (атитюдний / commitment-based; поведінково-адміністративний / behavioral trace; обмінний / social exchange; ідентифікаційно-ціннісний; калькулятивний / side-bet; залучення як «операційна лояльність»; мультифокусна й «безпекова» лояльність). Установлено, що інтеграція зазначених підходів забезпечила перехід від

разових атестацій до керованої, відтворюваної та підзвітної практики першої лінії захисту від ризиків людського чинника в системі економічної безпеки підприємства.

Обґрунтовано, що оцінювання персоналу має бути інтегрованим із ERM/BCM/ISMS і спиратися на стандартизовані EWI/KRI, «паспорти» індикаторів, RBAC/ABAC та SoD, а також на XAI-пояснюваність моделей і належне data governance. Доведено зв'язок результатів оцінювання з операційними та фінансовими метриками (OEE, FPY, MTTR, простої, P&L/CF) через механізми дисципліни виконання, стабільності процесів і якості рішень щодо доступів. Систематизовано інструментарій: від job analysis, BARS/робочих проб і SPC до каузальних та предиктивних моделей, сценарного аналізу і квазіекспериментів (DiD/ITS) для перевірки ефектів інтервенцій.

4. Досліджено оцінювання лояльності персоналу як окремий напрям: вивчено атитюдні виміри (афективна, нормативна, інструментальна прихильність), залученість, ідентифікацію та мультифокусну/«безпекову» лояльність. Показано, що лояльність виконує роль випереджального індикатора ризиків плинності, девіантної/інсайдерської поведінки та порушень HSE/ІБ; запропоновано комбінувати валідовані опитувальні шкали (OCQ, UWES, safety-climate) з поведінково-адміністративними слідами (HRIS/LMS/HSE/IAM/OT) і перетворювати їх на EWI/KRI із заздалегідь визначеними порогами та playbooks. Виявлено типові обмеження (упередженість опитувань, фрагментація даних, ризики приватності) і доведено, що їх нівелюють XAI, DPIA/PIA, уніфіковані словники/метадані та аудиторська трасованість.

За результатами дослідження запропоновано інтегровану рамку: «оцінювання компетентностей і лояльності → прив'язка до процесних/ризик-метрик → керовані інтервенції → перевірка економічного ефекту → оновлення моделей і політик». Зроблено висновок, що поєднане

оцінювання персоналу та його лояльності підвищило керованість людського чинника, зменшило імовірність і тяжкість інцидентів та сприяло стійкості промислового підприємства у вимірі економічної безпеки.

5. За результатами проведених досліджень було опубліковано 2 статті у фахових виданнях України та тези доповідей на конференціях різного рівня.

РОЗДІЛ 2
АНАЛІЗ СТАНУ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ ОЦІНЮВАННЯ ЛОЯЛЬНОСТІ ПЕРСОНАЛУ В СИСТЕМІ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПРОМИСЛОВИХ ПІДПРИЄМСТВ

2.1. Сучасний стан економічної безпеки промислових підприємств

Економічна безпека промислового підприємства (ЕБП) у сучасній науковій традиції трактується як інтегральна здатність господарюючої системи своєчасно ідентифікувати загрози, запобігати їх матеріалізації, витримувати вплив реалізованих ризиків і відновлювати цільові параметри функціонування без критичної втрати вартості, керованості та конкурентоспроможності. Така інтерпретація виходить за межі суто фінансових показників і охоплює виробничо-операційні, технологічні та інформаційні, екологічні та соціально-кадрові виміри безпеки, включно з корпоративним управлінням і комплаєнсом.

Актуальність проблематики зумовлюється поєднанням зовнішніх турбулентностей – ціновою волатильністю енергоресурсів, фрагментацією ланцюгів постачання, геоекономічними обмеженнями – та внутрішніх трансформацій, зокрема прискореною цифровізацією, автоматизацією виробництва і зростанням кіберзагроз. За цих умов ЕБП виступає не стільки «станом рівноваги», скільки динамічною властивістю адаптивності, що виявляється у здатності підтримувати безперервність критичних процесів та забезпечувати прийнятний рівень операційної і фінансової стійкості під дією шоків. Відповідно, дослідження сучасного стану ЕБП потребує одночасної уваги до короткострокових індикаторів ліквідності та безперервності, і до довгострокових чинників інвестиційної спроможності, інноваційності та технологічної зрілості. Важливо наголосити на

обмеженості традиційних лінійних та суто порогових підходів, які, попри простоту інтерпретації, часто ігнорують кореляційну структуру показників, асиметрію розподілу шоків і кумулятивний ефект взаємопов'язаних ризиків. На зміну «статичному знімку» безпеки приходить концепція профілю вразливостей і запасів міцності, що має відслідковуватися у часовій динаміці та постійно оновлюватися з урахуванням зміни зовнішніх і внутрішніх умов. Саме така концептуалізація задає рамку для коректної операціоналізації показників і підбору релевантного інструментарію оцінювання.

Оцінювання економічної безпеки (ЕБ) є необхідним для оперативного прийняття рішень менеджментом, наглядовими радами, кредиторами та державними органами. У періоди підвищеної турбулентності саме публічно верифіковані дані дають можливість швидко й відтворювано визначати, чи перебуває підприємство у «зеленій», «жовтій» чи «червоній» зоні ризику.

Методологічна архітектура оцінювання сучасного стану ЕБП має спиратися на п'ять взаємопов'язаних принципів: системність, превентивність, адаптивність, вимірюваність та порівнянність.

Принцип системності вимагає повного охоплення ланцюга створення вартості – від забезпечення ресурсами, виробничих процесів і якості продукції до збуту, сервісу та післяпродажної підтримки – а також горизонтального узгодження підсистем (фінанси, виробництво, ланцюги постачання, ІКТ/інформаційна безпека, HSE/екологія, персонал).

Превентивність означає пріоритет «випереджальних» (leading) індикаторів над «запізнілими» (lagging): інтенсивність інцидентів, аномалії в логістиці, збої в IT-активах, плинність критичних кадрів мають сигналізувати раніше, ніж з'являться втрати виручки чи зниження маржинальності.

Адаптивність передбачає регулярне сценарне моделювання і стрес-тестування (енергетичні, логістичні, попитні, кадрові та IT-сценарії) з

переглядом порогових значень у відповідь на структурні зрушення середовища. Вимірюваність потребує чіткої операціоналізації конструкта ЕБП: нормування показників (min–max, відстань до еталона), прозорого зважування (експертні методи на кшталт AHP або дано-керовані – ентропійні ваги), побудови композитних індексів та підіндексів із валідацією чутливості.

Порівнянність вимагає бенчмаркінгу як у динаміці (між періодами чи підрозділами), так і в статиці (відносно галузевих квартилів або ефективного фронту за допомогою DEA), що дозволяє відокремити ідеосинкратичні фактори від загальносекторних. Крос-секційна і часово-рядна інтерпретація результатів повинна супроводжуватися управлінням якістю даних (своєчасність, повнота, узгодженість, трасованість), оскільки низька якість інформації зумовлює спотворення сигналів і підвищує ймовірність хибних управлінських рішень. Додатковою умовою коректності оцінювання є інституційні механізми – політики та процедури контролю, внутрішній аудит, відповідність міжнародним стандартам (управління ризиками, безперервність бізнесу, інформаційна безпека), що забезпечують відтворюваність і надійність вимірювань.

За результатами проведених досліджень були систематизовані підходи до оцінки стану економічної безпеки промислових підприємств (Табл. 2.1).

Першим, концептуально-категоріальним, є підхід української школи, який трактує економічну безпеку підприємства як стан захищеності потенціалу, інтересів і здатності до розвитку в умовах загроз. Класичною працею тут є монографія Козаченко, Г. В., Пономарьова, В. П., та Ляшенка, О. М. (2003), де розкрито сутність та механізм забезпечення економічної безпеки через систему цілей, функцій і інструментів, що інтегрує фінансові, виробничі, інноваційні та організаційні аспекти. Саме ця рамка закладає ідею багатовимірності безпеки та необхідності її інституціалізації в управлінні підприємством.

Таблиця 2.1

Систематизовані підходи до оцінки стану економічної безпеки промислових підприємств

Підхід	Як працює (core idea)	Коли доречний	Переваги	Обмеження
Порогово-індикативний	Набір KPI з порогами (зелений/жовтий/червоний)	Старт, регулярний моніторинг	Простий, прозорий, швидкий	Статичні пороги «не бачать» контексту й кореляцій
Інтегральний індекс	Нормування показників → ваги → єдиний бал (0–1)	Порівняння цехів/філій/періодів	Системність, компактний результат	Вибір ваг суб'єктивний; приховує деталі
Таксономічний/ентропійний індекс	Відстань до «еталона» або ваги з інформаційної ентропії	Великі набори показників	Менше суб'єктивності, чутливий до «вузьких місць»	Вимогливий до якості даних
Ризик-орієнтований (ISO 31000)	Ідентифікація загроз, імовірність×вплив, карти ризиків, VaR/CVaR	Інвестпроєкти, безперервність, ланцюги постачань	Фокус на причинах і пріоритетах	Потребує експертів, баз даних інцидентів
Функціонально-компонентний	Окремі під-індекси: фінанси, виробництво, ІКТ, HSE, персонал тощо	Операційний контроль	Добре показує, «де болить»	Може дублювати метрики, важко агрегувати
Процесно-аудиторський/зрілість	Чек-листи/аудит за стандартами (COSO, ISO 9001/22301/27001)	Комплаєнс, сертифікація	Оцінює керованість і превенцію	«Ставить галочки», але не гарантує результат
Сценарії та стрес-тести	Моделювання шоків (ціна енергії, збут, відмова постачальника)	Енергомісткі, експортні підприємства	Показує запас міцності	Сценарії залежать від гіпотез
Бенчмаркінг/DEA	Порівняння з галузевим front-tier, ефективність перетворення ресурсів	Кластер/група підприємств	Об'єктивує цілі покращення	Потребує якісних зовнішніх даних
МКР та нечітка логіка (AHP/TOPSIS, fuzzy)	Мультикритеріальне зважування з невизначеністю	Коли багато якісних критеріїв	Гнучко враховує експертність	Складність пояснення, налаштування
Дані/ML, раннє попередження	Z-score, логрег, ML-класифікація, аномалії	Вчасне виявлення деградації	Сильний сигнал «на випередження»	Ризик оверфіту, потреба в історії даних

Джерело: систематизовано автором на основі [1-224]

Другий, фінансово-безпековий підхід, фокусується на фінансовій стійкості як «ядрі» економічної безпеки. У вітчизняній традиції його системно репрезентовано працями Барановського, О. І. (1999; 2004), який обґрунтовує методологію оцінки та механізми забезпечення фінансової безпеки через систему індикаторів платоспроможності, ліквідності, капіталізації та ризиків, а також зв'язує їх із державними та ринковими інститутами. Додатково, на рівні підприємства цей вектор підсилюють напрацювання Бланка, І. А., що формують управлінський контур фінансової безпеки (політика капіталу, боргу, ліквідності, інвестицій). Така призма задає «кістяк» кількісних показників для подальших інтегрованих індексів.

Третій підхід – індикативно-інтегральний – агрегує множину фінансових та нефінансових ознак в єдиний індекс (рейтинґ), що придатний для міжфірмового та міжчасового порівняння. Сутнісно він спирається на логіку багатовимірного вимірювання результативності, популяризовану у «збалансованій системі показників» (Kaplan, R. S., & Norton, D. P., 1992): поєднання фінансових і операційних перспектив, причинно-наслідкових зв'язків і цільових карт. У площині економічної безпеки такий підхід означає конструювання зважених субіндексів (ліквідність, борг, маржинальність, операційна безперервність тощо) з чіткими порогами та прозорими вагами.

Четвертий – ризик-орієнтований (ERM) – переносить акцент із постфактум-метрик на ідентифікацію, оцінювання та обробку ризиків на рівні стратегії й процесів. У міжнародних стандартах це відображено в ISO 31000:2018, який задає принципи, рамку і процес управління ризиками для будь-яких організацій, та в рамці COSO ERM (2017), що інтегрує ризик у стратегію, постановку цілей і моніторинг виконання. Для безпекового оцінювання підприємства це означає не лише вимір «стану» через коефіцієнти, а й оцінку «резервів стійкості» та зрілості процесів ризик-менеджменту.

П’ятий – предиктивно-діагностичний – використовує статистичні моделі для прогнозування дистресу/банкрутства. Класичні праці Beaver, W. H. (1966) продемонстрували прогностичність окремих фінансових коефіцієнтів (уніваріантний аналіз), що згодом було узагальнено Altman, E. I. (1968) у Z-рахунок на основі багатовимірної дискримінантної моделі. Для економічної безпеки такі моделі виконують функцію раннього попередження та калібрування «червоних зон» індикаторів.

Шостий – підхід багатокритеріального вибору (MCDM) – формалізує зважування суперечливих критеріїв безпеки. Аналітична ієрархічна процедура Saaty, T. L. (1980) надає механізм парних порівнянь і узгоджених ваг, тоді як Hwang, C.-L., & Yoon, K. (1981) (TOPSIS та інші MADM-методи) ранжують альтернативи за близькістю до «ідеальної» точки. В контексті ЕБ ці інструменти дозволяють об’єктивувати ваги субіндексів та обирати портфелі управлінських дій (наприклад, між інвестиціями в енергоефективність і підвищенням ліквідності) за множиною критеріїв.

Сьомий – нечітко-множинний (fuzzy) – моделює невизначеність і лінгвістичні оцінки (наприклад, «високий ризик», «помірна ліквідність») через функції належності; це дає змогу уникати жорстких порогів і втрат інформації на «краях» інтервалів. Теоретичне підґрунтя закладено Zadeh, L. A. (1965) та застосовується для побудови нечітких індексів ЕБ, коли дані фрагментарні або якісні.

Восьмий – ефективнісний/фронтирний – використовує Data Envelopment Analysis (DEA) для зіставлення підприємств відносно «кращої практики» з точки зору перетворення ресурсів на результати. Класична робота Charnes, A., Cooper, W. W., & Rhodes, E. (1978) пропонує нелінійне програмування для оцінювання технічної ефективності; в безпековій площині це дає змогу оцінити, наскільки «кошик ресурсів безпеки» (ліквідність, капітал, страхове покриття) трансформується у стійкість (стабільність потоків, витривалість до шоків) у порівнянні з еталоном.

Дев’ятий – підприємницько-стратегічний – наголошує на інституційних та ринкових механізмах зміцнення безпеки бізнесу (стійкість підприємництва, інвестиційна/інноваційна спроможність, антикризові інструменти). В українській літературі його репрезентовано, зокрема, монографією Васильціва, Т. Г. (2008), де систематизовано стратегії й механізми посилення економічної безпеки підприємництва в умовах високої турбулентності.

Нарешті, у межах організаційно-процесної оптики, «фінансова безпека підприємства» у працях Бланка, І. А. розглядається як керована підсистема корпоративних фінансів (стандартизація політик, ковенанти, розподіл ризик-апетиту, контроль ліквідності та інвестицій), що забезпечує інтеграцію безпекових рішень у щоденні фінансові процеси та капітальне планування. Ця перспектива зручна для регуляторного та банківського діалогу, коли ЕБ потрібно «приземлити» до фінансових KPI та договірних обмежень.

Узагальнюючи, означені підходи не взаємовиключні, а комплементарні: концептуальна рамка (Козаченко та ін.) задає предмет і функції безпеки; фінансово-безпековий блок (Барановський; Бланк) – вимірювальну основу; індикативний та MCDM-інструментарій (Kaplan & Norton; Saaty; Hwang & Yoon) – прозоре агрегування; ERM-стандарти (ISO 31000; COSO) – процесну вмонтованість у стратегію; предиктивні та ефективнісні моделі (Beaver; Altman; Charnes, Cooper & Rhodes) – раннє попередження і бенчмаркінг; нечітко-множинні методи (Zadeh) – роботу з невизначеністю та якісними розкриттями; підприємницько-стратегічна оптика (Васильців) – механізми зміцнення на рівні галузей і ринків. Разом вони формують послідовну методологію оцінювання економічної безпеки, здатну одночасно фіксувати «стан», прогнозувати «траєкторію» та підказувати «дії» для менеджменту.

За результатами проведеного дослідження, пропонуємо авторську

методику оцінювання стану економічної безпеки підприємства, яка відрізняється від інших підходів такими параметрами:

1. *Запропонована методика використовує дані виключно з відкритих джерел* – використовуються річна/квартальна фінзвітність (IFRS/НП(С)БО), аудиторський звіт і примітки (ризики, ковенанти, судові справи, події після дати балансу). Жодних внутрішніх операційних KPI, які недоступні широкому колу користувачів.
2. *Методика пропонує використовувати прозору формулу й «анти-black-box» дизайн* – інтегральний індекс S є зваженим поєднанням кількісного та якісного блоків із чітко прописаними порогами; шкали дискретні, інтервали не перетинаються, правила «гейткиперів» і гістерезису запобігають штучним «стрибкам».
3. *В запропонованій методиці збалансовані кількісні та якісні показники* – поряд із фінансовими коефіцієнтами враховано якість аудиторської думки, стан ковенантів, юридичні/регуляторні ризики та прозорість розкриття інформації про стан економічної безпеки підприємства.
4. *Легка імплементація* – запропонована методика від початку спроєктована для реалізації в Excel/BI без спеціалізованих статистичних пакетів.

Запропонована методика оцінювання стану економічної безпеки промислових підприємств побудована як прозора, відтворювана рамка, що спирається виключно на відкриту фінансову звітність (річну/квартальну за МСФЗ або НП(С)БО), аудиторський звіт і примітки до фінансових звітів. Її мета – перетворити наявні публічні дані на єдиний підсумковий індикатор, придатний для міжчасового та міжфірмового порівняння і безпосередньо прив’язаний до управлінських дій.

У центрі методики – інтегральний індекс $S \in [0;1]$, який конструюється як зважене поєднання двох блоків: кількісного й якісного.

Кількісний блок (S_{quant}) формують стандартні фінансові коефіцієнти з Форм №1–3 річної та квартальної фінансової звітності підприємства (Табл. 2.2). Кожен показник нормується за простою дискретною шкалою 0; 0,3; 0,6; 1,0 із чітко визначеними порогами. Після нормування ці оцінки агрегуються у зважене середнє з фіксованими вагами, що відображають їхню відносну предиктивність для платоспроможності, маржинальності та інвестиційної спроможності.

Таблиця 2.2

Кількісні показники оцінювання стану економічної безпеки підприємства

Код	Показник (джерело)	Формула	0 балів (умова)	0,3 бали (умова)	0,6 бали (умова)	1,0 бал (умова)	Вага
Q1	Поточна ліквідність (Баланс)	Оборотні активи / Поточні зобов’язання	< 1,00	1,00–<1,20	1,20–<1,50	≥ 1,50	0,12
Q2	Покриття відсотків (Звіт про фінрез.)	EBIT / Фінансові витрати	< 1,00	1,00–<2,00	2,00–<4,00	≥ 4,00	0,14
Q3	Чистий борг/EBITDA (Баланс+ФР)	(Позики – Гроші) / EBITDA	> 5,00 або EBITDA ≤ 0	>3,50 – ≤5,00	>2,00 – ≤3,50	≤ 2,00	0,14
Q4	Маржа операц. грош. потоку (РГК)	CFO / Виручка	< 0% (від’ємна)	0% – <5%	5% – <10%	≥ 10%	0,12
Q5	EBITDA-маржа (ФР)	EBITDA / Виручка	< 5%	5% – <10%	10% – <20%	≥ 20%	0,10
Q6	Оборотність активів (ФР+Баланс)	Виручка / Середні активи	< 0,30	0,30 – <0,50	0,50 – <1,00	≥ 1,00	0,08
Q7	DSO – дні дебіторки (Баланс+ФР)	365 × Дебіторка / Виручка	> 120 дн	>75 – ≤120 дн	>45 – ≤75 дн	≤ 45 дн	0,10
Q8	CAPEX/Амортизація (РГК+ФР/Прим.)	Капвкладення / Амортизація	< 0,70	0,70 – <1,00	1,00 – <1,50	≥ 1,50	0,10

Джерело: розроблено автором

Якісний блок (S_{qual}) ґрунтується на інформації, яку можна безпосередньо прочитати в аудиторському звіті та примітках до річної фінансової звітності: думка аудитора та ознаки «going concern», виконання фінансових ковенантів і профіль погашень, наявні юридичні/регуляторні ризики й умови резервування, концентрація клієнтського та кредитного ризику (у т.ч. ECL-політика), прояви та наслідки операційних шоків (безперервність/BCP, пошкодження активів, страхове покриття, доступність енергії й логістики), а також якість фінансового розкриття (повнота, узгодженість, сегментна деталізація). Кожна з шести якісних ознак оцінюється за уніфікованою шкалою 0–4 (від «критично негативний вплив» до «сильно позитивний»), далі лінійно приводиться до інтервалу [0;1] поділом на 4 і агрегується за наперед заданими вагами (Табл. 2.3).

Таблиця 2.3

Якісні показники оцінювання стану економічної безпеки підприємства

Код	Якісний показник	Де шукати в звітності	Приклади ознак для оцінки	Вага
QL1	Думка аудитора / going concern	Аудиторський звіт, IAS 1	Модифікації; застереження щодо GC; emphasis of matter	0,25
QL2	Ковенанти та графік погашень	Ноти до позик (IFRS 7/IAS 1)	Виконання/невиконання; покриття ковенантів; концентрація короткострокових погашень	0,20
QL3	Юридичні/регуляторні ризики	IAS 37, примітки про суди/штрафи	Розмір/ймовірність/резервування; наявність страхувань/гарантій	0,15
QL4	Кредитний та клієнтський ризик	IFRS 7 (концентрації)	Частка топ-клієнтів; очікувані кредитні збитки ECL; політика резервування	0,15
QL5	Операційна безперервність (BCP/наслідки шоків)	MD&A/подальші події	Пошкодження активів; плани відновлення; застрахованість; доступність енергії/логістики	0,15
QL6	Фінансова прозорість/якість розкриття	Увесь комплект приміток	Повнота, узгодженість, сегментні дані, гранулярність ризик-ноти	0,10

Джерело: розроблено автором

Питома вага для кількісних та якісних показників була розрахована за результатами проведеного опитування експертів у сфері економічної безпеки підприємств, за допомогою анкети (Додаток Д.2).

Підсумковий індекс стану економічної безпеки підприємства (S) визначається простою формулою:

$$S=0,70\ Squant+0,30\ Squal, \qquad (2.1)$$

де співвідношення 70/30 відображає пріоритет «твердих» фінансових метрік за одночасного врахування «якості цифр» (аудиторська думка, ковенанти, ризикові примітки).

Інтерпретація індексу стану економічної безпеки підприємства (S) здійснюється за єдиною шкалою, представленою у табл. 2.4. Запропонована шкала перетворює інтегральний індекс S на чіткі управлінські категорії – високий, задовільний, вразливий, критичний стан економічної безпеки підприємства.

Метою зазначеної шкали є перетворення безрозмірної оцінки на керовані управлінські категорії з однозначними тригерами дій, які можуть застосовуватись для скринінгу й моніторингу промислових підприємств на основі виключно відкритої фінансової звітності (річної/квартальної), аудиторського звіту та приміток.

Шкала побудована на чотирьох принципах: прозорості (чіткі пороги й детерміновані правила), сталості класифікації (захист від випадкових «стрибків»), обачності (санкції за неповноту або непідтвердженість даних) та пріоритеті безпекових «гейткиперів» (критичні ризик-сигнали мають перевагу над формально високим балом).

Зміст категорій має безпосередню управлінську інтерпретацію. *Високий рівень економічної безпеки* ($S\geq0,80$) означає підтверджену платоспроможність, маржинальність і якість розкриття; типовими діями є підтримка існуючих практик, точкові оптимізації та квартальні міні-стрес-

тести.

Таблиця 2.4

Шкала для підсумкового індексу стану економічної безпеки підприємства (S)

Діапазон S	Категорія	Управлінська інтерпретація	Мінімальні умови (гейткипери)	Базові управлінські дії	Частота перегляду
S≥0,80	Високий рівень економічної безпеки	Стійка платоспроможність і маржинальність; ризики покриті політиками/страхуванням; розкриття якісне	Squant≥0,75 і Squal≥0,70	Підтримувати практики; точкові оптимізації; щоквартальні міні-стрес-тести	Квартально
0,65≤S< 0,80	Задовільний рівень економічної безпеки	Переважно керований ризик-профіль; є «жовті зони», що не загрожують безперервності	Squant≥0,60 та відсутні критичні застереження аудитора (QL1≥2)	Цільові поліпшення (DSO, відсоткове покриття, CAPEX/Аморт); посилений моніторинг	Щомісяця (операційно) / щокварталу (рада)
0,50≤S< 0,65	Вразливий рівень економічної безпеки	Підвищена чутливість до шоків; окремі фінансові/правові тригери можуть спричинити касові розриви	Будь-який з фактів вимикає підвищення: Squant<0,50 QL1≤1 (going concern/модифікована думка), істотні невиконані ковенанти	«Програма відновлення»: план ліквідності (LCR), переговори з кредиторами/клієнтами, скорочення DSO, переоцінка CAPEX	Щотижня (операційно) / щомісяця (рада)
S<0,50	Критичний рівень економічної безпеки	Висока ймовірність втрати безперервності/порушення ковенантів; потрібні негайні заходи	Наявність модифікованої думки/суттєвої невизначеності GC (QL1=0), дефіцит відсоткового покриття (Q2=0)	Антикризова програма: стабілізація ліквідності, moratorium на некритичний CAPEX, реструктуризація, BCP/DR-тести	Щоденно (операційно) / щотижня (рада)

Джерело: розроблено автором

Задовільний рівень економічної безпеки (0,65–0,79) відображає керований ризик-профіль із «жовтими зонами»; доцільні цільові поліпшення (DSO, покриття відсотків, співвідношення CAPEX/амортизації) і посилений моніторинг. *Вразливий рівень економічної*

безпеки (0,50–0,64) сигналізує про підвищену чутливість до шоків та потребує програми відновлення (план ліквідності, переговори щодо ковенантів, прискорення інкасації дебіторки, ревізія інвестицій). *Критичний рівень економічної безпеки* (<0,50) вказує на високу ймовірність втрати безперервності діяльності та потребує антикризової програми: стабілізації ліквідності, реструктуризації зобов'язань, мораторію на некритичний CAPEX і регулярних BCP/DR-тестів.

Регламент застосування передбачає квартальне оновлення індексу, а також щорічний перегляд порогів для окремих коефіцієнтів з урахуванням секторальної специфіки (металургія, хімія, енергетика, транспорт) без порушення базової логіки шкали.

Для звітності рекомендуємо супроводжувати категорію числовими компонентами S_{quant} та S_{qual}, помітками про застосовані коригування (фільтр даних, gatekeepers, гістерезис) і використовувати уніфіковану візуалізацію (зелений/світло-зелений/жовтий/червоний). Пороги допускають обмежену секторальну адаптацію (±10–20% для окремих коефіцієнтів) за умови збереження базової логіки та щорічного перегляду; надмірна мінливість між кварталами є сигналом до розширення ε-зони або посилення гістерезису.

Для підвищення надійності одержаних розрахунків вважаємо за необхідне запровадити три допоміжні правила.

По-перше, «фільтр даних» знижує категорію на один рівень, якщо заповненість кількісних показників нижча за 80% або якісні оцінки не підтверджені у примітках/аудиторському звіті (принцип обачності).

По-друге, діють «гейткипери» (gatekeepers) безпеки: за наявності критичних тригерів (покриття відсотків <1; Net Debt/EBITDA >5 чи від'ємна EBITDA; невиконані або крихкі ковенанти без узгодженого плану; суттєва перерва діяльності чи пошкодження активів без фінансового плану

відновлення) підприємство не може бути класифіковане вище «вразливої» категорії незалежно від рівня S.

По-третє, застосовується гістерезис: підвищення категорії фіксується лише після двох послідовних періодів перебування в новому діапазоні, тоді як пониження відбувається негайно; це запобігає випадковим «стрибкам» і стабілізує траєкторію оцінки.

Таким чином, шкала є практичним містком між публічними даними звітності та рішеннями менеджменту/ради директорів, дозволяючи швидко і послідовно класифікувати рівень економічної безпеки підприємства.

Порогові діапазони узгоджені з практикою кредитного аналізу та ризик-менеджменту, але водночас залишаються достатньо простими для застосування в Excel/BI без додаткових внутрішніх KPI: усі розрахунки виконуються в електронних таблицях або BI-панелях шляхом підстановки значень із Форм 1–3 та позначення якісних ознак за текстом приміток і аудиторського звіту.

Отже, запропонована методика поєднує простоту й аналітичну строгість: вона мінімізує вимоги до даних, використовує лише публічно верифіковані джерела, надає «анти-black-box» правила агрегації та інтерпретації і водночас забезпечує пряму керованість – кожній категорії відповідає набір типових управлінських дій (підтримка практик, цільові поліпшення, програма відновлення, антикризова програма). Завдяки цьому індекс S слугує надійним «містком» між фінансовою звітністю та практичними рішеннями менеджменту й наглядових рад, дозволяючи швидко і послідовно оцінювати економічну безпеку підприємств у динаміці.

Для апробації запропонованої методики оцінювання економічної безпеки була сформована вибірка з 10 промислових підприємств як цілеспрямована (purposive) панель, що поєднує репрезентативність галузей реального сектору, системну значущість для національної економіки та

повноту публічних розкриттів. До складу панелі увійшли (Додатки Д.3-Д.4): АТ «Укрзалізниця», ПрАТ «НЕК “Укренерго”», АТ «Укргідроенерго», АТ «Укрнафта», ПАТ «Центренерго», ПАТ «Сумихімпром», АТ «Дніпроазот», ПрАТ «Полтавський ГЗК» (Ferrexpo), ПАТ «АрселорМіттал Кривий Ріг» та АТ «Запоріжсталь». Така конфігурація забезпечує одночасно широту варіації ризик-профілів і достатню однорідність джерел даних, що є критично важливим для коректної валідації індексу S, побудованого виключно на відкритій фінансовій звітності та її примітках.

Дана вибірка віддзеркалює ключові виробничо-інфраструктурні контури економіки. Група мережевих інфраструктур – АТ «Укрзалізниця», ПрАТ «НЕК “Укренерго”» та АТ «Укргідроенерго» – дозволяє протестувати методику в середовищі регульованих тарифів, високої капіталомісткості та екстремальних техногенних і воєнних ризиків. Енергогенерація та видобуток/переробка – АТ «Укрнафта» і ПАТ «Центренерго» – унаочнюють, як індекс реагує на циклічність цінових шоків, структуру боргу та ковенантні обмеження. Хімічний кластер – ПАТ «Сумихімпром» і АТ «Дніпроазот» – репрезентує високу енергоємність, залежність від газового фактора та чутливість до логістики. Нарешті, гірничо-металургійний блок – ПрАТ «Полтавський ГЗК» (Ferrexpo), ПАТ «АрселорМіттал Кривий Ріг» і АТ «Запоріжсталь» – забезпечує випробування моделі в експортноорієнтованих ланцюгах з істотною волатильністю попиту, транспортними обмеженнями та значним впливом імпейрментів на звітність.

Обрані підприємства формують збалансований, методологічно виправданий набір випадків для апробації індексу S: він одночасно забезпечує різноманіття ризик-профілів, повноту й аудиторську якість даних, релевантний часовий розріз і можливість узагальнення висновків для промислових секторів із різною регуляторною та ринковою природою.

Такий дизайн вибірки дозволяє переконливо перевірити як внутрішню логіку моделі, так і її прикладну корисність для управлінських рішень (табл. 2.5).

Таблиця 2.5

Результати оцінювання економічної безпеки підприємств (2020–2024)

Підприємство	2020	2021	2022	2023	2024
АТ «Укрзалізниця»	Вразлива (0,60)	Задовільна (0,72)	Критична (0,40)	Задовільна (0,73)	Вразлива (0,58)
ПрАТ «НЕК “Укренерго”»	Критична (0,35)	Задовільна (0,70)	Критична (0,40)	Задовільна (0,67)	Критична (0,30)
АТ «Укргідроенерго»	Висока (0,82)	Висока (0,85)	Задовільна (0,72)	Вразлива (0,62)	Вразлива (0,55)
АТ «Укрнафта»	Вразлива (0,58)	Вразлива (0,60)	Вразлива (0,59)	Висока (0,88)	Задовільна (0,75)
ПАТ «Центренерго»	Вразлива (0,55)	Вразлива (0,55)	Критична (0,30)	Вразлива (0,50)	Критична (0,28)
ПАТ «Сумихімпром»	Вразлива (0,56)	Вразлива (0,60)	Критична (0,35)	Критична (0,32)	Критична (0,38)
АТ «Дніпроазот»	Задовільна (0,70)	Задовільна (0,72)	Критична (0,30)	Вразлива (0,56)	Вразлива (0,55)
ПрАТ «Полтавський ГЗК» (Ferrexpo)	Висока (0,82)	Висока (0,85)	Вразлива (0,58)	Вразлива (0,55)	Задовільна (0,70)
ПАТ «АрселорМіттал Кривий Ріг»	Задовільна (0,70)	Задовільна (0,75)	Критична (0,30)	Вразлива (0,55)	Вразлива (0,58)
АТ «Запоріжсталь»	Задовільна (0,72)	Задовільна (0,75)	Критична (0,35)	Вразлива (0,58)	Задовільна (0,76)

Джерело: розраховано автором

АТ «Укрзалізниця». Траєкторія показників відображає високий ступінь залежності від тарифного контуру та воєнно-логістичних шоків. Після глибокого збитку 2020 р. і короткого відновлення у 2021 р. компанія зазнала кризового просідання у 2022 р. через пріоритет соціально важливих, але низькомаржинальних перевезень, руйнування інфраструктури й перерозподіл вантажної номенклатури. Прибуток 2023 р. (≈5,04 млрд грн) засвідчив ефект від регуляторних рішень і підвищення операційної дисципліни, однак збиток 2024 р. (≈–2,71 млрд грн) показав обмеженість «короткого циклу» відновлення за відсутності стабільного компенсаторного механізму й достатнього фінансування модернізації. З позицій ЕБ підприємство коливається між «вразливою» та «задовільною» зонами; підвищення стійкості вимагатиме risk-based тарифної моделі, таргетованого

капітального ремонту вузлів високого ризику, диверсифікації вантажопотоку й формування буфера ліквідності під інфраструктурні ризики.

ПрАТ «НЕК "Укренерго"». Профіль ЕБ детермінований регуляторикою, тарифним дефіцитом і масштабом пошкоджень мереж. Після збиткового 2020 р. і символічного прибутку 2021 р. підприємство у 2022 р. зіткнулося з безпрецедентними аварійно-відновлювальними витратами та операційними ризиками системного оператора. Попри прибуток 2023 р. (≈0,4 млрд грн), 2024 р. завершився великим збитком (публічно згадуваний порядок – десятки млрд грн), що відображає одночасно інвестиційні потреби реконструкції, навантаження від фінансування «зелених» зобов'язань і затримки компенсаторів. Сукупність чинників утримує рівень ЕБ у «критичній» зоні; для переходу щонайменше до «вразливої» потрібні: гарантовані джерела відновлення мереж (у т.ч. міжнародні програми), предиктивне тарифоутворення, інструменти страхування/гарантування та пріоритизація вузлів з найбільшим системним ефектом.

АТ «Укргідроенерго». До 2021 р. компанія демонструвала параметри «високої» ЕБ, однак у 2022–2024 рр. профіль суттєво змінився через втрати генеруючих потужностей, гідрологічні обмеження та юридичні спори, пов'язані з руйнуванням об'єктів (зокрема Каховської ГЕС). Навіть за позитивних фінрезультатів окремих років підвищений рівень операційного та відновлювального ризику знижує інтегральну оцінку до «вразливої» зони. Ключем до нормалізації стануть довгострокова програма реконструкції з гарантованим фінансуванням, поступове відновлення активів і посилення HSE/ESG-контурів як передумова залучення дешевшого капіталу.

АТ «Укрнафта». Період 2020–2022 рр. характеризувався волатильністю і «вразливим» профілем, однак у 2023 р. підприємство

зафіксувало рекордний прибуток (≈24–24,7 млрд грн), а у 2024 р. – утримало міцний результат (≈16,38 млрд грн, ауд.) попри складне середовище. Це свідчить про покращення операційної та комерційної дисципліни, оптимізацію витрат і сприятливішу ринкову кон'юнктуру. Водночас ризик-профіль зумовлений податково-фіскальними параметрами, доступністю логістики та безпекою активів. Підтримання «задовільної/високої» ЕБ потребує наперед контрактованих каналів збуту, програм зниження собівартості на зрілих родовищах, проєктів підвищення нафтовіддачі та хеджування цінових ризиків.

ПАТ «Центренерго». Компанія входить у 2022–2024 рр. із ослабленою фінансовою позицією та деградацією генеруючої бази: втрата Вуглегірської ТЕС у 2022 р. і знищення Трипільської ТЕС у 2024 р. радикально обмежили виробничий потенціал. Хронічні збитки, високе боргове навантаження та судові ризики (зокрема взаємини з постачальниками енергоносіїв) підтримують «критичний» статус ЕБ. Вихід з кризи можливий лише через комплексну програму: репауеринг (у т.ч. з урахуванням паливної диверсифікації), реструктуризацію зобов'язань, державні компенсатори втрат критичної інфраструктури і перегляд ринкової моделі, що реалістично відображає витрати ТЕС.

ПАТ «Сумихімпром». Після короткого покращення у 2021 р. підприємство знову увійшло в зону збитковості (2022–2024), фіксуючи у 2024 р. від'ємний фінрезультат (порядку –0,6 млрд грн). Сукупність чинників – енергоємність виробництва, логістичні обмеження, нестабільний попит на ключові продукти та потреба в модернізації – формує «критичний» профіль ЕБ. Рекомендована траєкторія оздоровлення: компактна «програма відновлення» з акцентом на енергоефективність, перегляд продуктової матриці на користь вищої маржинальності, тактичні збутові альянси й, за потреби, боргова реструктуризація.

АТ «Дніпроазот». Після стабільно прибуткових 2020–2021 рр.

підприємство у 2022 р. зазнало шоку через цінову динаміку газу та вимушені зупинки, що перевело його у «критичну» зону. У 2023 р. розпочалося поступове відновлення виробничих циклів, але 2024 р. завершився чистим збитком (≈–1,33 млрд грн), що утримує «вразливий» статус. Ключові вектори підсилення ЕБ: контрактування газу з елементами хеджування, підвищення енергоефективності агрегатів, розширення каналів збуту, формування буфера ліквідності для згладжування цінових/сезонних коливань.

ПрАТ «Полтавський ГЗК» (Ferrexpo). У 2020–2021 рр. компанія мала «високий» профіль ЕБ на тлі сприятливої цінової кон'юнктури та стабільної логістики. 2022–2023 рр. принесли суттєві обмеження експорту, підвищення витрат і юридичні резерви, що погіршило інтегральну оцінку до «вразливої». У 2024 р. відновлення морського коридору спричинило різке нарощення виробництва (порядку +66% р/р) і поліпшення до «задовільної» зони. Для закріплення динаміки необхідні контрактні гарантії логістичних «вікон», дисципліна капітальних витрат і робота з клієнтським портфелем ЄС на умовах довших серій і стабільніших маржин.

ПАТ «АрселорМіттал Кривий Ріг». Після позитивної динаміки 2021 р. компанія у 2022 р. зафіксувала глибокі збитки (≈–48,3 млрд грн) на тлі зупинок, імпейрментів і логістичних втрат, що перевело ЕБ у «критичну» зону. У 2023 р. збиток суттєво скоротився (≈–11,8 млрд грн), а у 2024 р. виробництво сталі зросло до ≈1,65 млн т (≈+70% р/р), хоча підсумок року залишився від'ємним (≈–8,85 млрд грн). Підприємство закріпилося у «вразливій» зоні з виразним потенціалом поліпшення за умов стабілізації енергопостачання, нарощення завантаження доменного/аглодоменного комплексу та стійкого доступу до експортних маршрутів.

АТ «Запоріжсталь» (група «Метінвест»). Підприємство пройшло шлях від «критичної» зони у 2022 р. до «вразливої» у 2023 р., а у 2024 р. продемонструвало двозначні темпи приросту випуску (зокрема прокату) та

повернулося до прибутковості (орієнтир – ≈10,7 млрд грн). Така динаміка відповідає «задовільній» ЕБ із помітною чутливістю до логістики та енергостійкості. Для переходу до «високої» зони доцільні інвестиції у вузькі місця ланцюга гарячого прокату, довші логістичні контракти з гарантованими слотами та подальша диверсифікація ринків збуту.

Сукупна картина підтверджує «зубчастість» ЕБ у 2020–2024 рр., зумовлену поєднанням воєнних руйнувань, тарифно-регуляторних лагів, логістичних обмежень і коливань енергоносіїв. Інфраструктурні компанії («Укрзалізниця», «Укренерго», «Укргідроенерго») найбільш залежні від якості компенсаторних механізмів і темпів відновлення активів; експортно орієнтовані виробники («Полтавський ГЗК», «АрселорМіттал Кривий Ріг», «Запоріжсталь») – від стабільності коридорів і енергопостачання; хімічні підприємства («Дніпроазот», «Сумихімпром») – від цін на газ і модернізаційного циклу; «Укрнафта» – від фіскально-регуляторної стабільності та логістики. У межах спрощеної методики підвищення інтегрального індексу S забезпечуватиметься комбінацією: стабілізації тарифів/компенсацій, адресних капіталовкладень у «вузькі місця», контрактної фіксації логістики, програм енергоефективності та інструментів страхування/хеджування ключових ризиків.

Отже, запропонована методика забезпечує порівнянність у часі та між компаніями, зберігаючи при цьому простоту застосування і низьку вартість збору інформації.

2.2. Аналіз інструментів оцінювання лояльності персоналу та її впливу на економічну безпеку промислових підприємств

У постійно мінливому ландшафті глобальної економіки лояльність працівників постає як ключовий чинник сталого успіху та стабільності підприємств. Здатність компанії формувати й підтримувати лояльний персонал може суттєво впливати на її продуктивність, знижувати рівень плинності кадрів і посилювати конкурентні переваги на ринку. Цей взаємозв'язок між лояльністю працівників і корпоративним успіхом підкреслює нагальність для організацій розробляти ефективні стратегії оцінювання та підвищення лояльності персоналу.

Водночас оцінювання лояльності працівників ускладнене через динамічну природу робочої сили та численні чинники, що впливають на поведінку й установки співробітників. Традиційні методи, як-от опитування та інтерв'ю, попри їхню цінність, часто потребують доповнення більш витонченими технологічними рішеннями, аби зафіксувати тонку палітру ставлень і рівнів відданості персоналу. Відтак сучасні підприємства дедалі частіше звертаються до розвинених систем управління людськими ресурсами (HRM) та аналітичних платформ, щоб здобути глибші уявлення про лояльність своєї робочої сили. Це дослідження є критично важливим, оскільки не лише сприяє вдосконаленню наявних методик оцінювання, а й допомагає адаптуватися до нових норм робочого середовища, підвищувати ефективність управління персоналом і забезпечувати сталий розвиток організацій.

Оцінювання лояльності працівників є ключовим аспектом управління людськими ресурсами, оскільки високий рівень лояльності сприяє зростанню продуктивності, зниженню плинності кадрів і поліпшенню атмосфери в колективі. В огляді розглядаються основні джерела інформації та інструменти, що застосовуються для оцінювання лояльності працівників.

Одним із найпоширеніших методів збирання інформації про лояльність працівників є опитування та анкети. Дослідження свідчать, що опитування можуть надавати кількісні дані щодо рівня задоволеності та лояльності працівників (Smith & Macko, 2014). Опитування можуть бути структуровані за різними параметрами, такими як задоволеність роботою, стосунки з колегами та керівництвом, рівень залученості.

Іншим ефективним способом збирання інформації є проведення інтерв'ю та дискусій із працівниками. Інтерв'ю дозволяють глибше зрозуміти особисті мотиви та почуття співробітників, які не завжди можна зафіксувати за допомогою опитувань (Kirkman & Rosen, 1999). Цей метод також сприяє побудові довіри між працівниками та керівництвом.

Показники плинності кадрів є важливою мірою рівня лояльності працівників. Дослідження показують, що висока плинність часто свідчить про низький рівень задоволеності та лояльності (Hancock et al., 2013). Аналіз цих показників може допомогти виявити проблеми та вжити заходів для їх розв'язання.

Багато підприємств використовують спеціалізовані HRM-системи, такі як SAP SuccessFactors або Workday, для збирання та аналізу даних щодо лояльності працівників. Ці системи дають змогу автоматизувати процеси збирання даних, зменшити ризик помилок і підвищити ефективність аналізу (Stone & Deadrick, 2015).

Використання статистичного аналізу й аналітичних платформ, таких як SPSS або Tableau, дає змогу здійснювати детальний аналіз даних про лояльність працівників і виявляти закономірності та тренди (Hair et al., 2010). Ці інструменти допомагають ухвалювати обґрунтовані управлінські рішення.

Контент-аналіз відгуків, отриманих від працівників через внутрішні корпоративні канали або соціальні мережі, є ще одним важливим

інструментом. Цей метод допомагає виявляти ключові проблеми та занепокоєння працівників і оцінювати їхню лояльність (Krippendorff, 2018).

Встановлення взаємозв'язку між лояльністю працівників і економічною безпекою підприємств дало змогу запропонувати нові методи оцінювання персоналу та ідентифікувати загрози (Mihus, I., 2011; Mihus, I., & Chernenko, S., 2013).

Дослідження проведено шляхом опитування працівників HR-підрозділів українських підприємств за допомогою Google Forms у лютому–березні 2024 року. Загалом участь узяли 525 осіб, серед них 56.8% жінки (298 осіб) і 43.2% чоловіки (227 осіб). Вікова структура респондентів подана на рис. 2.1.

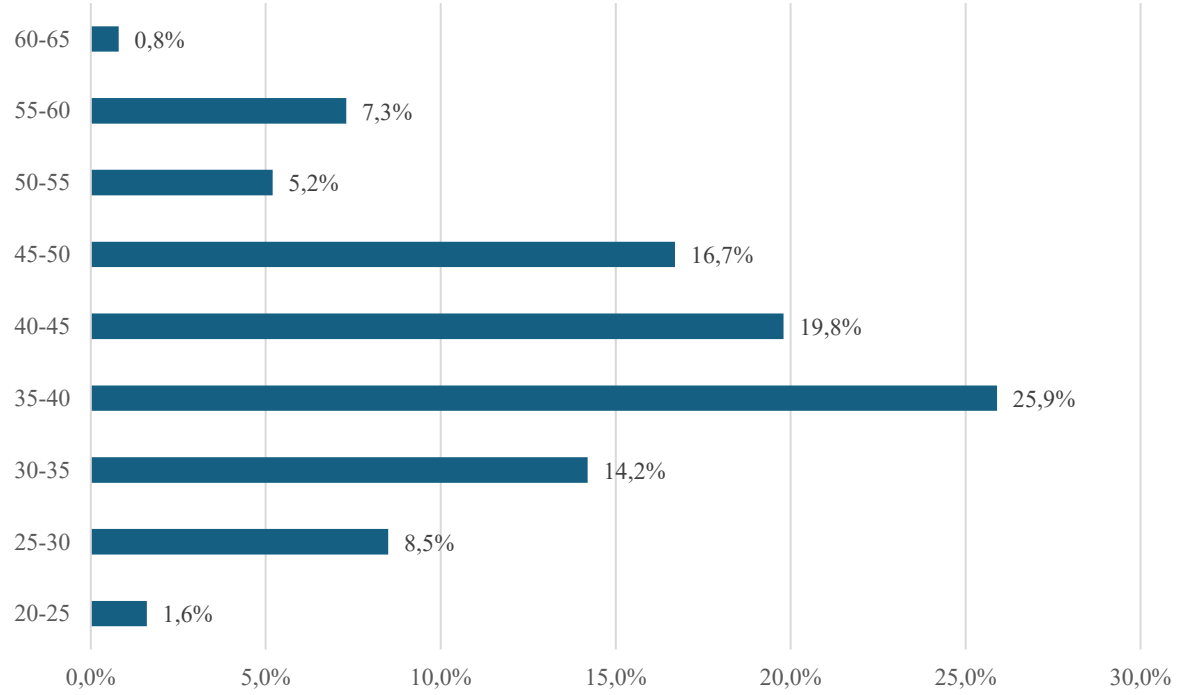

Рис. 2.1. Вікова структура опитаних працівників HR-підрозділів українських підприємств

Джерело: розроблено автором

Вибірка має виразне «ядро» у віці 35–50 років – 62,4% (35–40: 25,9%, 40–45: 19,8%, 45–50: 16,7%), що свідчить про переважання фахівців із

суттєвим професійним досвідом в управлінні та оцінюванні персоналу. Частка молодших до 30 років становить 10,1%, тоді як старших 55–65 років - 8,1% (плюс 50–55 років - 5,2%), тобто крайні вікові когорти представлені відносно нечисельно. Це підтверджує зрілість профілю респондентів і релевантність їхніх оцінок для тематики дослідження.

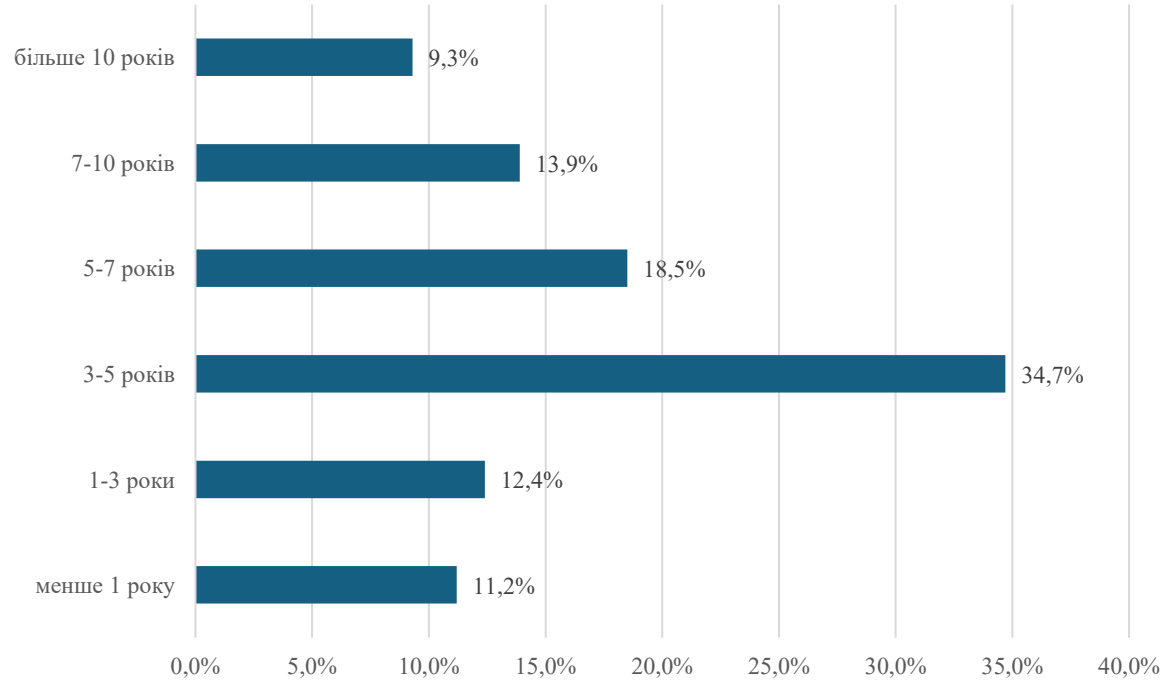

Рис. 2.2. Період роботи опитаних працівників HR-підрозділів українських підприємств на поточному місці роботи

Джерело: розроблено автором

Серед працівників HR-підрозділів, які взяли участь в опитуванні, близько 35% працюють на своєму останньому місці роботи 3–5 років, понад 18% – 5–7 років, і майже 14% – 7–10 років.

Переважна більшість працівників HR-підрозділів (Рис. 2.3), які взяли участь в опитуванні, працюють у IT-компаніях (37.3%) та виробничих компаніях (26.7%).

Під час опитування респондентам було поставлено 10 запитань, за допомогою яких ми прагнули визначити інструменти, що їх працівники HR-

підрозділів використовують для оцінювання лояльності персоналу українських підприємств.

Рис. 2.3. Сфери діяльності респондентів

Джерело: розроблено автором

Відповіді респондентів на запитання «Які основні джерела інформації ви використовуєте для оцінювання лояльності працівників на вашому підприємстві?» представлені на рис. 2.4.

Одержані відповіді вказують на те, що у більшості HR-підрозділів домінують формалізовані внутрішні джерела: опитування та анкетування - 96%, аналіз показників плинності кадрів - 95%, співбесіди та обговорення - 87%. Як додаткові канали використовують соціальні мережі та інші зовнішні джерела - 72% і зворотний зв’язок через внутрішні корпоративні канали - 67%. Отже, підприємства поєднують кількісні метрики та якісні інсайти, забезпечуючи триангуляцію даних для оцінювання лояльності персоналу.

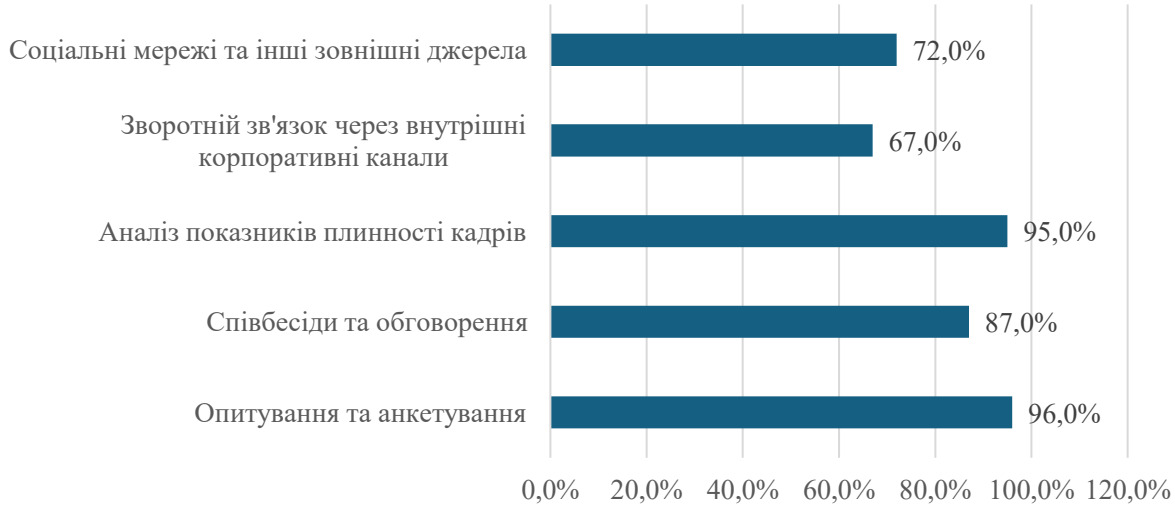

Рис. 2.4. Відповіді на запитання «Які основні джерела інформації ви використовуєте для оцінювання лояльності працівників на вашому підприємстві?»

Джерело: розроблено автором

Відповіді на запитання «Як часто ви проводите опитування або анкетування для оцінювання лояльності працівників?» представлені на рис. 2.5.

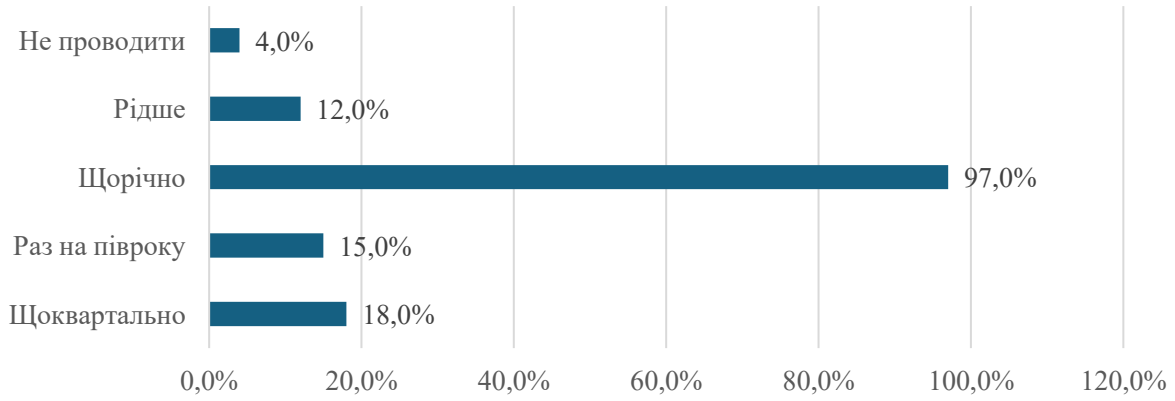

Рис. 2.5. Відповіді на запитання «Як часто ви проводите опитування або анкетування для оцінювання лояльності працівників?»

Джерело: розроблено автором

Оцінювання лояльності більшість HR-підрозділів проводять щорічно (97%); істотно менші частки практикують щоквартальні (18%) та піврічні (15%) хвилі, 12% роблять це рідше, а 4% не проводять опитувань. Домінування річної періодичності свідчить про низьку частоту зворотного зв'язку, що може обмежувати оперативність управлінських рішень; доцільно доповнювати річні опитування короткими «pulse»-зрізами..

Відповіді на запитання «Які інструменти або платформи ви використовуєте для збирання та аналізу даних щодо лояльності працівників?» представлено на рис. 2.6.

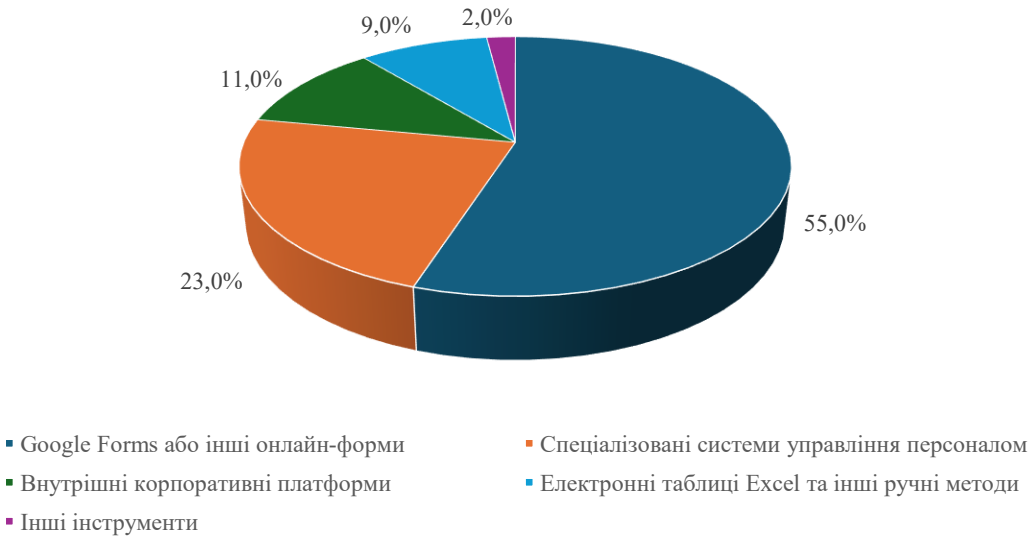

Рис. 2.6. Відповіді на запитання «Які інструменти або платформи ви використовуєте для збирання та аналізу даних щодо лояльності працівників?»

Джерело: розроблено автором

Як показало дослідження, екосистема збору й аналізу даних про лояльність має гібридний характер із домінуванням простих інструментів: Google Forms та інші онлайн-форми - 55%, спеціалізовані HRM-системи - 23%, внутрішні корпоративні платформи - 11%, Excel/ручні методи - 9%, інші - 2%. Отже, більшість підприємств покладаються на швидкі та

доступні рішення, що полегшує запуск опитувань, але обмежує інтеграцію, автоматизацію та глибину аналітики. Збільшення частки HRM і корпоративних платформ є ключовим резервом для підвищення якості даних, трасованості показників і оперативності управлінських рішень.

Відповіді на запитання «Як ви аналізуєте зібрані дані щодо лояльності працівників?» представлено на рис. 2.7.

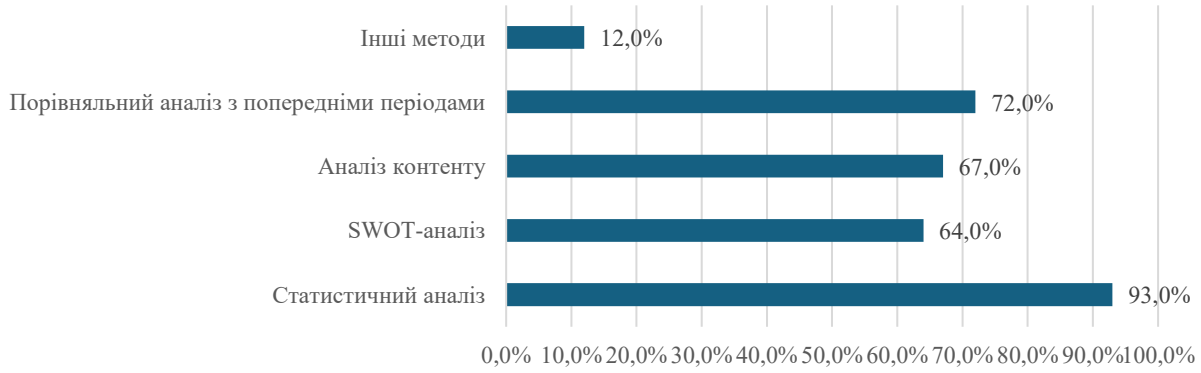

Рис. 2.7. Відповіді на запитання «Як ви аналізуєте зібрані дані щодо лояльності працівників?»

Джерело: розроблено автором

Аналіз даних про лояльність переважно спирається на кількісні підходи: статистичний аналіз - 93% і порівняльний аналіз із попередніми періодами - 72%. Водночас активно застосовують і якісні методи: контент-аналіз - 67%, SWOT-аналіз - 64%. Частка «інших методів» - 12%, що свідчить про обмежений, але наявний простір експериментування. Отже, підприємства використовують змішану методологію з домінуванням кількісної аналітики, доповненої якісними інсайтами для інтерпретації результатів.

Відповіді на запитання «Чи використовуєте ви будь-які автоматизовані системи або програмне забезпечення для аналізу даних щодо лояльності працівників?» представлено на рис. 2.8. Переважна більшість респондентів

- 79% - використовують автоматизовані системи або ПЗ для аналізу даних щодо лояльності, тоді як 21% - не використовують.

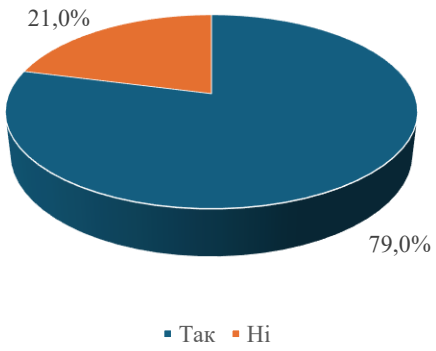

Рис. 2.8. Відповіді на запитання «Чи використовуєте ви будь-які автоматизовані системи або програмне забезпечення для аналізу даних щодо лояльності працівників?»

Джерело: розроблено автором

Це вказує на достатньо високий рівень цифровізації HR-аналітики, але й на наявний резерв для підвищення якості даних, автоматизації та відтворюваності оцінок у тих компаніях, які ще не застосовують такі інструменти.

Відповіді на запитання «Як часто ви отримуєте зворотний зв'язок від працівників щодо рівня їхньої задоволеності та лояльності?» представлено на рис. 2.9.

На жаль, система зворотного зв'язку на українських підприємствах має переважно епізодичний характер: лише 21% компаній отримують фідбек регулярно/постійно (14% і 7% відповідно), тоді як 46% - іноді (раз на рік), 22% - рідко, а 11% - ніколи. Така структура свідчить про недоінституціалізовану систему зворотного зв'язку, що подовжує цикл виявлення проблем і може занижувати рівень лояльності; доцільно запровадити короткі «pulse»-опитування, канали фідбеку в реальному часі та SLA на опрацювання звернень.

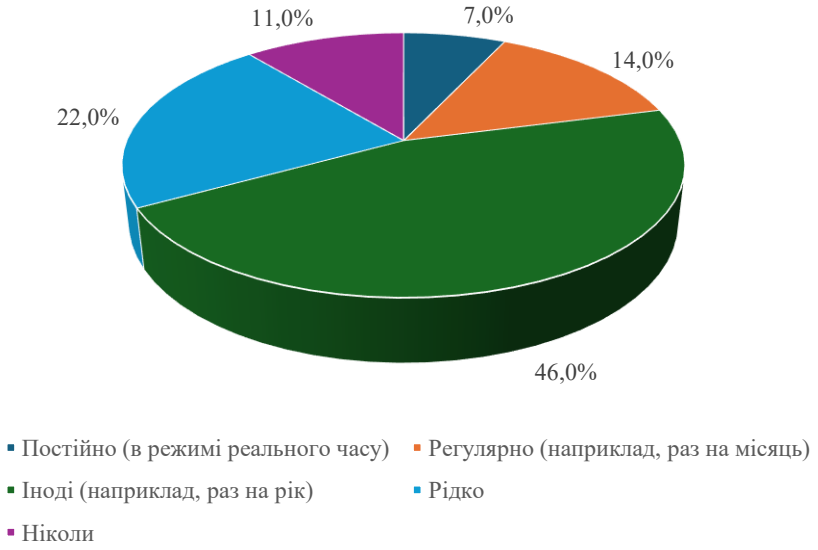

Рис. 2.9. Відповіді на запитання «Як часто ви отримуєте зворотний зв'язок від працівників щодо рівня їхньої задоволеності та лояльності?»

Джерело: розроблено автором

Відповіді на запитання «Які ключові показники ефективності (KPI) ви використовуєте для оцінювання лояльності працівників?» представлено на рис. 2.10.

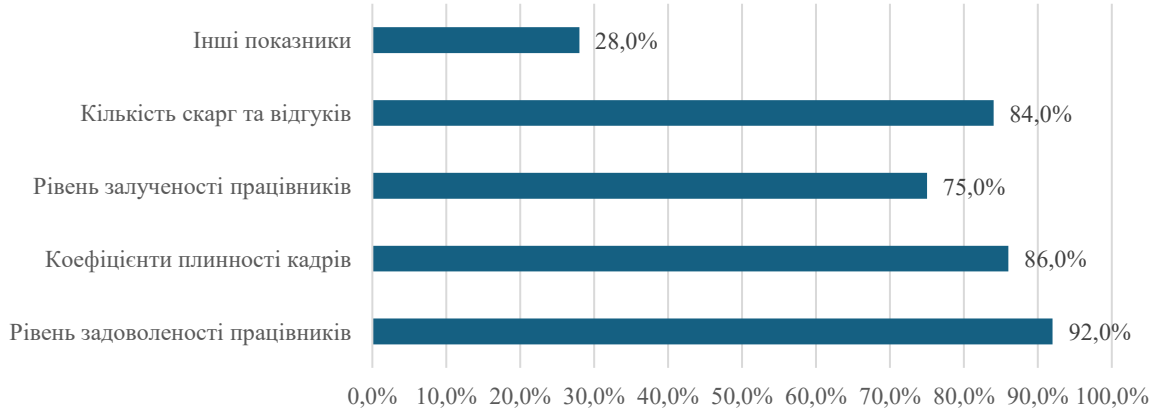

Рис. 2.10. Відповіді на запитання «Які ключові показники ефективності (KPI) ви використовуєте для оцінювання лояльності працівників?»

Джерело: розроблено автором

У наборі KPI для оцінювання лояльності домінують класичні метрики: рівень задоволеності (92%) і плинність кадрів (86%), доповнені операційним індикатором – кількістю скарг/відгуків (84%). Рівень залученості застосовують 75%, що свідчить про поступовий зсув до проактивної діагностики, тоді як інші специфічні показники використовують лише 28%.

Отже, існує резерв для розширення дашбордів за рахунок поєднання «ведучих» (leading) і «запізнілих» (lagging) індикаторів, що підвищить чутливість системи оцінювання та своєчасність управлінських рішень.

Відповіді на запитання «Чи аналізуєте ви дані щодо лояльності працівників у розрізі різних підрозділів або груп?» представлено на рис. 2.11.

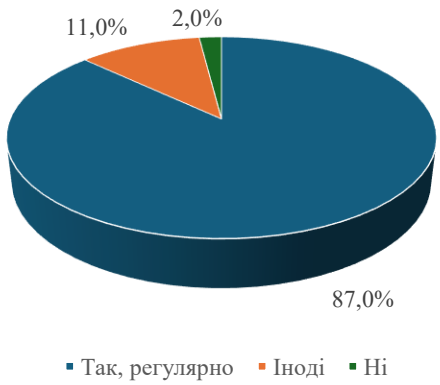

Рис. 2.11. Відповіді на запитання «Чи аналізуєте ви дані щодо лояльності працівників у розрізі різних підрозділів або груп?»

Джерело: розроблено автором

Переважна більшість компаній регулярно аналізують лояльність у розрізі підрозділів (87%), 11% роблять це іноді, і лише 2% – не проводять такого аналізу. Це свідчить про інституціоналізацію сегментного підходу, що підвищує точність діагностики та дозволяє таргетувати HR-інтервенції; мінорний сегмент потребує методичного й технічного підсилення.

Відповіді на запитання «Чи плануєте ви впроваджувати нові інструменти або методи для оцінювання лояльності працівників у найближчому майбутньому?» представлено на рис. 2.12.

Рис. 2.12. Відповіді на запитання «Чи плануєте ви впроваджувати нові інструменти або методи для оцінювання лояльності працівників у найближчому майбутньому?»

Джерело: розроблено автором

Переважна частка компаній ще не визначилася з упровадженням нових інструментів оцінювання лояльності (61%), 32% уже планують зміни, і лише 7% - не планують. Це вказує на значний потенціал модернізації та потребу в додаткових обґрунтуваннях (ROI, пілоти, методична підтримка) для прискорення впровадження.

Відповіді на запитання «Пропозиції щодо підвищення ефективності чинних методів оцінювання лояльності працівників на вашому підприємстві» представлено на рис. 2.13.

Найвищі пріоритети респонденти відводять анонімності та конфіденційності (96%) і «замиканню циклу» - зворотному зв’язку та діям за результатами (92%), а також інтеграції результатів оцінювання у стратегії та HR-процеси (91%). Далі - розвиток менеджерів (85%) і багатоканальний

збір даних (84%), що разом із автоматизацією (72%) та регулярністю оцінювань (67%) формує операційну спроможність системи.

Рис. 2.13. Відповіді на запитання «Пропозиції щодо підвищення ефективності чинних методів оцінювання лояльності працівників на вашому підприємстві»

Джерело: розроблено автором

Порівняно нижче оцінено розширення набору показників (58%) і залучення зовнішніх консультантів (34%), що свідчить: першочергово підприємства прагнуть підвищити довіру, вбудувати оцінювання в управлінський цикл і наростити внутрішні компетенції, а вже потім – розширювати метрики чи залучати зовнішню експертизу.

У контексті сучасних викликів для промисловості лояльність персоналу виступає ключовим чинником економічної безпеки підприємства, оскільки безпосередньо впливає на стабільність операцій, якість виробництва, частоту інцидентів, рівень плинності кадрів і, зрештою, на витрати та результативність. Узагальнені емпіричні матеріали свідчать, що домінуючими інструментами вимірювання лояльності є стандартизовані опитування та анкети (переважна більшість підприємств), аналіз показників

плинності кадрів та відсутностей, інтерв'ю і фокус-групи; водночас зростає роль контент-аналізу внутрішніх каналів зворотного зв'язку та аналітичних панелей. Переважає щорічний цикл оцінювання, однак саме поєднання річних хвиль із короткими регулярними опитуваннями, додержання принципів анонімності та конфіденційності, «замикання циклу» результатів у конкретні управлінські дії й поступова інтеграція даних у корпоративні інформаційно-аналітичні рішення є передумовою перетворення виміряної лояльності на керований внесок у економічну безпеку.

Акціонерне товариство «Укрзалізниця». Масштаб організації, різнорідність професій і розгалужена географія обумовлюють доцільність змішаного підходу: стандартизовані опитування для базової діагностики, короткі регулярні опитування для оперативного виявлення проблем у змінах, інтерв'ю «залишайся з нами» для критичних ролей (машиністи, ремонтні бригади, чергові станцій), а також систематичний аналіз плинності, незакритих змін і понаднормових робіт. Контент-аналіз звернень у внутрішніх каналах дає змогу локалізувати «вузькі місця» сервісу. Інтеграція цих даних у аналітичні панелі дозволяє співвідносити лояльність із частотою інцидентів з охорони праці, простоями та витратами на переробки, що безпосередньо зміцнює економічну безпеку через стабілізацію графіків і зниження непродуктивних витрат.

Приватне акціонерне товариство «Національна енергетична компанія "Укренерго"». Визначальними є ризики втоми та вигорання оперативно-диспетчерського персоналу і дисципліна безпечної роботи у виробничих автоматизованих системах керування і збору даних. Доцільно поєднати короткі регулярні опитування із запитаннями про навантаження, якість змін і психологічний стан, інтерв'ю у вузлах із найвищою складністю режимів, а також аналіз понаднормових, помилок у журналах і подій «майже інцидент». Таке зв'язування «м'яких» показників із фактичними операційними відхиленнями формує ранні сигнали зон ризику, знижує

імовірність відмов і сприяє підвищенню інтегральних показників економічної безпеки.

Акціонерне товариство «Укргідроенерго». З огляду на змінний режим роботи гідроелектростанцій ефективними є короткі опитування після зміни, інтерв'ю з майстрами та наглядачами, аналіз дотримання процедур безпеки і фіксації подій «майже інцидент». Важливо інституціалізувати наставництво і передачу знань від вузькопрофільних експертів, поєднавши це з програмами психологічної підтримки. Така конфігурація зменшує вплив людського чинника на аварійність і простої та, відповідно, підвищує стійкість операцій і економічну безпеку.

Акціонерне товариство «Укрнафта». Доцільною є сегментація вимірювання за ланцюгом «видобуток – переробка – роздріб»: опитування та короткі регулярні опитування – для кожного сегмента з урахуванням специфіки умов праці; інтерв'ю «залишайся з нами» – для дефіцитних професій; контент-аналіз звернень щодо порушень безпеки та неякісних практик у постачанні та збуті. Поєднання результатів із показниками виробничої травматизації, відмов обладнання, втрат і скарг дає змогу кількісно оцінити внесок лояльності у собівартість, маржинальність та санкційні ризики, підвищуючи керованість економічної безпеки.

Публічне акціонерне товариство «Центренерго». З огляду на зношеність обладнання і ризик втрати компетенцій, інструменти оцінювання лояльності слід пов'язати з «картами компетенцій» і планами розвитку персоналу. Регулярні короткі опитування у змінному персоналі, структуровані інтерв'ю з носіями критичних навичок і аналіз плинності у ключових ролях дають ранні попередження щодо загрози простоїв і затримок ремонтів. Аналітичні панелі з показниками «дефіцитних змін» і «вузьких місць» допомагають пріоритезувати навчання та наставництво, що зменшує тривалість ремонтів і підвищує коефіцієнт готовності, безпосередньо посилюючи економічну безпеку.

Публічне акціонерне товариство «Сумихімпром». У процесній хімії безпека і знання є вирішальними. Опитування та короткі регулярні опитування варто з'єднати з контент-аналізом журналів відхилень, реєстрів «майже інцидентів» і звернень до служб безпеки. Інтерв'ю з носіями унікальних знань і системне документування технологічних практик знижують ризик втрати «пам'яті процесу». Інтеграція цих потоків даних у аналітичні панелі конвертує лояльність у меншу аварійність, менші штрафи та нижчі витрати браку, що збільшує підсумковий рівень економічної безпеки.

Акціонерне товариство «Дніпроазот». Доцільно поєднати вимірювання лояльності з оцінкою «клімату безпеки»: стандартизовані анкети культури безпеки, короткі опитування після критичних змін, інтерв'ю з операторами небезпечних дільниць, контент-аналіз подій із викидами та зупинками. Перехід від епізодичних вимірювань до регулярних коротких зрізів скорочує час виявлення причин ризику, зменшує частоту і тяжкість інцидентів та, відповідно, регуляторні й страхові витрати, підвищуючи стійкість і економічну безпеку.

Приватне акціонерне товариство «Полтавський гірничо-збагачувальний комбінат» (Ferrexpo). Для керування ризиками у великих відкритих кар'єрах доцільні короткі опитування щодо втоми та умов праці, інтерв'ю з бригадирами, а також контент-аналіз повідомлень про події «майже інцидент» і зупинки конвеєрних ліній. Зіставлення показників лояльності з тривалістю простоїв, частотою браку та витратами на ремонт створює «петлю зворотного зв'язку» між людським чинником і виробничою ефективністю, що швидко транслюється у нижчу собівартість і стабільніші відвантаження, підсилюючи економічну безпеку.

Публічне акціонерне товариство «АрселорМіттал Кривий Ріг». Вимірювання лояльності у гарячих переділах має бути поєднане з даними про інциденти, переробки і своєчасність планових ремонтів. Інтерв'ю з

майстрами та профільними фахівцями допомагають ідентифікувати нематеріальні причини низької залученості, тоді як контент-аналіз звернень і скарг забезпечує якісне підґрунтя для змін у режимах роботи та організації праці. Такий підхід покращує дисципліну безпеки й якість, що напряму підвищує показники економічної безпеки.

Акціонерне товариство «Запоріжсталь». Пріоритетним є регулярне коротке опитування у гарячих цехах, інтерв'ю щодо умов і режимів праці, аналіз плинності і відсутностей у ключових ремонтних бригадах та систематичний облік подій «майже інцидент». Персоніфіковані плани розвитку і «карти компетенцій» мінімізують ризик «вузьких місць» у ремонтах. Інтеграція вимірів лояльності з показниками простоїв і якості продукції забезпечує швидке управлінське реагування та зростання операційної маржі, що підсилює інтегральний рівень економічної безпеки.

Таблиця 2.6

Використання інструментів оцінювання лояльності та їх впливу на економічну безпеку підприємств

Підприємство	Готовність до впровадження	Пріоритетні інструменти	Ключові дані / зв'язки з KPI	Очікуваний ефект на ЕБ	Горизонт ефекту
АТ «Укрзалізниця»	Висока	Опитування + короткі «pulse», інтерв'ю «залишайся з нами»	Плинність, незакриті зміни, понаднормові → простої, інциденти	Стабілізація графіків, ↓витрати переробок	1–2 квартали
ПрАТ «НЕК "Укренерго"»	Середньо-висока	«Pulse» у диспетчерів, аналіз журналів, інтерв'ю у критичних вузлах	Понаднормові, помилки в журналах, «майже-інциденти» → надійність мережі	↓операційні відмови, ↑керованість режимів	1–2 квартали
АТ «Укргідроенерго»	Висока	«Pulse» після змін, інтерв'ю майстрів, аудит дотримання процедур	Події «майже-інцидент», дисципліна процедур → аварійність/простої	↓ризик інцидентів, ↑готовність станцій	1–2 квартали
АТ «Укрнафта»	Висока	Сегментовані опитування (видобуток/переробка/роздріб), «stay»-інтерв'ю	Травматизм, відмови обладнання, скарги → собівартість/маржа	↓штрафи і брак, ↑операційна маржа	1–2 квартали
ПАТ «Центренерго»	Середня	«Pulse» у змін, інтерв'ю носіїв критичних	Плинність у ключових ролях, дефіцит змін → тривалість ремонтів	↓простої, ↑коефіцієнт готовності	1–2 квартали

Підприємство	Готовність до впровадження	Пріоритетні інструменти	Ключові дані / зв'язки з KPI	Очікуваний ефект на ЕБ	Горизонт ефекту
		навичок, карти компетенцій			
ПАТ «Сумихімпром»	Середньо-висока	Опитування + контент-аналіз відхилень, інтерв'ю носіїв знань	Реєстр відхилень/«майже-інцидентів» → брак/штрафи	↓аварійність і брак, ↑стійкість процесів	1–2 квартали
АТ «Дніпроазот»	Висока	Анкети «клімату безпеки», «pulse» після критичних змін, інтерв'ю операторів	Події з небезпечними речовинами, зупинки → регуляторні витрати	↓частота/тяжкість інцидентів, ↓ризик санкцій	1–2 квартали
ПрАТ «Полтавський ГЗК» (Ferrexpo)	Висока	«Pulse» про втому/умови, інтерв'ю бригадирів, аналіз «майже-інцидентів»	Простої, брак, ремонти → собівартість/випуск	↓простої і брак, ↑стабільність відвантажень	1–2 квартали
ПАТ «АрселорМіттал Кривий Ріг»	Середньо-висока	Опитування в гарячих цехах, інтерв'ю майстрів, контент-аналіз скарг	Інциденти, переробки, своєчасність ремонтів → якість/витрати	↑якість і безпека, ↓переробки	1–2 квартали
АТ «Запоріжсталь»	Висока	Регулярні «pulse» у гарячих цехах, інтерв'ю, карти компетенцій	Плинність/відсутності в ремонтних бригадах, «майже-інциденти» → простої	↓час простоїв, ↑операційна маржа	1–2 квартали

Джерело: розроблено автором

Отже, усі розглянуті підприємства мають реалістичні передумови для результативного впровадження інструментів оцінювання лояльності персоналу та перетворення отриманих даних на керовані дії з підвищення економічної безпеки. Найбільш ефективною є послідовність «від простого до складного»: поєднання щорічних вимірів із короткими регулярними опитуваннями, обов'язкове дотримання анонімності та конфіденційності, інтерв'ю для критичних професій, контент-аналіз внутрішнього зворотного зв'язку, а головне – системне зіставлення показників лояльності з операційними та фінансовими результатами (плинність, простої, брак, інциденти, скарги). У середньостроковому періоді доцільною є міграція від розрізнених інструментів до інтегрованих корпоративних інформаційно-аналітичних платформ, які забезпечують відтворюваність, швидкість і

трасованість управлінських рішень. В інфраструктурних компаніях очікуваний ефект проявляється поступово через технологічну та тарифну інерційність, натомість у переробних і видобувних – швидше і яскравіше через прямий зв'язок із собівартістю, якістю та стабільністю виробництва. Сукупний результат полягає у зниженні частоти та вартості інцидентів, стабілізації змін і скороченні витрат, що в підсумку зміцнює економічну безпеку підприємств.

За результатами опитування були узагальнені основні методи оцінювання лояльності працівників, які використовуються на досліджуваних промислових підприємствах (табл. 2.7).

Запропоновані заходи з удосконалення оцінювання лояльності персоналу здатні підвищити результативність чинних методів, поліпшити виробниче середовище та зміцнити довіру працівників до роботодавця. Проведене дослідження інформаційно-аналітичного забезпечення засвідчило динамічний зв'язок між практиками управління персоналом і організаційними результатами: лояльність працівників виступає системоутворювальним чинником продуктивності, зниження плинності кадрів і посилення конкурентоздатності.

Оцінювальний інструментарій охоплює як традиційні опитування й інтерв'ю, так і розвинені системи управління людськими ресурсами та аналітичні платформи. Кожен метод має власні сильні сторони і обмеження: опитування й інтерв'ю забезпечують безпосередній доступ до установок і мотивацій, але можуть бути чутливими до упереджень респондентів; автоматизовані системи та статистичні підходи підвищують об'єктивність і відтворюваність, проте інколи втрачають контекстуальну нюансованість, яку надають якісні методи. Тому оптимальним є комбінований підхід, що поєднує кількісні та якісні джерела даних у єдиній аналітичній рамці.

Таблиця 2.7

Методи оцінювання лояльності працівників, які використовуються на досліджуваних промислових підприємствах

Методи	Опис
Використання багатоканальних методів збору даних	Впровадження комплексного підходу до збору даних, включаючи опитування, інтерв'ю, групові дискусії та онлайн-опитування. Це дозволяє отримувати різноманітну інформацію та точніше оцінювати лояльність співробітників.
Автоматизація процесів збору та аналізу даних	Використання сучасних систем управління персоналом для автоматизації збору та аналізу даних щодо лояльності співробітників. Це зменшує ймовірність помилок та підвищує ефективність і швидкість обробки інформації.
Регулярні оцінювання	Впровадження регулярних оцінок лояльності, наприклад, щоквартально або раз на два роки. Це дозволяє відстежувати динаміку та оперативно реагувати на проблеми.
Анонімність та конфіденційність	Забезпечення повної анонімності та конфіденційності під час збору даних, підвищення довіри співробітників та заохочення до більш відкритого та чесного зворотного зв'язку.
Участь співробітників у процесі оцінювання	Створення робочих груп з представниками різних відділів для розробки опитувань та обговорення результатів. Це допомагає враховувати специфіку різних відділів та підвищує залученість співробітників.
Інтеграція результатів оцінювання у стратегії розвитку	Використання результатів оцінки лояльності для розробки та коригування стратегій розвитку підприємства, планів навчання та програм мотивації. Це демонструє співробітникам, що їхня думка враховується та цінується.
Розширення показників оцінювання	Включення якісних аспектів до оцінок, таких як задоволеність корпоративною культурою, стосунки з керівництвом та можливості професійного зростання.
Використання зовнішніх консультантів	Залучення зовнішніх консультантів для незалежних оцінок та аналізу лояльності. Це забезпечує об'єктивне уявлення про ситуацію та виявляє проблеми, які можуть бути пропущені внутрішніми спеціалістами.
Навчання та розвиток менеджерів	Проведення тренінгів та семінарів для менеджерів щодо важливості лояльності співробітників та методів оцінювання. Підвищення обізнаності керівництва про сучасні підходи до управління персоналом покращує робоче середовище.
Зворотній зв'язок та дії на основі результатів оцінювання	Надання співробітникам зворотного зв'язку щодо результатів оцінювання та інформування їх про заплановані заходи щодо покращення. Це показує, що думки співробітників не лише чуються, а й враховуються в подальших діях підприємства.

Джерело: розроблено автором

Ефективність вимірювання визначається не лише вибором інструментів, а й їх відповідністю культурному та організаційному

контексту. Підприємства мають адаптувати дизайн оцінювання до демографічних характеристик персоналу та специфічних драйверів лояльності, притаманних їхнім підрозділам і професійним групам. Сучасні цифрові рішення – зокрема системи класу SAP SuccessFactors чи Workday, а також методи машинного навчання – розширюють можливості глибинної аналітики і прогнозування поведінкових трендів, проте одночасно висувають підвищені вимоги до захисту персональних даних, етичного використання інформації та прозорості процедур.

З управлінської перспективи ключовим є інтегрування результатів вимірювання у цикл прийняття рішень: від формування програм утримання та розвитку персоналу до коригування організаційних процесів і систем мотивації. Комплексне використання інструментів дає змогу точніше ідентифікувати детермінанти лояльності, налаштовувати практики управління під конкретні потреби колективу та знижувати ризики, пов’язані з плинністю, простоєм і інцидентами. Водночас необхідними передумовами є постійне підвищення кваліфікації керівників у сфері сучасних HR-технологій та аналітики, а також запровадження чітких стандартів конфіденційності й підзвітності.

Отже, інформаційно-аналітичні системи та інструменти оцінювання лояльності, за умови їх методично виваженого застосування та етичного регулювання, формують інституційну основу для стійкого, продуктивного робочого середовища й довгострокової економічної безпеки підприємства. Така інтеграція даних, процесів і рішень підсилює керованість організації та створює передумови для її сталого розвитку.

2.3. Ідентифікація внутрішніх та зовнішніх загроз економічній безпеці промислових підприємств з боку персоналу

З початком війни в Україні 24 лютого 2022 року країна зазнала значних змін у всіх сферах життя, включаючи економіку, суспільство та бізнес. Конфлікт створив нові виклики для підприємств, які змушені були адаптуватися до нових умов, забезпечуючи безпеку своїх працівників, стабільність бізнес-процесів та підтримку економіки країни. Одним із ключових аспектів, що впливають на здатність компаній ефективно функціонувати в таких умовах, є лояльність персоналу до своїх роботодавців.

Лояльність працівників є важливим чинником стабільності та успіху підприємств. Вона впливає на продуктивність, мотивацію та здатність компанії утримувати кваліфікованих працівників. У воєнний час, коли стрес і невизначеність досягають високого рівня, підтримання високого рівня лояльності стає ще більш критичним завданням для керівництва підприємств.

У контексті безпрецедентних викликів, які постали перед українським бізнесом, важливо зрозуміти, як зберегти та підвищити лояльність працівників, забезпечуючи їм необхідну підтримку та створюючи сприятливі умови для роботи навіть у найскладніших обставинах.

Дослідження проводилося шляхом опитування працівників українських підприємств за допомогою гугл-форм у лютому-березні 2024 року. В опитуванні взяли участь 16250 осіб, з них 46,3% жінок (7524 осіб) і 53,7% (8726 осіб).

Вікова структура респондентів представлена на рис. 2.14 та має виразне ядро у групі 30–45 років (разом 58,9%): модальна когорта - 40–45 років (21,8%), далі 30–35 років (21,2%) і 35–40 років (15,9%). Помітну частку становлять і 25–30 років (18,4%), тоді як молодші 20–25 років - лише

4,6%. Старші вікові групи представлені скромніше (50–55 - 4,7%, 55–60 - 7,3%, 60–65 - 2,1%).

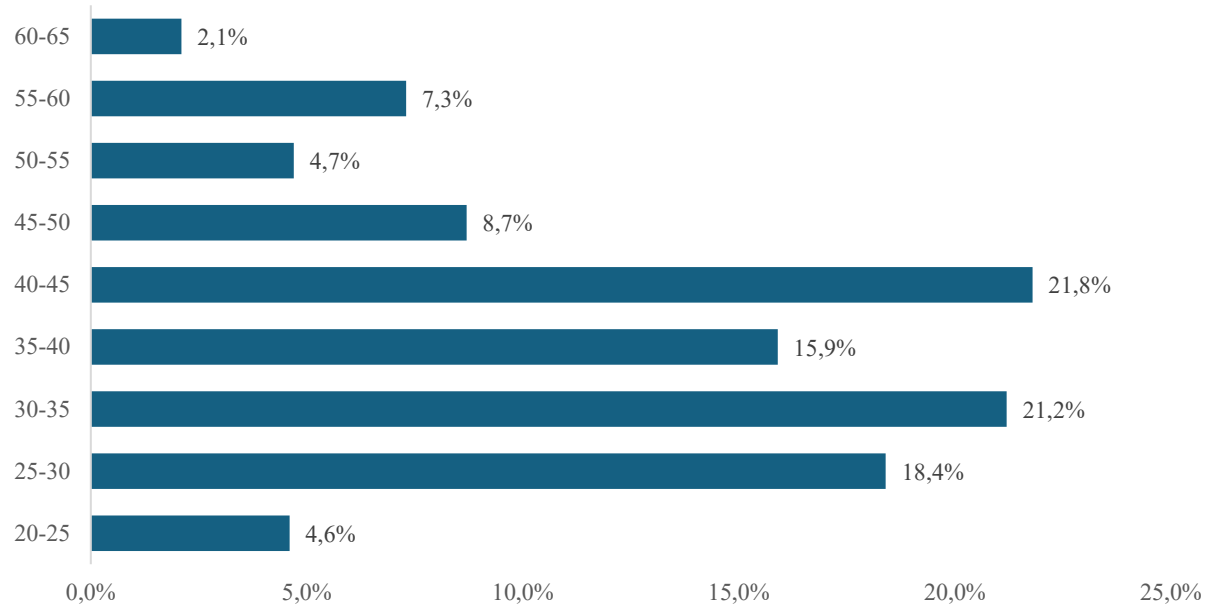

Рис. 2.14. Вікова структура опитаних працівників

Джерело: розроблено автором

Це свідчить, що вибірка переважно сформована з фахівців середнього кар'єрного стажу, що підвищує релевантність оцінок, пов'язаних із практиками зрілих колективів.

Рівень освіти опитаних працівників показав, про домінування вищої освіти: 42,8% мають рівень спеціаліста/магістра, 28,6% - бакалавра; ще 7,2% - науковий ступінь і 11,2% - незакінчену вищу. Сукупно це 89,8% осіб із (незакінченою чи завершеною) вищою освітою; частка із повною середньою та середньоспеціальною освітою становить 10,2% (рис. 2.15). Така освітня структура відображає високий рівень людського капіталу та водночас підвищує вимоги до сучасних HR-практик (розвиток, кар'єрні траєкторії, залучення), що є критично важливим для підтримання лояльності персоналу.

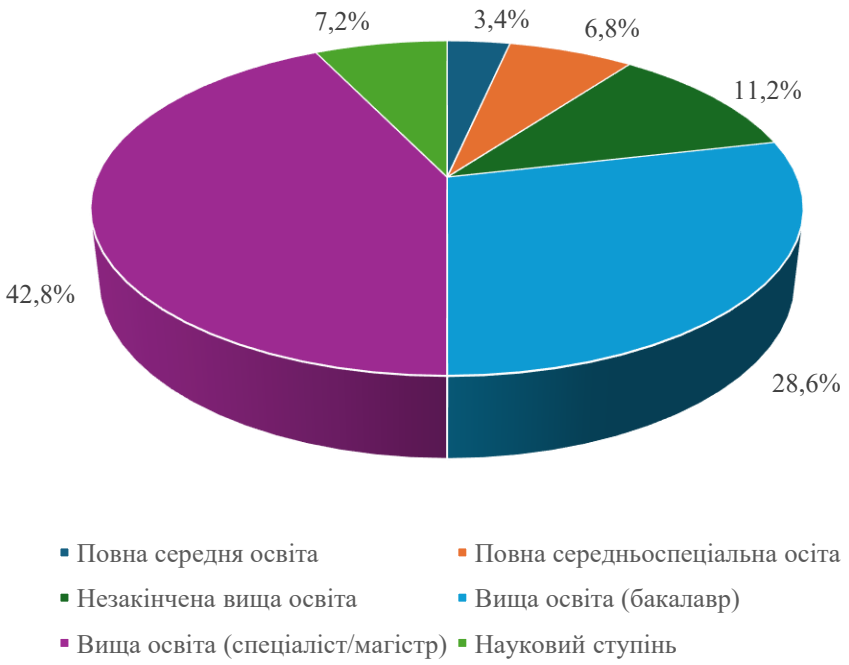

Рис. 2.15. Рівень освіти опитаних працівників

Джерело: розроблено автором

Водночас, роботодавці повинні враховувати сучасні виклики в управлінні персоналом задля підвищення лояльності персоналу.

Близько 35% респондентів працюють на поточному місці роботи понад 3-5 років, що свідчить про те, що вони змінили місце роботи напередодні пандемії COVID-19, разом з роботодавцем змогли подолати ті важкі часи та продовжили працювати під час війни (рис. 2.16). Це свідчить про підсвідому лояльність працівників до таких роботодавців та велику довіру до прийнятих ними рішень.

Достатньо висока частка працівників, які взяли участь у опитуванні, працює понад 7 років, але рівень лояльності значно менший та свідчить про те, що незважаючи на небажання працівників змінювати роботу під час війни, вони не завжди поділяють цінності роботодавців.

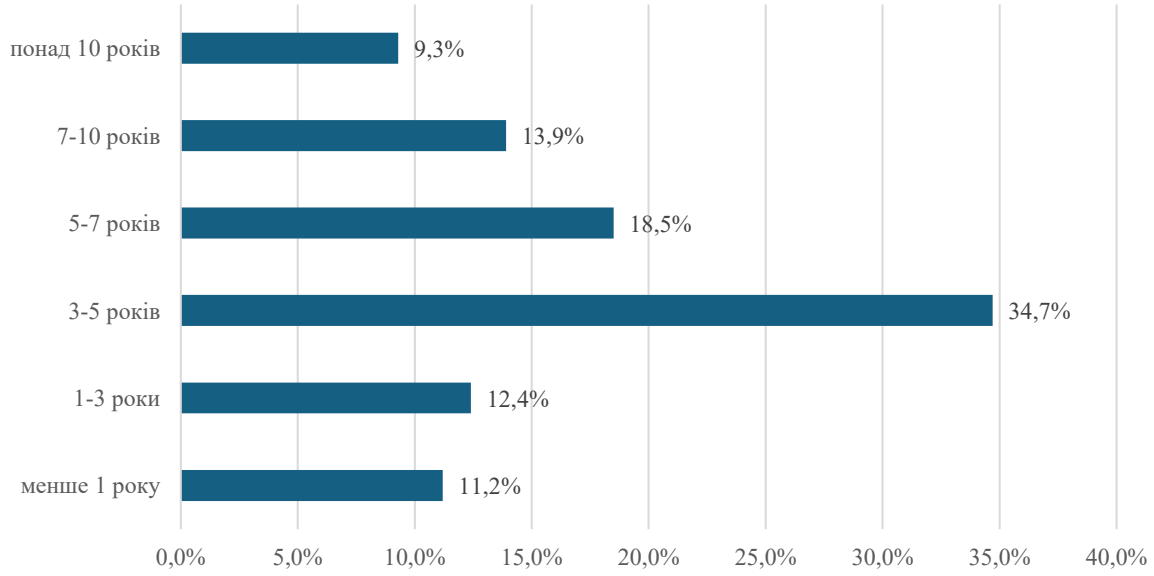

Рис. 2.16. Період роботи опитаних працівників на поточному місці роботи

Джерело: розроблено автором

Не високим є також рівень лояльності серед працівників, які працюють менше 3 років, що вказує на те, що їх роботодавці, до яких вони прийшли під час пандемії COVID-19, після її закінчення або вже під час війни, не завжди приділяють достатньо уваги щодо залучення нових працівників до цінностей їх компаній.

Відповіді респондентів на запитання «Як би ви оцінили рівень вашої лояльності до підприємства, на якому ви працюєте, під час війни з 24 лютого 2022 року?» представлені на рис. 2.17.

Розподіл самооцінок лояльності під час війни свідчить про поляризацію: частка з високою/дуже високою лояльністю становить 44,9% (23,5% і 21,4% відповідно), тоді як низька/дуже низька – 38,3% (18,9% і 19,4%). Частка середнього рівня – лише 16,8%. Отже, поряд із помітним ядром лояльних працівників зберігається значний сегмент із низькою лояльністю, що підтверджує попередні спостереження та вказує на потребу

цільових HR-інтервенцій (комунікація, підтримка, програми залучення) для зниження розриву між групами.

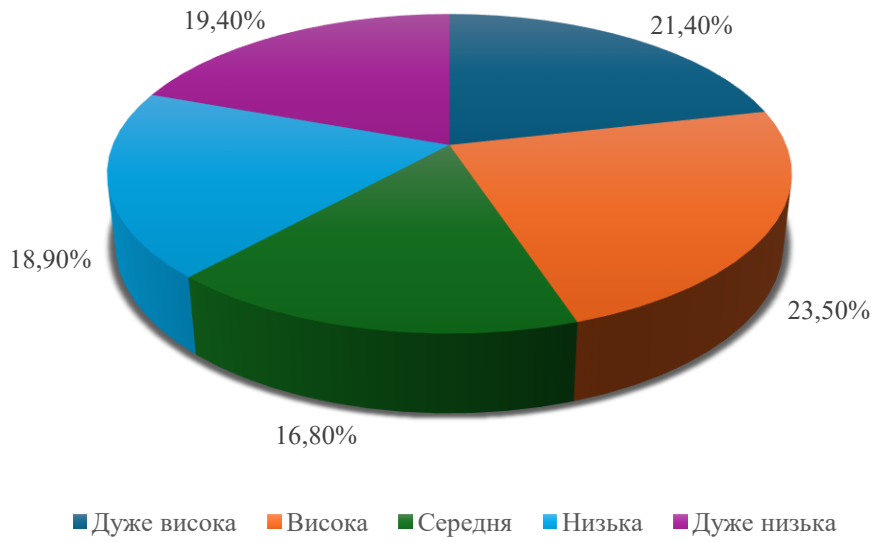

Рис. 2.17. Відповіді респондентів на запитання «Як би ви оцінили рівень вашої лояльності до підприємства, на якому ви працюєте, під час війни з 24 лютого 2022 року?»

Джерело: розроблено автором

Відповіді респондентів на запитання «Які з наступних факторів найбільше вплинули на вашу лояльність до підприємства під час війни?» (рис. 2.18) вказує, що найбільш вагомим фактором є фінансова стабільність та своєчасна виплата заробітної плати (96,7%) та забезпечення безпеки та охорони праці (85,3%).

Рис. 2.18. Відповіді респондентів на запитання «Які з наступних факторів найбільше вплинули на вашу лояльність до підприємства під час війни?»

Джерело: розроблено автором

Показником, який, на думку респондентів, найменше впливає на лояльність працівників до підприємства під час війни є можливості для професійного розвитку та навчання (57,8%). Водночас, серед інших факторів, які відзначили респонденти під час опитування, була відзначена можливість бронювання від мобілізації (57,8%).

Відповіді респондентів на запитання «Чи відчували ви достатню підтримку з боку керівництва підприємства під час війни?» представлені на рис. 2.19.

Під час війни переважна більшість працівників відчували підтримку керівництва: 83,1% відповіли «так, завжди/здебільшого так» (34,8% і 48,3%), 12,1% - «інколи», і лише 4,8% - «рідко/ніколи» (3,6% і 1,2%). Така структура відповідей свідчить про високий рівень управлінської підтримки, що є важливим драйвером лояльності та утримання персоналу.

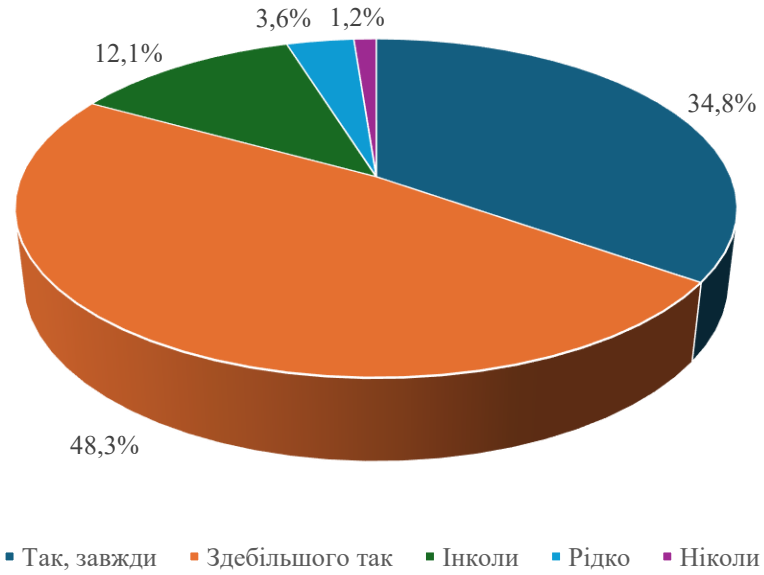

Рис. 2.19. Відповіді респондентів на запитання «Чи відчували ви достатню підтримку з боку керівництва підприємства під час війни?»

Джерело: розроблено автором

Відповіді респондентів на запитання «Чи задоволені ви рівнем комунікації та інформаційної підтримки, що надається підприємством у період війни?» вказують на нейтральне ставлення респондентів до комунікацій між керівництвом та працівниками (45,3%), задоволенні (12,5%) та високому рівні задоволенні (14,8%), що становить 72,6% (Рис. 2.20).

Вважаємо, що такий рівень комунікацій свідчить про достатній рівень ефективності інформаційної політики на підприємствах, чиї працівники брали участь в опитуванні.

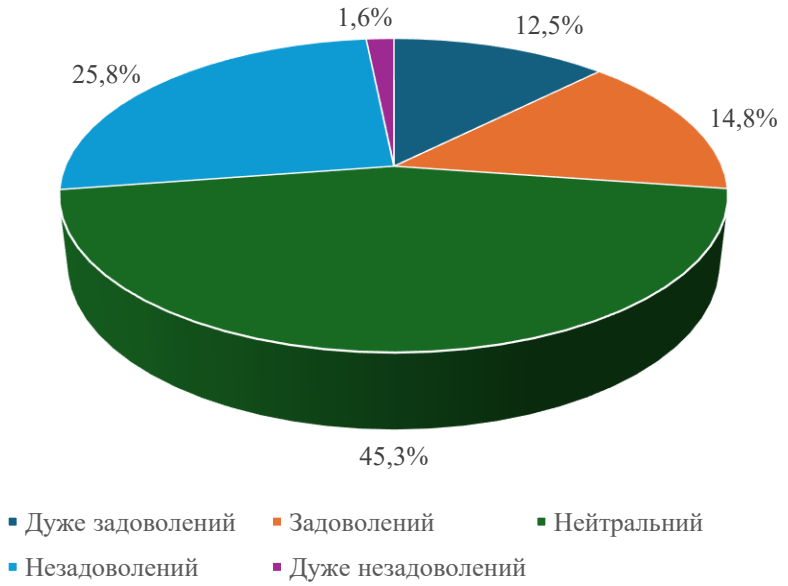

Рис. 2.20. Відповіді респондентів на запитання «Чи задоволені ви рівнем комунікації та інформаційної підтримки, що надається підприємством у період війни?»

Джерело: розроблено автором

Відповіді респондентів на запитання «Як часто ваше підприємство організовувало заходи з підтримки співробітників під час війни (психологічні тренінги, фінансова допомога, тощо)?» вказує на те, що на більшості підприємств проводяться відповідні заходи. Так «часто «проводяться такі заходи на 27,1% підприємствах, «дуже часто» - на 10,2% та «іноді» - 31,4% (рис. 2.21). Це свідчить про надання роботодавцями прямої підтримці своїм співробітникам.

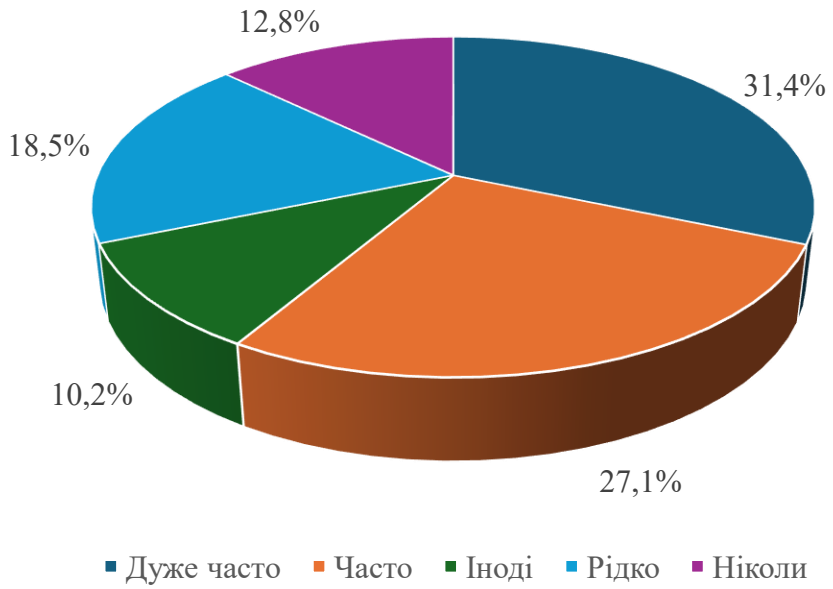

Рис. 2.21. Відповіді респондентів на запитання «Як часто ваше підприємство організовувало заходи з підтримки співробітників під час війни (психологічні тренінги, фінансова допомога, тощо)?»

Джерело: розроблено автором

Відповіді респондентів на запитання «Чи вплинула можливість працювати дистанційно на вашу лояльність до підприємства під час війни?» тісно пов'язані з попереднім питанням щодо терміну роботи, оскільки більшість підприємств змогло ефективно організувати свою діяльність під час пандемії COVID-19, що стало позитивним досвідом для організації роботи під час війни (Рис. 2.22). Певні складнощі в цьому, на нашу думку, могли мати лише ти працівники, які змінили своє місце роботи та/або не мають достатніх цифрових навичок.

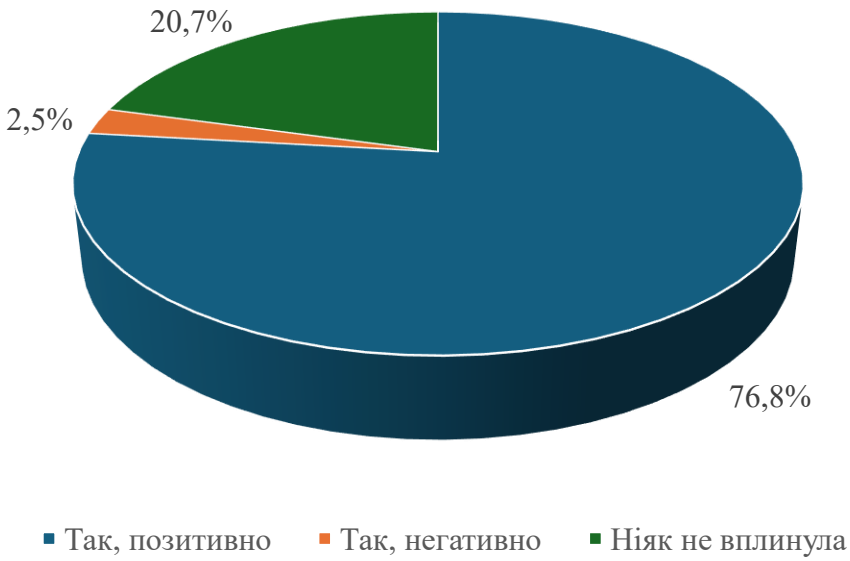

Рис. 2.22. Відповіді респондентів на запитання «Чи вплинула можливість працювати дистанційно на вашу лояльність до підприємства під час війни?»

Джерело: розроблено автором

Досить важливими в опитуванні стали відповіді респондентів на запитання «Чи змінилися ваші відчуття лояльності до підприємства з початком війни? Якщо так, то як саме?» (рис. 2.23). Так, у переважної більшості респондентів рівень лояльності залишився незмінним (68,8%), але також водночас наявні випадки зростання (16.4%) та зменшення (14,8%) лояльності, що підтверджують відповіді на попередні питання.

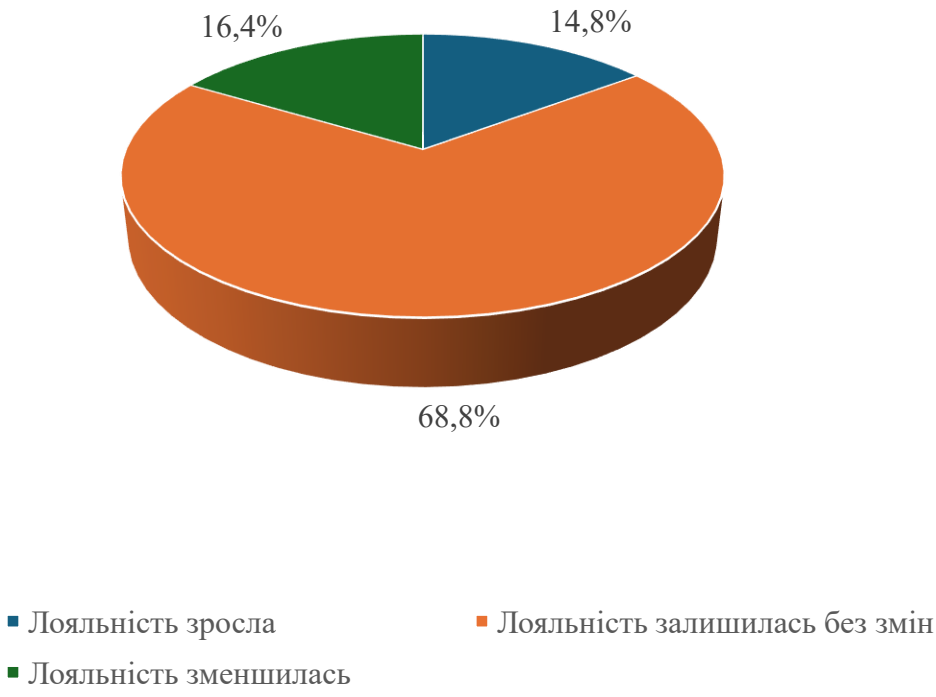

Рис. 2.23. Відповіді респондентів на запитання «Чи змінилися ваші відчуття лояльності до підприємства з початком війни? Якщо так, то як саме?»

Джерело: розроблено автором

Не менш важливими є відповіді респондентів на запитання «Чи плануєте ви продовжувати працювати в цьому підприємстві після завершення війни?», оскільки саме вони напряму характеризують лояльність працівників до роботодавців (рис. 2.24). Результати свідчать, що переважна більшість респондентів не планує змінювати місце роботи (56,4%) і лише 27,8% - планують. Основними причинами такої ситуації, зрозуміло, стала війна, яка триває вже третій рік поспіль, а також зміни в умовах праці для тих, хто працює з-за кордону, посилення мобілізації, скорочення бізнесу та ін.

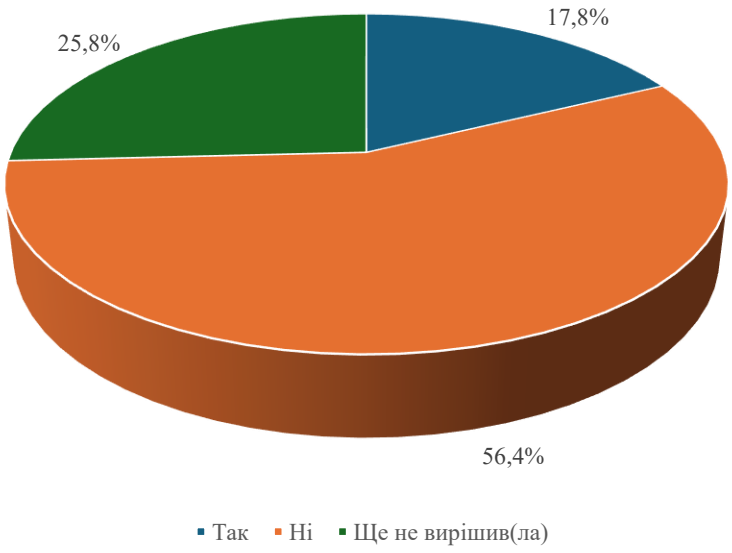

Рис. 2.24. Відповіді респондентів на запитання «Чи плануєте ви продовжувати працювати в цьому підприємстві після завершення війни?»

Джерело: розроблено автором

Відповіді респондентів на запитання «Які додаткові заходи, на вашу думку, могли б зміцнити вашу лояльність до підприємства в умовах війни?» (рис. 2.25) показали, що найвагоміше значення має своєчасність виплати заробітної плати в кризових умовах (98,2%), забезпечення безпечних та комфортних умов праці (85,(%) та забезпечення можливості працювати з дому або за гнучким графіком (82,5%).

Найменш важливими заходами, на думку респондентів, є надання необхідних засобів індивідуального захисту та обладнання (37,6%) та організація заходів та програм для дітей працівників (38,9%).

Рис. 2.25. Відповіді респондентів на запитання «Які додаткові заходи, на вашу думку, могли б зміцнити вашу лояльність до підприємства в умовах війни?»

Джерело: розроблено автором

Повномасштабна війна спричинила радикальну перебудову соціально-економічного середовища функціонування промислових підприємств України. У таких умовах лояльність персоналу перетворюється на критичний детермінант економічної безпеки, оскільки безпосередньо впливає на стабільність операцій, дотримання вимог охорони праці, дисципліну виконання процедур, частоту інцидентів, рівень плинності кадрів і, зрештою, на витрати та результативність. Дані опитування працівників, проведеного у лютому–березні 2024 року, вказують на

поляризацію самооцінок лояльності, домінування фінансової стабільності та своєчасної виплати заробітної плати серед ключових чинників прихильності, високе значення підтримки й комунікації з боку керівництва та недостатню регулярність зворотного зв'язку. Ці емпіричні сигнали задають рамку для аналізу внутрішніх і зовнішніх загроз економічній безпеці з боку персоналу в розрізі окремих підприємств і дозволяють окреслити цілеспрямовані управлінські відповіді.

Акціонерне товариство «Укрзалізниця». Внутрішні загрози формується насамперед через недоукомплектованість змін, втому локомотивних і ремонтних бригад, порушення вимог охорони праці на коліях і в депо, а також через ризики недоброчесності на точках продажу послуг, що здатні знижувати довіру пасажирів і вантажовідправників. Додатково загрозою є втрата унікальних компетенцій у вузьких спеціалізаціях. Зовнішній контур підсилюється дефіцитом кваліфікованих кадрів на ринку праці, міграційними процесами, психологічним тиском на працівників у прифронтових регіонах та загрозами соціальної інженерії й фішингу проти користувачів корпоративних систем. Підвищення лояльності через своєчасні виплати, безпечні умови праці, опіку керівництва та прозору комунікацію прямо зменшує імовірність операційних відмов і супутніх фінансових втрат.

Приватне акціонерне товариство «Національна енергетична компанія "Укренерго"». Внутрішні ризики зумовлені професійним вигоранням диспетчерського персоналу, помилками в роботі з автоматизованими системами керування та інцидентами, що походять з людського чинника. Уразливими є також питання розмежування доступів та збереження інженерних знань. Зовнішні загрози реалізуються через таргетовані кібервпливи на працівників (фішинг, соціальна інженерія), хронічний дефіцит інженерів-енергетиків і часті регуляторні зміни, що збільшують навантаження на лінійний персонал. Підтримка змін, чіткі

протоколи дій, системна профілактика втоми та жорсткі стандарти інформаційної гігієни знижують імовірність інцидентів і стабілізують показники надійності.

Акціонерне товариство «Укргідроенерго». Внутрішні загрози концентруються у площині дотримання регламентів гідробезпеки, перевантаження чергових змін і залежності від вузьких експертів, що підвищує чутливість до відсутності окремих фахівців. Зовнішній контур посилюється психологічним тиском війни, дефіцитом гідроенергетичних спеціалістів на ринку праці та маніпуляціями через соціальну інженерію. Інституціалізація наставництва, регулярні «післязмінні» оцінки стану персоналу, а також безкомпромісна культура безпеки забезпечують зменшення аварійності та простоїв.

Акціонерне товариство «Укрнафта». Внутрішні ризики передусім пов’язані з порушеннями охорони праці у видобутку та переробці, а також із ризиками недоброчесності у закупівлях і логістиці, що можуть конвертуватися у прямі втрати та санкції. Втрата технологічних і геологічних знань погіршує стабільність виробництва. Зовнішні загрози формуються волатильністю ринку праці для дефіцитних спеціальностей, підвищенням вимог до дотримання правил і вразливістю роздрібних точок до соціальної інженерії. Підсилення лояльності через надійну компенсацію, безпечні умови та адресні «причинно-наслідкові» зворотні зв’язки знижує частоту інцидентів, стабілізує зміни та витрати.

Публічне акціонерне товариство «Центренерго». Внутрішні загрози зумовлені дефіцитом компетенцій на теплових електростанціях, старінням обладнання і падінням залученості, що підвищує ризик помилок і простоїв. Зовнішні – дефіцит фахівців відповідного профілю, психологічний тиск персоналу та інтенсивні кібератаки через людський чинник. Інвентаризація й розвиток критичних компетенцій, регулярні короткі заміри настроїв змін

і політика невідкладної реакції на сигнали працівників підвищують коефіцієнт готовності та зменшують тривалість ремонтних вікон.

Публічне акціонерне товариство «Сумихімпром». Внутрішній контур ризику формується складністю процесної хімії: порушення технологічної дисципліни, витік технологічних знань, старіння кадрового складу, що збільшує чутливість до незаповнених змін. Зовнішні загрози – дефіцит інженерно-хімічних кадрів, посилення екологічного нагляду і соціальна напруга в громаді навколо екологічних питань. Підвищення лояльності через прозорі комунікації, стабільну оплату, наставництво та чіткі карти знань безпосередньо зменшує аварійність і витрати на брак.

Акціонерне товариство «Дніпроазот». Внутрішні загрози пов'язані з роботами з небезпечними речовинами, де будь-які відхилення від процедур мають високі наслідки; додатково ризиковими є недоброчесні практики у закупівлях і збуті та відтік операторів критичних дільниць. Зовнішні – конкуренція за кваліфікованих хіміків і операторів, інформаційні впливи на персонал і зміни в регулюванні небезпечних речовин. Систематичні «клімат-опитування» безпеки, підтримка психологічної стійкості й сувора відповідальність за дотримання регламентів зменшують частоту та тяжкість інцидентів.

Приватне акціонерне товариство «Полтавський гірничо-збагачувальний комбінат» (Ferrexpo). Внутрішні загрози зосереджені навколо втоми операторів великовантажної техніки, порушень безпеки на дробильних і конвеєрних лініях, а також ризиків недоброчесності у логістиці. Зовнішні – дефіцит машиністів і механіків на ринку праці, фішингові впливи та спірні питання якості продукції, що створюють додаткове навантаження на персонал. Інтеграція коротких «пульсових» вимірів стану змін із даними про простої, брак і ремонти забезпечує адресні управлінські інтервенції й швидко конвертує лояльність у нижчу собівартість.

Публічне акціонерне товариство «АрселорМіттал Кривий Ріг». Внутрішні ризики стосуються безпеки у гарячих процесах, дефіциту сталеварів і ремонтників та можливих соціально-трудових конфліктів у напружених виробничих режимах. Зовнішні – конкуренція за рідкісні компетенції, психологічне навантаження та релокація працівників і стійкі кібервиклики через персонал. Посилення культури безпеки, цілеспрямоване утримання фахівців, регулярний якісний зворотний зв'язок і видимість управлінських рішень за результатами вимірювань знижують частоту переробок і підвищують якість.

Акціонерне товариство «Запоріжсталь». Внутрішні загрози пов'язані з порушеннями безпеки у гарячих переділах, дисбалансом компетенцій у ремонтних підрозділах і можливими зловживаннями в ланцюгах постачання. Зовнішні – селективний відтік кадрів, соціально-психологічні ризики великого міста та інформаційні впливи на працівників. Регулярні короткі вимірювання лояльності у цехах, персоніфіковані плани розвитку і сувора політика доступів підтримують стабільність змін, скорочують час простоїв і підсилюють операційну маржу.

Таблиця 2.8 узагальнює типові внутрішні та зовнішні загрози, що походять від персоналу, показує канали їх передачі на економічну безпеку (через помилки, інциденти, простої, плинність) і пропонує базові контрзаходи. Наведені індикатори слугують «ранніми сигналами» для моніторингу, а перелік управлінських відповідей – мінімальним набором інструментів швидкого реагування.

Спільним знаменником виступає людський фактор під високим навантаженням, дисципліна безпеки та інформаційна гігієна. Найвищий ефект забезпечують регулярні «пульсові» вимірювання, безкомпромісна охорона праці, утримання критичних компетенцій і антифішингові практики, за умови «замикання циклу» результатів у конкретні дії.

Таблиця 2.8

Спільні внутрішні та зовнішні загрози діяльності промислових підприємств, спричинені персоналом

Тип загрози	Узагальнений зміст	Вплив на економічну безпеку	Індикатори/сигнали (приклади)	Базові контрзаходи
Внутрішні загрози				
Перевтома, вигорання	Перевантаження змін, стрес у воєнних умовах	Зростання помилок, інцидентів, простоїв	Абсентеїзм, понаднормові, «майже-інциденти»	«Пульсові» опитування, ротація змін, підтримка ментального здоров'я
Порушення регламентів безпеки	Недотримання процедур ОП та технологічної дисципліни	Аварійність, штрафи, збитки від браку	Актування порушень, частота переробок	Наставництво, аудит дотримання процедур, навчання high-risk ролей
Втрата критичних компетенцій	Відтік/старіння вузьких фахівців, незакриті зміни	Довші ремонти, зниження якості та випуску	Час виходу на продуктивність, «вузькі місця» у графіках	Карти знань, «stay»-інтерв'ю, планування наступництва
Недоброчесність/ комплаєнс	Ризики в закупівлях, логістиці, продажах	Прямі фінансові втрати, репутаційні ризики	Скарги, нетипові операції, інциденти контролю	Розмежування доступів, 4-очі, аналітика транзакцій
Інформаційна гігієна	Людський фактор у IT/OT контурах	Кіберинциденти, простої	Фішингові кліки, порушення політик	Тренінги, фішинг-симуляції, MFA, мінімальні доступи
Зовнішні загрози				
Дефіцит кадрів	Конкуренція за інженерів та робітничі професії	Зростання витрат, нестабільність змін	Вакансії>90 днів, рівень відмов	Пакети утримання, дуальна освіта, релокація/бронювання
Психологічний тиск війни	Тривожність, релокації сімей	Зниження залученості, плинність	«Нейтральні»/«низькі» тональності фідбеку	Підтримка, гнучкі графіки, дистанційні формати там, де можливо
Регуляторна турбулентність	Часті зміни вимог і перевірок	Незаплановані витрати, простої	Зростання комплаєнс-подій	Оперативні SOP, legal-комунікація, навчання «швидких змін»
Соціальна інженерія/ фішинг	Таргет-атаки на персонал	Компрометація систем, простій	Частка позитивних кліків	Постійні симуляції, «security champions» у підрозділах

Джерело: розроблено автором

Таблиця 2.9 диференціює профілі загроз і управлінські пріоритети за підприємствами, фіксуючи технологічні, організаційні та ринкові особливості. Такий зріз дозволяє зіставити чутливі ділянки та підібрати адресні інтервенції замість універсальних, але малоефективних рішень.

Таблиця 2.9

Внутрішні та зовнішні загрози, специфічні для кожного з досліджених промислових підприємств

Підприємство	Специфічні внутрішні загрози	Специфічні зовнішні загрози	Найчутливіші ділянки	Пріоритетні відповіді
АТ «Укрзалізниця»	Недоукомплектованість змін, втома локомотивних/ремонтних бригад, ризики недоброчесності на точках сервісу	Міграція кадрів, тиск у прифронтових регіонах, фішинг	Експлуатація, депо, касові/клієнтські сервіси	Стабілізація графіків, «пульс»-опитування, контроль продажів, програми утримання
ПрАТ «НЕК “Укренерго”»	Вигорання диспетчерів, помилки в АСК/SCADA, розмежування доступів	Таргетовані кібератаки, дефіцит енергетиків, регуляторний тиск	Диспетчерські центри, IT/OT інтерфейси	Антифішинг, протоколи втоми, тестування готовності, резервні зміни
АТ «Укргідроенерго»	Перевантаження чергових, залежність від вузьких експертів, дисципліна гідробезпеки	Дефіцит гідроспеців, психологічний тиск	Гідровузли, оперативні зміни	Наставництво, «післязмінні» скринінги, аудит процедур
АТ «Укрнафта»	Порушення ОП у видобутку/переробці, комплаєнс у закупівлях/збуті, втрата технологічних знань	Волатильність ринку праці для дефіцитних ролей, соціальна інженерія на АЗС	Видобуток, НПЗ, роздріб	«Stay»-інтерв’ю, карти знань, жорсткий комплаєнс-скрінінг ланцюгів
ПАТ «Центренерго»	Дефіцит компетенцій на ТЕС, падіння залученості, ризик помилок	Дефіцит профільних фахівців, кібервпливи	Змінний персонал, ремонтні бригади	Карти компетенцій, короткі заміри настроїв, пріоритезація навчання
ПАТ «Сумихімпром»	Порушення технологічної дисципліни, витік знань, старіння кадрів	Дефіцит інженерів-хіміків, посилення економ	Реактори, контроль якості	Контент-аналіз відхилень, наставництво, документування процедур
АТ «Дніпроазот»	Високий ризик відхилень у роботі з небезпечними речовинами, комплаєнс-загрози	Конкуренція за операторів, зміни регулювання небезпечних речовин	Цехи небезпечних речовин, аварійні служби	«Клімат» безпеки, стрес-менеджмент, нульова толерантність до порушень
ПрАТ «Полтавський ГЗК» (Ferrexpo)	Втома операторів важкої техніки, порушення безпеки на конвеєрах, недоброчесність у логістиці	Дефіцит механіків/машиністів, спори щодо якості	Кар’єри, дробильно-збагачувальні лінії	«Пульс» про втому, аналіз «майже-інцидентів», адресні інтервенції
ПАТ «АрселорМіттал Кривий Ріг»	Ризики у гарячих процесах, дефіцит сталеварів/ремонтників	Конкуренція за рідкісні	Плавка, прокат, ремонти	Культура безпеки, утримання

Підприємство	Специфічні внутрішні загрози	Специфічні зовнішні загрози	Найчутливіші ділянки	Пріоритетні відповіді
	, соціально-трудові напруги	компетенції, релокація кадрів		ключових, регулярний якісний фідбек
АТ «Запоріжсталь»	Порушення безпеки у гарячих цехах, дисбаланс компетенцій у ремонтах, ризики зловживань у поставках	Відтік кадрів у великих містах, інформаційні впливи	Гарячі переділи, ремонтні служби	Часті «пульси», персоніфікований розвиток, сувора політика доступів

Джерело: розроблено автором

Спільний знаменник загроз – людський фактор під високим навантаженням, дисципліна безпеки, дефіцит компетенцій і кібервразливості через персонал. Відмінності зумовлені технологічним профілем (інфраструктура, енергетика, хімія, ГЗК, металургія) та організаційною інерцією. Пріоритети: регулярні «пульсові» вимірювання, безкомпромісна охорона праці, утримання критичних фахівців, комплаєнс і інформаційна гігієна, із «замиканням» результатів у конкретні управлінські дії.

Узагальнюючи результати, доцільно змістити акцент із переліку загроз і типових заходів на інституціоналізацію управління:

по-перше, запровадити єдину рамку даних і підзвітності (відповідальні за показники, паспорти метрик, пороги ескалації) з інтеграцією кадрових, виробничих та ризикових індикаторів у спільні аналітичні панелі;

по-друге, здійснювати пріоритизацію втручань на основі карт «гарячих точок» (підрозділи/зміни з найвищим очікуваним ефектом), поєднуючи короткі цикли покращень із програмами розвитку критичних компетенцій;

по-третє, забезпечити керованість процесу через чіткі договірні рівні сервісу для зворотного зв’язку і коригувальних дій, бюджетування заходів та регулярну оцінку результативності (наприклад, динаміка часу виходу на продуктивність, довжина ремонтного беклогу, частота «майже інцидентів»).

Це дозволить перевести роботу з персоналом у ризик-орієнтований, доказовий формат, що підвищує відтворюваність рішень, прискорює локалізацію вразливостей і, відповідно, зміцнює агрегований рівень економічної безпеки кожного з розглянутих підприємств.

Результати проведеного дослідження дозволили систематизувати основні напрями підвищення лояльності персоналу українських компаній під час війни в Україні (табл. 2.10).

Таблиця 2.10

Пропозиції щодо підвищення лояльності персоналу українських промислових підприємств під час війни в Україні

Напрями	Заходи	Опис
Фінансова підтримка та стабільність	Своєчасна виплата заробітної плати	Забезпечення регулярних і своєчасних виплат заробітної плати навіть у складних умовах
	Бонуси та премії	Впровадження системи додаткових фінансових заохочень для працівників, які демонструють високу відданість і продуктивність
Безпека та охорона праці	Фізична безпека	Створення та підтримка безпечних умов праці, включаючи облаштування укриттів та забезпечення засобами індивідуального захисту
	Психологічна підтримка	Організація регулярних психологічних консультацій та тренінгів для зниження рівня стресу серед працівників
Гнучкість робочого графіку та умов праці	Дистанційна робота	Надання можливості працювати з дому або за гнучким графіком, що дозволить працівникам адаптуватися до нових умов
	Додаткові вихідні дні	Впровадження додаткових днів відпочинку для зменшення стресу та підтримки здоров'я працівників
Соціальна підтримка та добробут	Медична допомога	Надання доступу до медичних послуг та страхування для працівників та їхніх родин
	Підтримка родин співробітників	Допомога родинам, які постраждали від війни, через надання житла, їжі та інших необхідних ресурсів
Комунікація та інформаційна підтримка	Прозорість та відкритість	Регулярне інформування працівників про поточну ситуацію в компанії, плани та заходи, що вживаються
	Використання внутрішніх комунікаційних платформ	Створення каналів для оперативного зв'язку з працівниками та отримання зворотного зв'язку
Професійний розвиток та навчання	Програми навчання	Запровадження курсів та тренінгів для підвищення кваліфікації працівників, що допоможе їм адаптуватися до нових умов

Напрями	Заходи	Опис
	Кар'єрне зростання	Створення можливостей для професійного розвитку та підвищення по службі всередині компанії
Залучення працівників до прийняття рішень	Комітети та робочі групи	Формування груп для обговорення важливих питань та прийняття рішень, що стосуються умов праці
	Регулярні опитування та фокус-групи	Проведення опитувань для збору думок працівників та їх пропозицій щодо покращення умов праці
Соціальна відповідальність та благодійність	Участь у соціальних проектах	Залучення компанії до благодійних акцій та проектів, що підтримують місцеві громади та постраждалих від війни
	Підтримка волонтерських ініціатив	Заохочення працівників до участі у волонтерських проектах та підтримка їхньої діяльності
Поліпшення умов праці	Оновлення інфраструктури	Поліпшення робочого середовища та умов праці, включаючи модернізацію офісів та виробничих приміщень
	Запровадження додаткових пільг	Надання працівникам додаткових пільг, таких як оплачувані відпустки, гнучкі години роботи та інші бонуси
Репутація та брендинг	Підтримка позитивного іміджу	Активне просування позитивного іміджу компанії як соціально відповідального роботодавця, що дбає про своїх працівників
	Визнання та нагородження працівників	Організація заходів для визнання досягнень та заслуг працівників, що підвищує їхню мотивацію та лояльність

Джерело: розроблено автором

Отже, лояльність персоналу є критично важливим аспектом успішного функціонування підприємств, особливо в умовах війни. Використання різних джерел інформації та інструментів дозволяє отримати комплексне уявлення про рівень лояльності працівників та вжити відповідних заходів для її підвищення. Сучасні технології та аналітичні методи значно спрощують цей процес, надаючи менеджерам потужні інструменти для прийняття обґрунтованих рішень.

Висновки до другого розділу

За результатами проведеного дослідження, можна зробити наступні висновки, які дозволяють оцінити стан економічної безпеки підприємств та встановити вплив лояльності персоналу на її забезпечення.

1. Уточнено трактування економічної безпеки підприємства як інтегральної здатності системи своєчасно ідентифікувати загрози, запобігати їх реалізації, витримувати вплив ризиків і відновлювати цільові параметри без критичної втрати вартості та керованості. Такий підхід свідомо виходить за межі суто фінансових метрик і включає виробничо-операційні, технологічні, інформаційні, екологічні та соціально-кадрові виміри, що відображає сучасну багатовимірність безпеки. Додатково окреслено зовнішні та внутрішні драйвери турбулентності (цінова волатильність енергоресурсів, розриви ланцюгів постачання, цифровізація, кіберзагрози), які формують актуальний контекст оцінювання на промислових підприємствах. Цим закладено концептуальну та предметну рамку для подальшого зв’язування «людського» виміру з процесними, фінансовими та ризиковими індикаторами.

2. Сформовано емпіричну базу й проведено прикладний аналіз інструментарію вимірювання лояльності. По-перше, описано та інтерпретовано результати опитування (лютий–березень 2024 р.) працівників підрозділів управління персоналом українських підприємств; на основі відповідей зафіксовано домінування комбінованого використання кількісних і якісних методів. По-друге, ідентифіковано структуру інструментів збирання даних: поширеність онлайн-форм на кшталт Google Forms (переважаючий канал), застосування спеціалізованих систем управління людськими ресурсами, внутрішніх корпоративних платформ та ручних підходів; показано наслідки такої структури для інтеграції, автоматизації та глибини аналітики. По-третє, розкрито практики

аналітичної обробки (переважання статистичного та порівняльного аналізу із доповненням контент- і SWOT-аналізом) та рівень цифровізації (використання автоматизованих систем для обробки даних про лояльність). Нарешті, узагальнено роль HRM-систем і аналітичних платформ (SPSS, Tableau) у підвищенні відтворюваності, точності та управлінської корисності оцінок, що дає змогу пов’язувати метрики лояльності з ризик- та фінансово-процесними показниками економічної безпеки.

3. Побудовано системну карту загроз «з боку персоналу» з розподілом на внутрішні та зовнішні контури, уточнено їх механізми впливу на економічну безпеку й окреслено релевантні контрольні заходи. До внутрішніх віднесено ризики дисципліни та культури безпеки, плинність і дефіцит критичних компетенцій, відхилення у виробничій якості, інциденти інформаційної безпеки та комплаєнсу, ситуативні порушення технологічної дисципліни; наголошено на зв’язку цих ризиків із профілем лояльності. До зовнішніх – регуляторні та юридичні впливи, інформаційні операції та соціальна інженерія, логістичні обмеження, фактори війни та дефіцит кадрів, що опосередковано активують внутрішні вразливості. Запропоновано інструменти ризик-менеджменту для пріоритизації та стримування таких загроз, включно з картами ризиків, паспортами показників, протоколами ескалації та посиленою інформаційною гігієною.

4. За результатами проведених досліджень було опубліковано одна стаття у фаховому виданні України, одна стаття у іноземному журналі та тези доповідей на конференції.

РОЗДІЛ 3
КОНЦЕПТУАЛЬНІ ЗАСАДИ УДОСКОНАЛЕННЯ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ ОЦІНЮВАННЯ ЛОЯЛЬНОСТІ ПЕРСОНАЛУ В СИСТЕМІ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПРОМИСЛОВИХ ПІДПРИЄМСТВ

3.1. Модель інтеграція результатів оцінювання лояльності в систему забезпечення економічної безпеки промислового підприємства

Запропонована Модель інтеграції результатів оцінювання лояльності персоналу в систему забезпечення економічної безпеки промислового підприємства (далі - Модель) подається як цілісна соціотехнічна конструкція, що перетворює дані про ставлення працівників, їх поведінкові патерни та практики взаємодії на керовані управлінські впливи.

У запропонованій Моделі, лояльність трактується як багатовимірна характеристика прихильності до організації з афективним, нормативним і інструментальним вимірами, яка проявляється у дотриманні технологічної дисципліни, безпеці праці, стабільності продуктивності, готовності до навчання та участі в удосконаленні процесів. Лояльність працівників впливає на продуктивність, якість, безпеку праці, дотримання процедур, дисципліну витрат, збереження компетенцій і ризик подій через людський фактор. Тому її вимірювання і кероване вбудовування у контур ризик-менеджменту є ключем до зниження операційних втрат і підвищення стійкості.

Економічна безпека підприємства у цій моделі розуміється як стан і спроможність підприємства своєчасно виявляти, запобігати та нейтралізувати дестабілізуючі фактори без критичної втрати вартості, керованості й операційної стійкості.

Теоретична передумова Моделі полягає у визнанні лояльності ведучим індикатором, що передує змінам у ключових показниках ризику, операційних коефіцієнтах і фінансових результатах, а отже може слугувати основою для випереджального управління загрозами.

За результатами проведеного у дослідження, було уточнено теоретико-методологічні засади інтеграції людського чинника у контур економічної безпеки промислового підприємства, з урахуванням вимог сучасного управління ризиками та резилієнс-орієнтованої логіки.

Метою розробленої Моделі є концептуально і операційно поєднати оцінювання лояльності персоналу з кількісними і якісними індикаторами економічної безпеки, щоб зменшити часовий лаг між появою деструктивних чинників і загроз та управлінським втручанням. Структура побудована навколо трьох положень, кожне з яких має власну сферу застосування і набір верифікованих індикаторів.

По-перше, лояльність персоналу пропонується розуміти як багатовимірну прихильність до організації з чітко відокремленими, але взаємопов’язаними вимірами: афективним, нормативним та інструментальним. Афективний вимір відображає емоційне прийняття цінностей і соціальну ідентифікацію з колективом, що проявляється у добровільній участі в ініціативах удосконалення та позитивній тональності внутрішніх комунікацій. Нормативний вимір фіксує відчуття зобов’язання дотримуватися правил і підтримувати стандарти якості та безпеки, що конкретизується стабільністю виконання процедур і готовністю брати на себе чергування у пікові періоди. Інструментальний вимір відбиває раціональну оцінку співвідношення вигод і витрат від трудових відносин, що виявляється у готовності продовжувати контракт, у зниженні пошуку альтернативних вакансій та у прагматичній підтримці змін, якщо вони покращують умови праці.

Для переходу від концепту до операціоналізації ці три виміри репрезентуються індикаторами двох типів. Перший тип охоплює самооцінні шкали та короткі опитувальні хвилі, що забезпечують чутливість до настроєвих зсувів. Другий тип містить поведінкові спостережувані показники, зокрема плинність, абсентеїзм, своєчасність проходження інструктажів, участь у навчанні, частоту порушень технологічних регламентів і частку раціоналізаторських пропозицій, що пройшли валідацію. Виміри поєднуються у композит через нормування до інтервалу від нуля до одиниці, перевірку внутрішньої узгодженості індикаторів і зважування за критеріями надійності та стратегічної релевантності для конкретної технологічної системи. Така конструкція мінімізує методні упередження та забезпечує збалансоване відображення як установок, так і фактичної поведінки.

По-друге, економічна безпека промислового підприємства розглядається як інтегрований індекс стану та спроможності системи підтримувати цільові параметри у п’яти доменах, важливих для створення вартості. До кількісного контуру належать грошові потоки, рентабельність і ліквідність, що фіксують фінансову стійкість у короткому та середньому горизонтах. До процесного контуру належать безперервність операцій, ефективність використання обладнання, оборотність запасів і дисципліна виконання графіків, що відтворюють технологічну керованість та здатність протидіяти збоям. До виробничо-технологічного контуру належить дотримання нормативів якості та безпеки праці, що безпосередньо впливають на ризик інцидентів і витрати на переробки. До інформаційного контуру належить захищеність даних і реєстр подієвих порушень доступу, що визначають стійкість до кіберзагроз і соціальної інженерії. До управлінсько-комплаєнсного контуру належить статус аудиторських застережень, наявність тригерів кредитних ковенантів і результати контрольних перевірок. Індикатори кожного домену проходять єдину

процедуру нормування, валідації та зважування з урахуванням секторальної специфіки, після чого агрегуються у підсумковий показник зі шкалою інтерпретації, що відображає зміну управлінського режиму при переходах через ключові пороги. Така інтегральна конструкція не редукує безпеку до фінансових коефіцієнтів, а поєднує фінансові, операційні та організаційні властивості системи, що робить її чутливою до ранніх відхилень.

По-третє, інтеграція лояльності в забезпечення економічної безпеки здійснюється у логіці підприємницького управління ризиками з повним циклом від контексту до моніторингу. На етапі задавання контексту визначаються стратегічні цілі, карти процесів і критичні ролі, для яких лояльність має найбільший вплив на операційні результати. На етапі ідентифікації ризиків формується перелік факторів впливу (загроз) з боку персоналу, що модулюються рівнем лояльності, зокрема порушення процедур, виробничі інциденти з людським чинником, витоки інформації та незакриття змін. На етапі аналізу встановлюється причинний ланцюг від змін індексу лояльності до ключових індикаторів ризику у процесному та фінансовому контурах, а також визначаються локальні еластичності, які відбивають чутливість кожного показника до поведінкових зсувів. На етапі оцінювання ризику результати інтегруються у карту ризиків з порогами для ескалації і з типологією сценаріїв реагування. На етапі реагування обираються інтервенції, що мають найбільшу маржинальну віддачу з огляду на вузькі місця, зокрема корекція графіків змін, утримання критичних компетенцій, посилення стандартів охорони праці та адресні програми розвитку керівників. На етапі моніторингу та комунікації впроваджується ритм коротких хвиль вимірювання, узгоджується частота оновлення дашбордів і фіксуються правила «замикання циклу», що вимагають перетворення сигналів про відхилення у конкретні дії з визначеними строками та відповідальними. У цій архітектурі лояльність виконує роль ведучого індикатора для підсистем операційного, кадрового,

технологічного та комплаєнс ризику і тим самим зменшує часовий лаг між появою слабкого сигналу та управлінським втручанням. Такий підхід зміцнює прогностичну спроможність контуру безпеки і підвищує резилієнтність підприємства в умовах високої невизначеності.

Концептуальна рамка Моделі має п’ять взаємопов’язаних шарів, які формують безперервний цикл від даних до рішень (рис. 3.1).

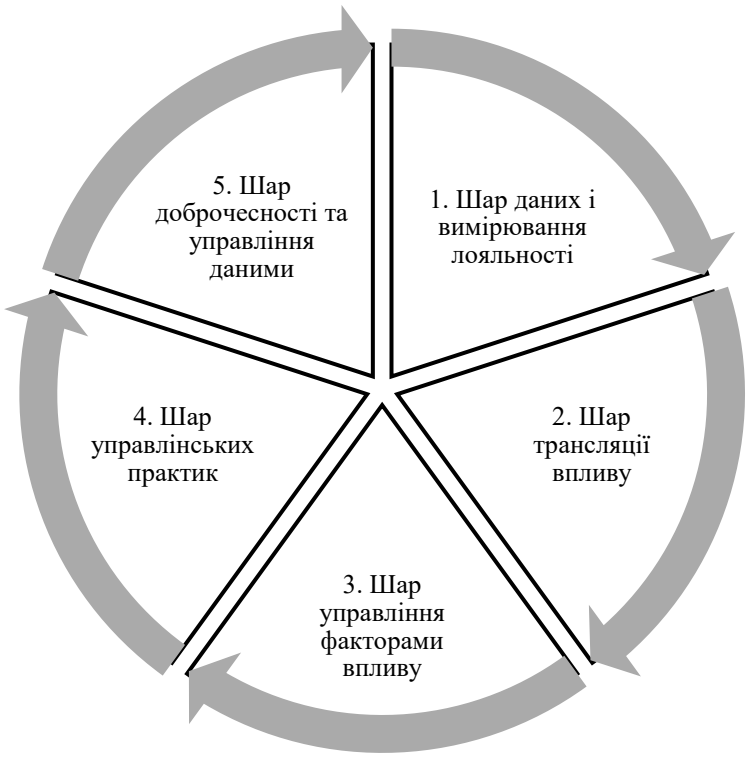

Рис. 3.1. П’ять взаємопов’язаних шарів концептуальної рамки Моделі інтеграція результатів оцінювання лояльності в систему забезпечення економічної безпеки промислового підприємства

Джерело: розроблено автором

Перший шар відповідає за збір і уніфікацію даних про лояльність з опитувань, коротких «pulse»-хвиль, інтерв’ю, метрик плинності, абсентеїзму, участі у навчанні, результатів оцінювання, внутрішніх тікетів підтримки і зворотного зв’язку. Дані нормуються до шкали від нуля до одиниці, перевіряється внутрішня узгодженість інструментів і стабільність шкал між хвилями.

Другий шар задає механізм передавання впливу лояльності в ключові показники діяльності. Для кожного показника визначається еластичність щодо змін лояльності, показники перетворюються в нормовані компоненти індексу безпеки з прозорими вагами, а також зберігаються коефіцієнти нормування для відтворюваності.

Третій шар реалізує управління факторами впливу через формування реєстру ризиків з боку персоналу, карти ризиків, ключових індикаторів ризику та тригерів ескалації на основі порогових значень інтегрального індексу.

Четвертий шар фокусується на управлінських практиках і включає плани утримання критичних компетенцій, зміни в режимах роботи змін, протоколи безпеки, стандарти комунікації та цільові програми навчання керівників.

П’ятий шар забезпечує етичність і якість даних за рахунок політик згоди, знеособлення, рольових доступів, паспортів показників, журналів аудиту та контролю якості.

Вимірювання лояльності здійснюється через інтегральний показник L, який агрегує три підіндекси прихильності та блок поведінкових сигналів. Афективний компонент відображає емоційне прийняття організаційних цінностей і команди, нормативний фіксує відчуття зобов’язання залишатися та підтримувати стандарти, інструментальний репрезентує раціональні вигоди співпраці з роботодавцем. Поведінкові сигнали включають стабільність відвідуваності, частку участі у навчанні, своєчасність проходження інструктажів з охорони праці, частоту подання раціоналізаторських пропозицій і показники дисциплінарних інцидентів. Для кожного блоку задаються ваги, що визначаються на основі надійності індикаторів та їх стратегічної релевантності для конкретної технологічної структури підприємства. Отриманий індекс інтерпретується на шкалі від низької до високої лояльності з використанням контрольних точок, які

встановлюються за результатами ретроспективного аналізу і маркують зміни управлінського режиму.

Індекс лояльності персоналу та його зв'язок з економічною безпекою. Індекс лояльності персоналу розглядається як латентна багатовимірна характеристика, що відображає готовність працівників залишатися в організації, підтримувати її цілі та дотримуватися встановлених норм поведінки в умовах підвищеної невизначеності. У межах моделі він позначається як L і належить інтервалу від 0 до 1, де значення, близькі до 0, відповідають низькій лояльності, а значення, близькі до 1, відповідають високій, стабільній лояльності. Концептуально індекс L формується на основі трьох підіндексів: афективної лояльності, нормативної лояльності та інструментальної лояльності, що дає змогу пов'язати суб'єктивні установки працівників з їх реальною поведінкою і подальшим впливом на ризики економічної безпеки.

Базове представлення індексу лояльності задається у вигляді зваженої лінійної композиції:

$$L = w_a L_a + w_n L_n + w_i L_i, \qquad (3.1)$$

де L_a афективна лояльність (емоційна прихильність до підприємства), L_n нормативна лояльність (відчуття зобов'язаності й морального обов'язку залишатися в організації), L_i інструментальна лояльність (раціональна оцінка вигід і втрат від продовження роботи в підприємстві).

Вагові коефіцієнти w_a, w_n, w_i належать інтервалу від 0 до 1 та задовольняють умову $w_a + w_n + w_i = 1$. Їх значення визначаються або експертно, або шляхом калібрування на історичних даних, виходячи з того, які компоненти лояльності є найбільш значущими для конкретного типу промислового підприємства.

Кожний підіндекс формується на основі системи первинних індикаторів, отриманих з кількох груп джерел. Для афективної лояльності ключовими є результати анонімних опитувань працівників, зокрема

середній бал за шкалою ставлення до роботодавця, готовності рекомендувати підприємство як місце роботи, суб'єктивної гордості за належність до компанії. Наприклад, афективний підіндекс може обчислюватися як

$$L_a = \frac{\bar{S}_{\text{аф}} - 1}{5 - 1}, \qquad (3.2)$$

де $\bar{S}_{\text{аф}}$ середній бал за низкою афективних тверджень за п'ятибальною шкалою Лайкерта, 1 мінімально можливе значення, 5 максимально можливе. Таким чином афективний компонент переводиться у нормовану шкалу від 0 до 1.

Нормативна лояльність L_n спирається на індикатори, що характеризують відчуття зобов'язання залишатися в організації, зокрема згоди з твердженнями типу «я відчуваю моральний обов'язок залишатися в цьому підприємстві», «було б неправильно залишити компанію за теперішніх умов», а також на поведінкові маркери тривалості роботи в підприємстві. Нормування може мати вигляд:

$$L_n = \alpha_1 \frac{\bar{S}_{\text{нор}} - 1}{5 - 1} + \alpha_2 \frac{T_{\text{стаж}}}{T_{\text{макс}}}, \qquad (3.3)$$

де $\bar{S}_{\text{нор}}$ середній бал за нормативними твердженнями, $T_{\text{стаж}}$ фактичний стаж роботи працівника в роках, $T_{\text{макс}}$ обраний верхній поріг стажу (наприклад, 10 років), α_1 та α_2 вагові коефіцієнти, що узгоджують внесок опитувальних та стажових показників. Якщо стаж перевищує $T_{\text{макс}}$, значення частки фіксується як 1.

Інструментальна лояльність L_i відображає раціональну оцінку працівником матеріальних та нематеріальних вигід від залишення в організації. Вона базується на самооцінці задоволеності заробітною платою, соціальним пакетом, умовами праці, можливостями бронювання від мобілізації, а також на даних щодо поведінки працівників на ринку праці.

У спрощеному вигляді:

$$L_i = \beta_1 \frac{\bar{S}_{\text{комп}} - 1}{5-1} + \beta_2 \left(1 - \frac{R_{\text{звіл,добров}}}{R_{\text{еталон}}}\right), \qquad (3.4)$$

де $\bar{S}_{\text{комп}}$ середній бал задоволеності компенсацією і пільгами, $R_{\text{звіл,добров}}$ річний рівень добровільних звільнень, $R_{\text{еталон}}$ референтний (критичний) рівень плинності для галузі.

Якщо фактична плинність перевищує референтний поріг, відповідна частка обмежується нульовим значенням. Таким чином поєднуються суб'єктивні оцінки працівників і об'єктивна статистика щодо збереження персоналу. Щоб забезпечити прозорість розрахунків, первинні дані для формування індексу L структуруються у вигляді єдиної таблиці джерел. У табл. 3.1 наведено приклад переліку типових показників, їх позначень, одиниць виміру та джерел для розрахунку індексу лояльності персоналу підприємства.

Усі первинні показники перетворюються у нормовані змінні на інтервалі від 0 до 1. Для опитувальних шкал використовується лінійне нормування за формулою:

$$z = \frac{x - x_{\min}}{x_{\max} - x_{\min}}, \qquad (3.5)$$

де x фактичний середній бал, $x_{\min}$ та $x_{\max}$ межі шкали (наприклад, 1 та 5).

Для показників, у яких більше означає гірший стан (рівень звільнень, незаплановані відсутності, кількість скарг), застосовується інверсія:

$$z = 1 - \frac{x - x_{\min}}{x_{\max} - x_{\min}},$$

що забезпечує єдину інтерпретацію: чим більший нормований показник, тим вищий очікуваний внесок у лояльність. Після нормування для кожного блоку обчислюється середнє або зважене середнє значення, яке і виступає відповідним підіндексом L_a, L_n, L_i.

Таблиця 3.1

Основні первинні показники для розрахунку індексу лояльності персоналу промислового підприємства

Блок лояльності	Показник	Позначення	Одиниця виміру	Джерело даних	Періодичність збирання
Афективна лояльність	Середній бал згоди з твердженням «я пишаюся тим, що працюю в цьому підприємстві»	$S_{1,\text{аф}}$	бал за шкалою від 1 до 5	Анонімне онлайн опитування працівників	один раз на рік, за потреби частіше
	Готовність рекомендувати підприємство як місце роботи (eNPS або аналог)	$S_{2,\text{аф}}$	бал або індекс від 0 до 10	Опитування, модуль eNPS в HRM системі	один раз на рік
Нормативна лояльність	Узагальнений бал за твердженнями про моральний обов’язок залишатися в організації	$S_{\text{нор}}$	бал від 1 до 5	Опитування працівників	один раз на рік
	Стаж роботи працівника в підприємстві	$T_{\text{стаж}}$	роки	Дані кадрового обліку, HRM система	щомісячне оновлення
Інструментальна лояльність	Середній бал задоволеності заробітною платою і соціальним пакетом	$S_{\text{комп}}$	бал від 1 до 5	Опитування, модуль задоволеності	один раз на рік
	Рівень добровільних звільнень	$R_{\text{звіл,добров}}$	відсотки до середньо-списковоі чисельності	Звітність HR і бухгалтерії	щоквартально
	Частка працівників, які мають можливість офіційного бронювання від мобілізації	$P_{\text{брон}}$	частка від 0 до 1	HRM система, юридичний відділ	щоквартально
Поведінковий компонент	Рівень незапланованих відсутностей (без лікарняних і відпусток)	$A_{\text{незапл}}$	дні на одного працівника	Система табелювання, HRM	щомісячне оновлення
	Кількість внутрішніх скарг і звернень щодо умов праці на 100 працівників	$C_{\text{скар}}$	кількість на 100 осіб	Канали зворотного зв’язку, служба персоналу	щоквартально

Джерело: розроблено автором

Зв’язок між лояльністю та економічною безпекою у моделі задається через інтегральний індекс економічної безпеки S, який також нормується на інтервалі від 0 до 1. У загальному вигляді:

$$S = 0{,}70S_{\text{quant}} + 0{,}30S_{\text{qual}}, \qquad (3.6)$$

де S_{quant} агрегований блок фінансових і процесних індикаторів (ліквідність, рентабельність, операційні витрати, оборотність запасів, показники безперервності виробництва), а S_{qual} блок якісних індикаторів (наявність аудиторських застережень, кількість значущих інцидентів охорони праці, судові спори, тригери кредитних ковенантів, якість інформаційної безпеки). У цьому контексті індекс лояльності L виступає однією з ключових пояснювальних змінних, що впливають як на окремі базові показники S_{quant} та S_{qual}, так і на інтегральне значення S.

Формалізований зв’язок між лояльністю персоналу та інтегральним індексом економічної безпеки описується через декілька типів індикаторів. По-перше, застосовується коефіцієнт кореляції між L та S, який у найпростішому вигляді обчислюється як:

$$r_{LS} = \frac{\text{cov}\,(L,S)}{\sigma_L \sigma_S}, \qquad (3.7)$$

де $\text{cov}\,(L,S)$ коваріація між індексами, σ_L та σ_S їх стандартні відхилення. Значення r_{LS}, наближені до 1, свідчать про сильний прямий зв’язок між зростанням лояльності та підвищенням рівня економічної безпеки, тоді як значення, близькі до нуля, вказують на слабкий або відсутній лінійний зв’язок.

По-друге, оцінюється еластичність економічної безпеки щодо лояльності на основі регресійної моделі

$$S_t = \alpha + \beta L_{t-1} + \gamma' Z_{t-1} + \varepsilon_t, \qquad (3.8)$$

де S_t значення інтегрального індексу економічної безпеки в періоді t, L_{t-1} індекс лояльності у попередньому періоді, Z_{t-1} вектор контрольних змінних (зовнішні макроекономічні умови, ціни на енергоносії, регуляторні

шоки, події воєнного характеру), α вільний член, β коефіцієнт чутливості економічної безпеки до змін лояльності, γ вектор коефіцієнтів для контрольних змінних, ε_t випадкова похибка. У цій моделі β інтерпретується як наближена оцінка похідної $\partial S / \partial L$, тобто як величина зміни інтегрального індексу безпеки за одиничної зміни лояльності за фіксованих інших умов.

По-третє, для управлінських інтерпретацій застосовуються індикатори типу «різниця середніх», які відображають відмінності у середньому рівні економічної безпеки між групами підприємств з високою та низькою лояльністю. Формально це можна записати як:

$$\Delta S = \bar{S}^{\text{вис}L} - \bar{S}^{\text{низ}L}, \qquad (3.9)$$

де $\bar{S}^{\text{вис}L}$ середнє значення індексу економічної безпеки для когорти підприємств із високими значеннями L (наприклад, $L \geq 0{,}75$), а $\bar{S}^{\text{низ}L}$ середнє значення для підприємств із низькою лояльністю (наприклад, $L \leq 0{,}50$). Додатне і статистично значуще ΔS свідчить про те, що вища лояльність персоналу пов'язана з більш сприятливим станом економічної безпеки.

Окрему групу становлять індикатори подійного типу, що пов'язують зміну лояльності з імовірністю настання негативних подій у сфері безпеки. Наприклад, для частоти інцидентів охорони праці можна оцінювати коефіцієнт регресії у моделі

$$\lambda_{\text{інц}} = \delta_0 + \delta_1 L + u, \qquad (3.10)$$

де $\lambda_{\text{інц}}$ інтенсивність інцидентів охорони праці (кількість інцидентів на 100 працівників або на 1 мільйон відпрацьованих людино-годин), δ_1 параметр, що відображає зміну інтенсивності інцидентів при змінах лояльності. Негативне значення δ_1 свідчить про те, що зростання лояльності пов'язане зі зниженням частоти інцидентів, тобто з покращенням одного з ключових вимірів економічної безпеки.

Узагальнення основних індикаторів зв’язку між лояльністю персоналу та економічною безпекою промислового підприємства наведено у табл. 3.2.

Таблиця 3.2

Індикатори зв’язку між індексом лояльності та економічною безпекою

Тип індикатора	Формалізоване визначення	Що вимірює	Управлінська інтерпретація
Кореляція між лояльністю і безпекою	$r_{LS} = \mathrm{cov}\,(L, S)/(\sigma_L \sigma_S)$	Силу лінійного зв’язку між L і S	Чи варто очікувати односпрямованих змін S при змінах L
Еластичність економічної безпеки	β з регресії $S_t = \alpha + \beta L_{t-1} + \gamma' Z_{t-1} + \varepsilon_t$	Маржинальну чутливість S до L	Наскільки підвищення лояльності змінює інтегральний рівень безпеки
Різниця середніх рівнів безпеки	$\Delta S = \bar{S}^{\text{вис}L} - \bar{S}^{\text{низ}L}$	Структурні відмінності між групами	Наскільки підприємства з високою лояльністю стійкіші за безпекою
Індикатори подійного ризику	$\lambda_{\text{інц}} = \delta_0 + \delta_1 L + u$	Вплив L на частоту інцидентів	Якою мірою зростання лояльності знижує ризик подій, що загрожують безпеці

Джерело: розроблено автором

Таким чином, індекс лояльності L, побудований на основі чітко визначених і нормованих первинних показників, вбудовується у систему економічної безпеки не лише як описовий соціально-психологічний параметр, а як кількісно визначений фактор ризику. Це відкриває можливість для сценарного моделювання, побудови прогнозів та цілеспрямованих управлінських інтервенцій, спрямованих на одночасне підвищення лояльності персоналу і зміцнення інтегральної економічної безпеки промислового підприємства.

Математичний механізм інтеграції результатів оцінювання лояльності в індекс економічної безпеки. Математичний механізм інтеграції результатів оцінювання лояльності персоналу в систему управління економічною безпекою промислового підприємства має на меті формалізувати ланцюг "лояльність персоналу - ключові показники діяльності - інтегральний індекс економічної безпеки". Інакше кажучи, необхідно чітко описати, яким чином зміна індексу лояльності L

трансформується в зміну конкретних операційних, фінансових і ризикових показників, а через них - у зсув інтегрального індексу економічної безпеки S. Такий підхід забезпечує не лише описовий аналіз, а й дає змогу проводити сценарне моделювання і кількісно оцінювати ефект управлінських інтервенцій, спрямованих на підвищення лояльності.

Система показників, нормування та побудова індексу безпеки. Початковим елементом є система ключових показників результативності та ризику $\{KPI_i\}$, які відображають основні виміри економічної безпеки підприємства. До цієї системи, зокрема, можуть входити: рівень добровільної плинності персоналу, частота виробничих інцидентів, частка браку, коефіцієнти ліквідності, операційна маржа, частота порушень комплаєнсу, виконання кредитних ковенантів, частка незапланованих простоїв, інтенсивність незапланованих відсутностей працівників. Для подальшої інтеграції всі показники переводяться в безрозмірну шкалу $[0; 1]$ у вигляді нормованих компонентів Z_i, де 0 відповідає найбільш несприятливому стану, а 1 - найкращому.

У загальному вигляді інтегральний індекс економічної безпеки підприємства задається як зважена сума нормованих компонентів:

$$S = \sum_{i=1}^{n} w_i Z_i, \qquad (3.11)$$

де Z_i нормований компонент, який відповідає i-му показнику, w_i ваговий коефіцієнт, що відображає відносну важливість цього компоненту в загальній структурі економічної безпеки, n кількість компонентів. Ваги задовольняють умову:

$$\sum_{i=1}^{n} w_i = 1, w_i \geq 0 \qquad (3.12)$$

Пропонуємо групувати показники у такі блоки: фінансові, операційні, кадрові, інформаційно-безпекові, юридично-комплаєнсні. Для кожного блоку пропонуємо обчислювати проміжний субіндекс, після чого формується інтегральний індекс S у відповідності до прийнятої моделі.

Нормування кожного показника KPI_i здійснюється за обраною функцією перетворення $f_i(\cdot)$, що відображає характер і напрямок його впливу. У найпростішому випадку використовується лінійне нормування типу:

$$Z_i = f_i(KPI_i) = \begin{cases} \dfrac{KPI_i - KPI_i^{\min}}{KPI_i^{\max} - KPI_i^{\min}}, & \text{якщо "більше - краще",} \\ 1 - \dfrac{KPI_i - KPI_i^{\min}}{KPI_i^{\max} - KPI_i^{\min}}, & \text{якщо "менше - краще".} \end{cases} \quad (3.13)$$

Тут $KPI_i^{\min}$ та $KPI_i^{\max}$ нижня і верхня референтні межі показника, які можуть задаватися на основі галузевих стандартів, історичних даних або цільових орієнтирів. Таким чином, позитивна динаміка показника в "правильному" напрямку завжди відображається зростанням відповідного Z_i.

Для подальших розрахунків важливим є коефіцієнт нормування g_i, який визначається як похідна нормувальної функції:

$$\mathrm{g_i} = \frac{\partial \mathrm{Z_i}}{\partial \mathrm{KPI_i}} \quad (3.14)$$

У випадку лінійного нормування g_i є сталою величиною і дорівнює:

$$g_i = \frac{1}{KPI_i^{\max} - KPI_i^{\min}} \quad (3.15)$$

для показника типу "більше - краще" або:

$$g_i = -\frac{1}{KPI_i^{\max} - KPI_i^{\min}} \quad (3.16)$$

для показника типу "менше - краще". Саме знак і величина g_i надалі визначають, яким чином зміна базового показника впливає на нормований компонент та на індекс S.

Для наочності у табл. 3.3 подано приклади базових показників, що можуть бути включені до моделі, відповідні нормовані компоненти та очікуваний напрямок впливу підвищення лояльності персоналу L на ці показники.

Таблиця 3.3

Приклади ключових показників, нормування та очікуваний зв'язок з лояльністю

Блок ризику	Базовий показник KPI_i	Тип нормування	Нормований компонент Z_i	Очікуваний вплив зростання Lна KPI_i	Очікуваний знак g_i
Кадровий	Рівень добровільної плинності персоналу, %	"менше - краще"	$Z_{\text{плин}} = 1 - \frac{KPI - KPI^{\min}}{KPI^{\max} - KPI^{\min}}$	Зниження плинності	негативний
	Середній час закриття вакансій у критичних ролях, днів	"менше - краще"	аналогічне нормування	Скорочення часу закриття	негативний
Операційний	Частка браку в загальному обсязі продукції, %	"менше - краще"	аналогічне нормування	Зменшення частки браку	негативний
	Частка незапланованих простоїв, %	"менше - краще"	аналогічне нормування	Зменшення простоїв	негативний
Охорона праці	Частота інцидентів з порушенням правил безпеки	"менше - краще"	аналогічне нормування	Зменшення частоти інцидентів	негативний
Фінансовий	Операційна маржа, %	"більше - краще"	$Z_{\text{маржа}} = \frac{KPI - KPI^{\min}}{KPI^{\max} - KPI^{\min}}$	Підвищення маржі через зменшення втрат	позитивний
Інформаційна безпека	Кількість інцидентів через "людський фактор"	"менше - краще"	аналогічне нормування	Зменшення інцидентів	негативний

Джерело: розроблено автором

Таким чином, індекс економічної безпеки S є детермінованою функцією набору нормованих компонентів $\{Z_i\}$, які, своєю чергою, залежать від базових показників $\{KPI_i\}$. Наступним кроком є формалізація того, як індекс лояльності L впливає на ці показники.

Передатна функція "лояльність - показники - індекс безпеки". Для побудови математичного зв'язку між лояльністю персоналу та індексом економічної безпеки використовується концепція "передатної функції". Вона описує, як невелика зміна індексу лояльності ΔLпередається через систему показників $\{KPI_i\}$ до зміни інтегрального індексу безпеки ΔS.

На першому кроці задається еластичність кожного базового показника щодо лояльності:

$$\alpha_i = \frac{\partial KPI_i}{\partial L} \qquad (3.17)$$

Цей параметр відображає, на скільки одиниць змінюється показник KPI_i при зміні лояльності на одну умовну одиницю в нормованій шкалі. Наприклад, $\alpha_{\text{плин}} = -4$ може означати, що підвищення індексу лояльності на 0,1 пункту пов'язане зі зниженням добровільної плинності персоналу на 0,4 відсоткового пункту, за інших рівних умов.

На другому кроці враховується нормування $KPI_i \to Z_i$. Для цього використовується раніше визначений коефіцієнт:

$$g_i = \frac{\partial Z_i}{\partial KPI_i} \qquad (3.18)$$

Якщо нормування лінійне, g_i є сталою, і його знак та величина відображають, наскільки чутливою є нормована шкала до змін базового показника. У випадку нелінійного нормування g_i може залежати від поточного значення KPI_i, але в рамках практичного застосування для невеликих змін часто використовують локальну лінійну апроксимацію.

На третьому кроці використовується структура самого індексу S. Оскільки:

$$S = \sum_{i=1}^{n} w_i Z_i, \qquad (3.19)$$

його похідна за нормованими компонентами дорівнює:

$$\frac{\partial S}{\partial Z_i} = w_i. \qquad (3.20)$$

Об'єднуючи ці три зв'язки (вплив L на KPI_i, вплив KPI_i на Z_i, вплив Z_i на S), отримуємо за правилом ланцюгової похідної:

$$\frac{\partial S}{\partial L} = \sum_{i=1}^{n} \frac{\partial S}{\partial Z_i} \cdot \frac{\partial Z_i}{\partial KPI_i} \cdot \frac{\partial KPI_i}{\partial L} = \sum_{i=1}^{n} w_i \cdot g_i \cdot \alpha_i. \qquad (3.21)$$

Позначимо:

$$\beta \equiv \frac{\partial S}{\partial L} = \sum_{i=1}^{n} w_i g_i \alpha_i. \qquad (3.22)$$

Параметр β виступає агрегованою чутливістю індексу економічної безпеки до змін лояльності. Він інтегрує три важливі аспекти: управлінські

пріоритети (через ваги w_i), техніку нормування та шкалювання (через g_i) і емпіричний вплив лояльності на конкретні показники (через α_i).

У практиці параметри α_i оцінюються на основі історичних даних методом регресійного аналізу. Для кожного показника будується модель виду:

$$KPI_{i,t} = a_i + b_i L_{t-1} + c_i' X_{t-1} + \varepsilon_{i,t}, \qquad (3.23)$$

де $KPI_{i,t}$ значення показника в періоді t, L_{t-1} індекс лояльності у попередньому періоді, X_{t-1}вектор контрольних змінних (зовнішні умови, цінові шоки, регуляторні зміни), $\varepsilon_{i,t}$ стохастична похибка. Оцінений коефіцієнт b_i інтерпретується як емпірична апроксимація α_i. Надалі ці оцінки масштабуються відповідно до обраної шкали L і діапазону KPI_i та використовуються в розрахунку β.

Для забезпечення прозорості зв'язків між лояльністю та економічною безпекою доцільно узагальнити інформацію про внесок окремих показників у табличній формі. У табл. 3.4 показано приклади такого узагальнення.

Таблиця 3.4

Узагальнення передатного механізму

«лояльність - показники - індекс безпеки»

Показник KPI_i	Вага w_iу індексі S	Нормувальний коефіцієнт g_i	Оцінена еластичність α_i	Частковий внесок у β: $w_i g_i \alpha_i$	Інтерпретація впливу зростання L
Добровільна плинність персоналу	$w_{\text{плин}}$	$g_{\text{плин}} < 0$	$\alpha_{\text{плин}} < 0$	додатний	Підвищення лояльності знижує плинність, що поліпшує безпеку
Частота інцидентів охорони праці	$w_{\text{інц}}$	$g_{\text{інц}} < 0$	$\alpha_{\text{інц}} < 0$	додатний	Лояльні працівники рідше порушують правила безпеки
Частка браку	$w_{\text{брак}}$	$g_{\text{брак}} < 0$	$\alpha_{\text{брак}} < 0$	додатний	Зростання лояльності зменшує брак, підвищуючи стійкість
Операційна маржа	$w_{\text{маржа}}$	$g_{\text{маржа}} > 0$	$\alpha_{\text{маржа}} > 0$	додатний	Вища лояльність сприяє кращим фінансовим результатам
Частота інцидентів інформаційної безпеки	$w_{\text{ІБ}}$	$g_{\text{ІБ}} < 0$	$\alpha_{\text{ІБ}} < 0$	додатний	Лояльність зменшує ризик "людського фактора" в ІБ

Джерело: розроблено автором

У таблиці 3.4 видно, що для більшості "ризикових" показників, де "менше - краще", еластичність α_i має негативний знак, а коефіцієнт нормування g_i також негативний. Це означає, що добуток $g_i\alpha_i$ є додатним, і, з урахуванням додатних ваг w_i, загальний внесок у β буде додатним. Тобто підвищення лояльності в типових випадках пов'язане із зростанням інтегрального індексу економічної безпеки.

Базова оцінка сценаріїв зміни індексу безпеки. Для практичного застосування моделі необхідно перейти від диференціальної характеристики $\beta = \partial S / \partial L$ до наближеної оцінки зміни індексу безпеки S за наявності конкретного сценарію зміни лояльності ΔL. Якщо розглядати відносно невеликі зміни лояльності і припускати, що β у відповідному діапазоні значень L залишається сталою, можна застосувати лінійне наближення:

$$S' = S_0 + \beta \cdot \Delta L, \qquad (3.24)$$

де S_0 базове значення індексу економічної безпеки у вихідному періоді, S' змодельоване значення індексу за умов зміни лояльності на ΔL.

Якщо ж зміни лояльності є більшими або якщо підприємство вже знаходиться у верхньому сегменті шкали S, доцільно враховувати ефекти насичення. У такому разі може використовуватися модифікована формула:

$$S' = S_0 + \beta \cdot \Delta L \cdot (1 - \gamma S_0), \qquad (3.25)$$

де $\gamma \in [0; 1]$ параметр, що "гасить" приріст у міру наближення S_0 до максимального значення 1. При високих значеннях S_0 множник $(1 - \gamma S_0)$ зменшує ефективний приріст, відображаючи той факт, що подальше підвищення безпеки є дедалі дорожчим і менш відчутним. Аналогічно, можна задавати різні значення βдля різних зон шкали (критична, вразлива, задовільна, висока), що відображає різну маржинальну віддачу від підвищення лояльності: у кризових ситуаціях навіть невелике зростання

лояльності може давати значний ефект, тоді як у стабільних системах цей ефект є більш помірним.

Таким чином, математичний механізм інтеграції результатів оцінювання лояльності в індекс економічної безпеки забезпечує формальний, відтворюваний і прозорий зв’язок між "м’якими" соціально-психологічними характеристиками персоналу та "жорсткими" фінансовими, операційними і ризиковими метриками. Завдяки використанню передатної функції, агрегованої чутливості β та сценарних розрахунків S' система управління отримує можливість планувати і кількісно оцінювати очікуваний ефект програм підвищення лояльності на інтегральний рівень економічної безпеки промислового підприємства.

Калібрування чутливості здійснюється на панельних даних декількох років з контролем зовнішніх факторів, зокрема цін на енергоносії, логістичних обмежень і подійних шоків. Для уникнення зміщення застосовуються робастні оцінювачі, перевіряється стабільність параметрів у підвибірках та роках, а також проводиться крос перевірка на відкладених даних. Отримані коефіцієнти коригуються у нормовану шкалу індексів, щоб зміни лояльності коректно проєктувалися у зміни безпеки. За потреби вводяться нелінійності, наприклад насичення ефекту у верхній частині шкали або диференційовані чутливості у вразливих і задовільних зонах, де наявність вузьких місць у процесах зумовлює більшу маржинальну віддачу від зростання лояльності.

Таблиця 3.5 відображає сценарну зміну індексу економічної безпеки S для вибірки промислових підприємств за трьома моделями впливу факторів та загроз, пов’язаних із персоналом. Базовим рівнем для порівняння виступає значення S за 2024 рік, розраховане за даними таблиці 2.5. Далі виконано моделювання трьох станів: S_1 характеризує зміну S під дією специфічних внутрішніх загроз, ідентифікованих у колонці 2 таблиці 2.9; S_2 характеризує зміну S під дією специфічних зовнішніх загроз із колонки 3

таблиці 2.9; S_3 відображає сумарний ефект одночасної дії внутрішніх і зовнішніх загроз, узагальнених у таблиці 2.8. Таким чином, таблиця 3.5 дає змогу простежити чутливість економічної безпеки підприємств до різних конфігурацій ризикового впливу та порівняти, як змінюється стан безпеки за умов домінування внутрішніх чинників, зовнішніх чинників або їх комбінованого впливу.

Таблиця 3.5

Симуляція змін індексу економічної безпеки промислових підприємств S під впливом факторів, спричинених персоналом

Назва підприємства	S (2024)	S_1 (внутрішні)	S_2 (зовнішні)	S_3 (спільний вплив)
АТ «Укрзалізниця»	Вразлива (0,58)	Вразлива (0,53)	Вразлива (0,51)	Критична (0,46)
ПрАТ «НЕК “Укренерго”»	Критична (0,30)	Критична (0,25)	Критична (0,23)	Критична (0,18)
АТ «Укргідроенерго»	Вразлива (0,55)	Вразлива (0,50)	Критична (0,48)	Критична (0,43)
АТ «Укрнафта»	Задовільна (0,75)	Задовільна (0,70)	Задовільна (0,68)	Вразлива (0,63)
ПАТ «Центренерго»	Критична (0,28)	Критична (0,23)	Критична (0,21)	Критична (0,16)
ПАТ «Сумихімпром»	Критична (0,38)	Критична (0,33)	Критична (0,31)	Критична (0,26)
АТ «Дніпроазот»	Вразлива (0,55)	Вразлива (0,50)	Критична (0,48)	Критична (0,43)
ПрАТ «Полтавський ГЗК» (Ferrexpo)	Задовільна (0,70)	Задовільна (0,65)	Вразлива (0,63)	Вразлива (0,58)
ПАТ «АрселорМіттал Кривий Ріг»	Вразлива (0,58)	Вразлива (0,53)	Вразлива (0,51)	Критична (0,46)
АТ «Запоріжсталь»	Задовільна (0,76)	Задовільна (0,71)	Задовільна (0,69)	Вразлива (0,64)

Джерело: розроблено автором

Отримані значення S_1-S_3 інтерпретуються як прогнозно-аналітичні оцінки, сформовані шляхом коригування базового індексу S на величину сценарного зниження, що відповідає інтенсивності та характеру загроз. Логіка перерахунку полягає в тому, що загрози, пов’язані з персоналом, знижують стійкість підприємства через погіршення виконання процедур, зростання ймовірності інцидентів, порушення дисципліни процесів і виникнення комплаєнс-відхилень. У результаті S може переходити в іншу категорію стану економічної безпеки, що фіксується як кількісно (значення індексу), так і якісно (класифікаційна зона за шкалою).

АТ «Укрзалізниця». Базовий стан економічної безпеки у 2024 році є вразливим (S=0,58). Під впливом специфічних внутрішніх загроз (S_1=0,53) відбувається погіршення в межах тієї самої зони, що свідчить про чутливість підприємства до внутрішніх чинників персоналу, але без негайного переходу в критичний стан. За сценарієм зовнішніх загроз (S_2=0,51) стан також погіршується і наближається до межі критичної зони, що означає посилення ризиків, пов'язаних із зовнішнім середовищем і його впливом на поведінкові та операційні процеси. За сумарного впливу всіх внутрішніх і зовнішніх загроз (S_3=0,46) підприємство переходить у критичний стан, тобто комбінована дія загроз створює якісно новий рівень ризику і потребує посиленого режиму управління безпекою.

ПрАТ «НЕК "Укренерго"». Початковий стан економічної безпеки є критичним (S=0,30), що вказує на високий рівень загроз і обмежену стійкість системи. За внутрішніми загрозами (S_1=0,25) відбувається подальше погіршення в межах критичної зони, що демонструє домінування внутрішніх ризиків та обмеженість компенсаторних механізмів. За зовнішніми загрозами (S_2=0,23) негативна динаміка посилюється, що відображає додаткову вразливість до факторів середовища. За спільного впливу загроз (S_3=0,18) формується найгірший сценарій, за якого підприємство входить у нижній сегмент критичної зони, а пріоритетом стають антикризове управління, жорстка ескалація ризиків і стабілізаційні інтервенції.

АТ «Укргідроенерго». Базовий стан є вразливим (S=0,55), тобто підприємство функціонує із суттєвими ризиками, однак зберігає певний запас стійкості. За внутрішнім сценарієм (S_1=0,50) показник знижується до межі критичного стану, що сигналізує про високий вплив внутрішніх загроз, зокрема тих, що пов'язані з персоналом і виконанням регламентів. За зовнішнім сценарієм (S_2=0,48) підприємство вже переходить у критичну зону, отже зовнішні фактори мають сильніший руйнівний ефект, ніж

внутрішні, і потребують окремого контуру управління. Сумарний вплив (S_3=0,43) закріплює критичний стан і поглиблює його, що означає необхідність комплексного пакета заходів з одночасною роботою із внутрішніми й зовнішніми ризиками.

АТ «Укрнафта». Базовий стан економічної безпеки є задовільним (S=0,75), що відображає відносно стабільну позицію та наявність механізмів стримування ризиків. За сценарієм внутрішніх загроз (S_1=0,70) підприємство зберігає задовільний стан, хоча відбувається помітне погіршення, яке може зменшувати запас стійкості при тривалому впливі. За зовнішніх загроз (S_2=0,68) також зберігається задовільний стан, однак зниження є більш відчутним і підвищує ймовірність переходу до вразливої зони за посилення зовнішнього тиску. За спільного впливу (S_3=0,63) підприємство переходить у вразливий стан, тобто комбінований тиск загроз має критичний для статусу ефект і потребує розширення превентивних механізмів.

ПАТ «Центренерго». Базовий стан є критичним (S=0,28), що свідчить про істотну нестабільність і високу ризик-експозицію. За внутрішніми загрозами (S_1=0,23) відбувається подальше погіршення в критичній зоні, що відображає недостатність внутрішніх бар'єрів безпеки. За зовнішніми загрозами (S_2=0,21) негативна динаміка посилюється, а спільний вплив (S_3=0,16) формує найбільш проблемний стан, який потребує невідкладних стабілізаційних управлінських рішень, посилення контролю та перегляду критичних процесів.

ПАТ «Сумихімпром». Початковий стан є критичним (S=0,38), але ближчим до верхньої межі критичної зони, що означає потенціал для стабілізації за умови належних заходів. За внутрішнім сценарієм (S_1=0,33) стан погіршується, залишаючись критичним, отже внутрішні загрози суттєво знижують рівень безпеки. За зовнішнім сценарієм (S_2=0,31) погіршення є додатковим, що вказує на значний вплив зовнішніх факторів.

За сумарного впливу (S_3=0,26) підприємство віддаляється від межі виходу з критичної зони, що підкреслює потребу одночасної роботи над внутрішніми причинами ризиків і над зменшенням зовнішньої вразливості.

АТ «Дніпроазот». Базовий стан є вразливим (S=0,55). За внутрішніх загроз (S_1=0,50) підприємство знижується до порогового значення, що означає майже критичний рівень та залежність від внутрішньої керованості персоналом. За зовнішніх загроз (S_2=0,48) відбувається перехід у критичну зону, тобто зовнішні ризики для підприємства є більш руйнівними, ніж внутрішні. За сумарного впливу (S_3=0,43) критичний стан поглиблюється, що потребує комплексної програми стабілізації і підсилення процедур безпеки.

ПрАТ «Полтавський ГЗК» (Ferrexpo). Базовий стан є задовільним (S=0,70). За внутрішніх загроз (S_1=0,65) підприємство зберігає задовільний стан, але опиняється на його нижній межі, що свідчить про відчутний вплив внутрішніх ризиків і необхідність підтримки лояльності та дисципліни процесів. За зовнішніх загроз (S_2=0,63) підприємство переходить у вразливий стан, отже зовнішні чинники мають вирішальніший вплив на зміну статусу економічної безпеки. За сумарного впливу (S_3=0,58) підприємство залишається у вразливій зоні, але з погіршенням, що означає зменшення запасу стійкості та зростання потреби в інтегрованих інтервенціях.

ПАТ «АрселорМіттал Кривий Ріг». Базовий стан є вразливим (S=0,58). За внутрішніх загроз (S_1=0,53) погіршення відбувається в межах вразливої зони, що свідчить про значну, але не критичну чутливість до внутрішніх ризиків. За зовнішніх загроз (S_2=0,51) показник наближається до межі критичної зони, що підкреслює важливість зовнішніх факторів. За сумарного впливу (S_3=0,46) підприємство переходить у критичний стан, тобто комбінована дія загроз створює системний ефект та потребує посиленого управління економічною безпекою.

АТ «Запоріжсталь». Базовий стан є задовільним (S=0,76). За внутрішніх загроз (S_1=0,71) підприємство зберігає задовільний стан, демонструючи достатній запас стійкості, хоча індекс знижується. За зовнішніх загроз (S_2=0,69) стан також залишається задовільним, але з більшим падінням, що робить систему більш чутливою до змін середовища. За сумарного впливу (S_3=0,64) підприємство переходить у вразливий стан, тобто одночасна дія внутрішніх і зовнішніх загроз є вирішальною для зміни статусу і вимагає комплексного набору превентивних та коригувальних заходів.

У більшості підприємств сценарії S_1 і S_2 спричиняють зниження індексу S без негайної зміни якісної зони, однак помітно скорочують запас стійкості, наближаючи показники до порогів переходу. Найсильніший ефект має комбінований сценарій S_3, який у частини підприємств переводить стан економічної безпеки в гіршу категорію: «Укрзалізниця» та «АрселорМіттал Кривий Ріг» переходять із вразливої в критичну, «Укрнафта» та «Запоріжсталь» із задовільної у вразливу. «Укргідроенерго» і «Дніпроазот» демонструють перехід у критичну зону вже за зовнішніх загроз (S_2), що вказує на високу чутливість до факторів середовища. Найпроблемнішими залишаються «НЕК “Укренерго”», «Центренерго» та «Сумихімпром», які перебувають у критичній зоні за всіма сценаріями, причому S_3 додатково поглиблює кризовий рівень. Загалом результати підтверджують, що сумарний вплив внутрішніх і зовнішніх загроз має нелінійний, підсилювальний ефект і є вирішальним для переходу підприємств у більш ризикові стани.

Більш детально процесна архітектура моделі інтеграції результатів оцінювання лояльності в управління загрозами економічній безпеці представлена у п.3.2 дисертації. Етичні, правові та організаційні аспекти використання результатів оцінювання лояльності персоналу більш детально представлені у п. 3.3 дисертації.

У підсумку модель формує відтворюваний контур управління, де валідоване вимірювання лояльності поєднується з формалізованим передатним механізмом у процесні та фінансові показники, пороговою інтерпретацією індексу безпеки і регламентованими управлінськими діями. Архітектура замкнуто поєднує моніторинг, аналіз, рішення і навчання, що забезпечує зниження частоти інцидентів, стабілізацію випуску та зростання резилієнтності промислового підприємства в умовах високої невизначеності. На практиці невелике, але стале підвищення лояльності, зафіксоване системою регулярних вимірювань, здатне змістити індекс економічної безпеки на достатню величину для переходу у вищу категорію ризику. Це відкриває можливості для кращих умов фінансування, зниження регуляторного тиску та підвищення довіри стейкхолдерів, що у сукупності створює довготривалий ефект посилення стійкості та вартості бізнесу.

Отже, запропонована модель забезпечує кероване вбудовування результатів оцінювання лояльності у систему управління загрозами економічній безпеці промислового підприємства. Вона поєднує валідовані інструменти вимірювання лояльності, формалізований передатний механізм до процесних і фінансових показників, інтегрований індекс економічної безпеки і чіткі управлінські тригери. Процесна архітектура моделі закриває цикл від моніторингу до дії та навчання, що дозволяє зменшувати частоту інцидентів, стабілізувати випуск і підвищувати стійкість підприємства. Інституціоналізація моделі через політики, ролі, дані та регламенти створює довгострокову основу для зростання економічної безпеки за умов високої невизначеності.

3.2. Процесна архітектура моделі інтеграції результатів оцінювання лояльності в систему забезпечення економічної безпеки промислового підприємства

Процесна архітектура моделі інтеграції результатів оцінювання лояльності персоналу в систему забезпечення економічної безпеки промислового підприємства, представлена у п.3.1 дисертації (далі - Модель) описує, як саме результати оцінювання лояльності персоналу перетворюються на управлінські рішення, що впливають на індекс економічної безпеки підприємства. Вона поєднує дані, ролі, регламенти, цикли перегляду показників та механізми зворотного зв'язку. Якщо математичний блок моделі відповідає на запитання "скільки" і "наскільки", то процесна архітектура пояснює "як", "хто" і "коли". У цьому контексті оцінювання лояльності персоналу розглядається не як разова діагностична процедура, а як елемент безперервного циклу управління ризиками економічної безпеки, який включає моніторинг, аналіз, ухвалення рішень, реалізацію заходів і повторну оцінку ефектів.

Цикл управління: етапи та логіка проходження даних. Цикл управління інтеграцією результатів оцінювання лояльності в систему економічної безпеки складається з послідовності етапів, кожен з яких має власні вхідні та вихідні дані, відповідальних осіб і регламент виконання (рис. 3.2). Йдеться про замкнений контур, у якому інформація про лояльність не накопичується у вигляді ізольованих звітів, а системно впливає на карти ризиків, реєстр загроз і програмні дії.

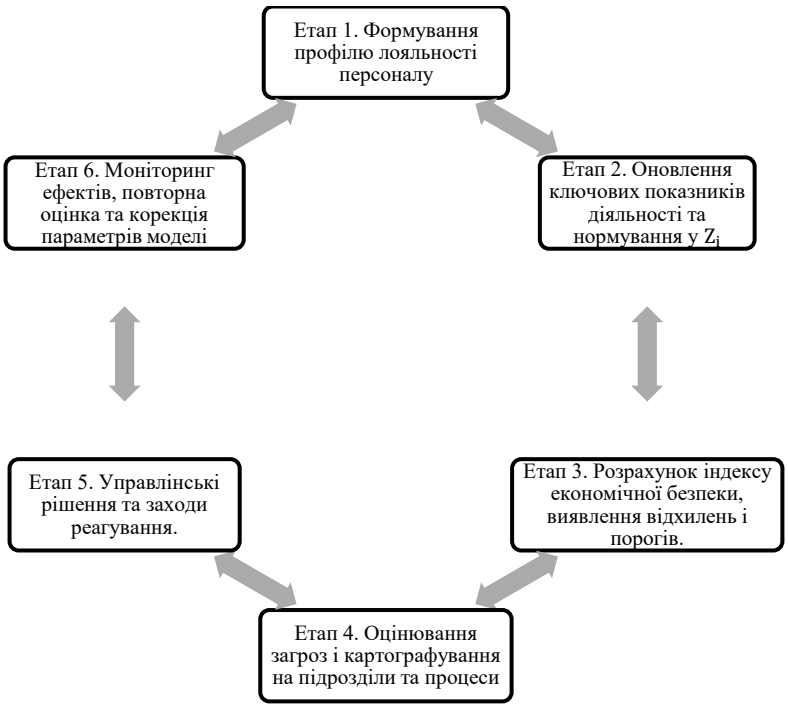

Рис. 3.2. Основні етапи циклу управління інтеграцією результатів оцінювання лояльності в систему економічної безпеки

Джерело: розроблено автором

Етап 1. Формування профілю лояльності персоналу. На першому етапі здійснюється багатоканальне збирання даних про лояльність. До нього входять періодичні повні опитування, короткі "пульсові" хвилі, які дають змогу відстежувати динаміку настроїв, а також аналіз вторинних джерел. Такі джерела включають показники плинності, дані про незаплановані звільнення, внутрішні звернення до HR-служби, скарги, результати оціночних інтерв'ю, дані про участь у навчанні та проєктах, відгуки у внутрішніх комунікаційних системах. Важливим принципом є триангуляція даних, коли для формування індексу лояльності поєднуються щонайменше два типи джерел – опитувальні індикатори та поведінкові метрики. Результатом етапу є оновлений профіль лояльності у розрізі підприємства загалом, окремих підрозділів, категорій посад і критичних ролей.

Етап 2. Оновлення ключових показників діяльності та нормування у Z_i. Другий етап передбачає оновлення ключових показників діяльності, що

входять до структури індексу економічної безпеки. На основі фактичних даних бухгалтерського та управлінського обліку, систем управління виробництвом та охороною праці, кадрових систем формуються оновлені значення показників: плинність персоналу, частота простоїв, частка браку, частота інцидентів охорони праці, показники операційної маржі, виконання ковенантів, частота інцидентів інформаційної безпеки, тощо. Далі ці сирі значення переводяться у нормовані компоненти Z_iза заздалегідь визначеними шкалами. Нормування фіксується у "паспорті показників" з чітким описом формул, референтних меж і логіки "більше - краще" або "менше - краще". Цей етап забезпечує порівнюваність показників і дає змогу інтегрувати їх в єдиний індекс.

Етап 3. Розрахунок індексу економічної безпеки, виявлення відхилень і порогів. На третьому етапі обчислюється інтегральний індекс економічної безпеки S на основі оновлених нормованих компонентів Z_i та ваг w_i. Паралельно розраховуються субіндекси за блоками ризиків, наприклад: кадровий, операційний, фінансовий, інформаційно-безпековий, юридично-комплаєнсний. Отримані значення порівнюються з установленими порогами, які відповідають управлінським режимам: критичний, вразливий, задовільний, високий рівень безпеки. Виявляються відхилення від цільових значень, тенденції до погіршення або покращення, а також "зони напруження", де високий рівень лояльності не конвертується у покращення показників, або навпаки – зниження лояльності супроводжується погіршенням ключових метрик.

Етап 4. Оцінювання загроз і картографування на підрозділи та процеси. Четвертий етап полягає в інтеграції результатів індексних розрахунків у реєстр ризиків і карти загроз. Для кожного підрозділу, цеху, виробничого майданчика або бізнес-процесу визначаються поєднання "рівень лояльності – рівень безпеки". Наприклад, високий рівень лояльності при критичному стані економічної безпеки може сигналізувати про

структурні зовнішні ризики, тоді як низька лояльність на тлі вразливої або задовільної безпеки вказує на посилення внутрішніх загроз, пов'язаних з людським фактором. Такі комбінації позначаються на карті ризиків кольоровими зонами та рівнем пріоритету реагування. На цьому етапі також аналізуються специфічні сценарії: ризики саботажу, витоку інформації, невиконання критичних процедур безпеки, зростання ймовірності кадрових провалів у вузлових компетенціях.

Етап 5. Управлінські рішення та заходи реагування. П'ятий етап є центральним з точки зору практичного управління. На основі виявлених загроз формуються набори заходів, які з одного боку орієнтовані на підвищення лояльності, а з іншого – безпосередньо зменшують ризики та підсилюють економічну безпеку. До таких заходів належать: програми утримання та розвитку критичних компетенцій, зміна режимів роботи та конфігурації змін для зниження перевтоми, посилення контролю якості на ділянках з високою імовірністю браку, посилення процедур охорони праці, адаптація графіків роботи під групи підвищеного ризику, програми наставництва, модернізація систем внутрішніх комунікацій та підтримки, запуск цільових програм мотивації. Рішення можуть бути як тактичними (швидкі кроки в межах одного кварталу), так і стратегічними (перегляд кадрової політики, зміна підходів до управління змінами, модернізація HR-аналітики).

Етап 6. Моніторинг ефектів, повторна оцінка та корекція параметрів моделі. Заключний етап замкненого циклу передбачає оцінювання ефективності впроваджених заходів. Через певний період (наприклад, квартал або півріччя) знову здійснюються "пульсові" вимірювання лояльності, оновлюються показники діяльності, повторно обчислюється індекс економічної безпеки. Порівняння з попередніми значеннями дає змогу оцінити фактичний вплив інтервенцій. На основі отриманих даних коригуються ваги w_i, при потребі уточнюється структура

індексу, переглядаються порогові значення та переоцінюється агрегована чутливість β. Такий підхід забезпечує навчання системи управління на основі власного досвіду, підвищує точність моделей і зменшує ризик формальної "паперової" відповідності.

Для узагальнення логіки циклу управління доцільно представити його у вигляді таблиці 3.6.

У процесному вимірі наведений цикл формує "контур керованого впливу", в якому лояльність не розглядається як абстрактна категорія, а інтегрується в процедури і механізми управління економічною безпекою.

Регламенти та ролі в системі інтеграції лояльності і безпеки. Другим ключовим блоком процесної архітектури є розподіл ролей і формалізація регламентів. Без чітко визначених відповідальностей навіть добре налаштована модель ризикує залишитися інструментом для звітності, а не практичним засобом управління. Рольовий контур повинен забезпечувати прозорий ланцюг "дані - аналіз - рішення - дії - контроль".

Таблиця 3.6

Цикл інтеграції результатів оцінювання лояльності в забезпечення економічної безпеки промислових підприємств

Етап	Зміст етапу	Основні вхідні дані	Основний результат
1	Формування профілю лояльності	Опитування, поведінкові дані, HR-записи	Індекс лояльності у розрізі сегментів
2	Оновлення показників і нормування у Z_i	Бухгалтерські, виробничі, ризик-метрики	Нормовані компоненти Z_i
3	Розрахунок індексу безпеки, виявлення порогів	Набір Z_i, ваги w_i	Значення S та субіндексів
4	Оцінювання загроз, картографування на підрозділи	Індекс лояльності, індекс безпеки, карти процесів	Оновлена карта ризиків, реєстр загроз
5	Прийняття рішень і реалізація заходів	Карта ризиків, аналітика, пріоритети підприємства	План дій, реалізовані інтервенції
6	Моніторинг ефектів, переоцінка параметрів, корекція моделі	Оновлені дані, порівняння періодів, показники ефекту	Скориговані ваги, пороги, параметр β

Джерело: розроблено автором

У моделі виділяються щонайменше чотири базові ролі.

Роль 1. Власник даних з управління персоналом (HR Data Owner). Власник даних управління персоналом відповідає за коректність, повноту та законність використання інформації про працівників. До його функцій належать: контроль за актуальністю довідників, правильністю відображення кадрових подій у системах, дотримання вимог законодавства і внутрішніх політик щодо захисту персональних даних, забезпечення анонімізації та агрегування опитувальних результатів, організація процедур отримання інформованої згоди працівників на обробку даних. Ця роль забезпечує довіру до вихідних даних і запобігає використанню інструментів оцінювання лояльності як засобу неетичного контролю.

Роль 2. Аналітик з економічної безпеки або ризик-аналітик. Аналітик безпеки відповідає за технічну частину моделі: побудову та підтримку індексів, нормування показників, валідацію розрахунків, аналіз чутливості, підготовку аналітичних звітів для управлінських рішень. Він розробляє та веде паспорт показників, адмініструє схему ваг, контролює якість даних після завантаження з різних джерел, проводить калібрування зв'язку між індексом лояльності та індексом економічної безпеки. Аналітик також відповідає за дотримання принципів прозорості: усі формули, параметри і зміни до моделі мають бути задокументовані і доступні для аудиту.

Роль 3. Власник ризику на рівні підрозділу. Власник ризику у підрозділі – керівник структурної одиниці, який безпосередньо відповідає за реалізацію планів заходів та закриття ідентифікованих інцидентів. Саме він інтерпретує результати оцінювання лояльності та індексу безпеки в контексті конкретного виробничого або функціонального процесу, визначає пріоритети втручання, розробляє і впроваджує коригувальні заходи, організовує додаткове навчання, змінює розподіл навантаження, удосконалює внутрішні комунікації. Власник ризику також зобов'язаний фіксувати виконані дії і їх ефект у системі, що забезпечує замикання циклу зворотного зв'язку.

Роль 4. Комітет з економічної безпеки або міжфункціональний координаційний орган. Комітет з економічної безпеки виконує функцію колективного органу, що приймає ключові рішення за результатами аналізу індексів, оцінює відповідність рівня ризиків апетиту до ризику підприємства, встановлює та переглядає порогові значення, затверджує зміни у ваговій структурі індексу, погоджує стратегічні програми розвитку персоналу, що впливають на лояльність і безпеку. До складу комітету зазвичай входять представники вищого керівництва, служби економічної безпеки, HR, фінансового підрозділу, виробничих дирекцій та, за можливості, внутрішнього аудиту. Комітет контролює відтворюваність моделі, розглядає результати валідації та періодично ініціює зовнішній або внутрішній аудит підходів.

Для систематизації ролей доцільно подати їх у вигляді узагальнюючої таблиці 3.7.

Таблиця 3.7

Ролі та основні зони відповідальності в моделі інтеграції лояльності в забезпечення економічної безпеки промислових підприємств

Роль	Основні функції	Ключові продукти діяльності
Власник даних HR	Якість і законність даних, анонімізація, управління доступом	Бази даних, паспорти джерел, регламенти обробки даних
Аналітик безпеки	Нормування, побудова індексів, аналітика, валідація	Розрахунок L, Z_i, S, аналітичні звіти
Власник ризику в підрозділі	Інтерпретація результатів, планування і виконання дій	Плани заходів, звіти про виконання, оновлені карти ризиків
Комітет з економічної безпеки	Стратегічні рішення, затвердження порогів і ваг, контроль	Протоколи рішень, оновлені політики, пріоритети програм

Джерело: розроблено автором

За необхідності Модель може бути доповнена іншими ролями, наприклад, представником юридичної служби, представником служби інформаційної безпеки, представником профспілки або представником від працівників. Таке розширення посилює легітимність прийнятих рішень і зменшує ризик того, що інструменти оцінювання лояльності будуть

сприйняті персоналом як односторонній контроль, а не як елемент двостороннього партнерства.

Узгоджена процесна архітектура, яка поєднує чіткий цикл управління та прозорий розподіл ролей, забезпечує практичну реалізованість усієї моделі інтеграції результатів оцінювання лояльності в систему управління загрозами економічній безпеці промислового підприємства. Вона перетворює індекси і показники з "абстрактних чисел" на інструмент, що безпосередньо керує діями, розподілом ресурсів і пріоритетами управлінських рішень.

Реєстр загроз з боку персоналу та ключові індикатори ризику. Реєстр загроз з боку персоналу є центральним елементом моделі інтеграції оцінювання лояльності в систему управління загрозами економічній безпеці промислового підприємства. У цьому реєстрі системно фіксуються всі релевантні ризики, що виникають через поведінку, мотивацію, компетентності та стан працівників, а також зовнішні впливи, які реалізуються через персонал. Реєстр поєднує опис загрози, її джерело, можливі сценарії реалізації, відповідальні підрозділи, пов’язані показники та тригери активації управлінських дій. На його основі формується панель ключових індикаторів ризику, яка дозволяє виявляти ранні сигнали погіршення ситуації та пов’язувати їх із динамікою лояльності персоналу.

Внутрішні загрози економічній безпеці з боку персоналу. Внутрішні загрози пов’язані з прямою або опосередкованою поведінкою працівників, що впливає на безперервність операцій, якість продукції, фінансовий результат та репутацію підприємства. Вони включають як ненавмисні помилки, зумовлені перевантаженням, втомою або низькою залученістю, так і свідомі порушення, що можуть мати характер саботажу чи зловживань.

До ключових груп внутрішніх загроз належать:

1. *Зниження дисципліни безпеки та порушення процедур.* Йдеться про систематичне недотримання встановлених регламентів з охорони праці,

техніки безпеки, операційних інструкцій, процедур технічного обслуговування та ремонту обладнання, правил допуску до робіт підвищеної небезпеки. Низький рівень лояльності і довіри до керівництва часто посилює готовність персоналу ігнорувати формальні вимоги, особливо якщо працівники не бачать реального зв'язку між правилами та власною безпекою і добробутом. Це може призводити до зростання частоти виробничих інцидентів, аварій, пошкодження основних фондів, зупинок агрегатів, штрафів з боку наглядових органів.

2. *Помилки у роботі з критичним обладнанням та технологічними вузлами.* У критичних виробничих процесах навіть одноразова помилка оператора може спричинити значні економічні втрати, порушення екологічних норм або загрозу життю та здоров'ю працівників. Ризик цих помилок зростає за умов емоційного вигорання, високої плинності персоналу, незаповнених вакансій у ключових ролях, недостатнього навчання або відсутності системи наставництва. Лояльність у цьому контексті впливає на готовність працівників дотримуватися стандартів, вчасно повідомляти про несправності, ініціювати превентивні дії, а також брати участь у програмах підвищення кваліфікації.
3. *Витік інформації та порушення режиму конфіденційності.* Низька лояльність поєднана з відсутністю чіткої культури інформаційної безпеки створює підвищену імовірність несанкціонованого передання даних третім особам, неформального обміну конфіденційною інформацією, використання особистих пристроїв і неконтрольованих каналів комунікації для роботи з критичною інформацією. Це стосується як комерційних та технологічних секретів, так і внутрішніх фінансових даних, планів ремонтів, маршрутів перевезень, схем енергопостачання. Витік може бути як навмисним, так і ненавмисним, проте в обох випадках він підриває економічну безпеку.

4. *Зрив змін і операцій через некомплект персоналу та неузгодженість графіків.* Формально цей ризик може виглядати як проблема планування, але в реальності він часто пов’язаний з мотивацією, ставленням до підприємства, готовністю залишатися в організації за складних умов. Низька лояльність посилює ризик неявок, запізнень, відмови виходити на додаткові зміни у кризові періоди, формує фонову напруженість у колективі. У промислових підприємствах зі складними технологічними ланцюгами зрив навіть однієї зміни здатен запускати каскад операційних та фінансових наслідків.
5. *Крайні форми внутрішніх загроз, включно із саботажем.* За умов високого стресу, конфліктів із керівництвом, нерозв’язаних трудових спорів або цілеспрямованого зовнішнього впливу окремі працівники можуть свідомо завдавати шкоди підприємству. Це може проявлятися в умисному пошкодженні обладнання, свідомому порушенні процедур, блокуванні інформаційних систем, організації неформальних протестних акцій, створенні конфліктів між змінами. Хоча такі випадки зустрічаються рідко, їхній потенційний вплив на економічну безпеку є надзвичайно високим, тому вони мають бути окремо відображені в реєстрі загроз.

Для систематизації внутрішніх загроз доцільно використовувати узагальнену структуру, наведену в таблиці 3.8.

Зовнішні загрози, що реалізуються через персонал. Зовнішні загрози економічній безпеці можуть реалізовуватися через персонал, якщо зовнішні суб’єкти прямо або опосередковано впливають на працівників, використовуючи їх як канал доступу до інформації, інфраструктури або управлінських рішень. У воєнний та поствоєнний періоди цей контур загроз посилюється через зростання інформаційних атак, соціальної інженерії, психологічного тиску та регуляторної турбулентності.

Таблиця 3.8

Внутрішні загрози економічній безпеці з боку персоналу промислового підприємства

Група загроз	Зміст загрози	Типові наслідки для економічної безпеки	Ключові процеси та зони ризику
Порушення дисципліни безпеки	Ігнорування інструкцій, формальний підхід до процедур	Аварії, травматизм, штрафи, зупинки виробництва	Охорона праці, технічне обслуговування, ремонти
Помилки при роботі з критичним обладнанням	Некоректні дії операторів, неправильні налаштування	Вихід з ладу обладнання, втрати продукції, порушення екологічних норм	Операційні лінії, енергетичні вузли, хімічні цехи
Витік інформації	Несанкціонований обмін даними, робота через неконтрольовані канали	Репутаційні збитки, втрата конкурентних переваг, юридичні претензії	Інформаційні системи, офісні служби, IT інфраструктура
Зрив змін та некомплект	Неявки, запізнення, відмова від додаткових змін	Простої, недовиконання плану, порушення графіків ремонту та постачання	Планування змін, диспетчеризація, логістика
Крайні форми протидії, саботаж	Свідоме завдання шкоди, блокування систем	Масштабні операційні збої, значні фінансові втрати, загроза безперервності діяльності	Критичні виробничі та IT контури

Джерело: розроблено автором

До основних груп зовнішніх загроз через персонал належать:

1. *Цілеспрямована соціальна інженерія.* Йдеться про спроби зовнішніх суб’єктів отримати доступ до критичних систем, комерційної інформації або виробничих даних через маніпуляції працівниками. Типовими інструментами є фішингові листи, підроблені повідомлення від імені партнерів або керівництва, телефонні дзвінки від псевдопредставників державних органів, підроблені сторінки внутрішніх сервісів. Низька лояльність, слабка інформаційна гігієна та відсутність регулярного навчання з інформаційної безпеки підвищують успішність таких атак.
2. *Маніпуляції в соціальних мережах та інформаційний тиск.* Працівники промислових підприємств перебувають в інформаційному просторі, де циркулюють фейкові новини, дезінформація, пропагандистські

повідомлення, які можуть викликати зневіру, страх, агресію або відчуття несправедливості. Це здатне послаблювати довіру до керівництва, провокувати внутрішні конфлікти, сприяти поширенню деструктивних наративів у колективі. За низького рівня внутрішніх комунікацій працівники схильні орієнтуватися на зовнішні джерела інформації, що підсилює вразливість підприємства.

3. *Юридичний, регуляторний та політичний тиск, спрямований на окремих працівників*. Працівники, які займають ключові позиції або мають доступ до чутливих даних, можуть ставати об'єктами персоналізованого тиску, наприклад через судові позови, вимоги надати відомості, що виходять за рамки закону, спроби використати їх як свідків у конфліктах інтересів. За відсутності чіткої політики підтримки та юридичного супроводу персоналу такі ситуації здатні трансформуватися в реальні загрози витоку інформації, прийняття невигідних рішень або свідомого дистанціювання працівника від відповідальності.
4. *Психологічні наслідки воєнного часу та хронічний стрес.* Воєнні дії, втрата близьких, вимушене переселення, загроза мобілізації, невизначеність майбутнього спричиняють хронічний стрес, тривожність, епізоди емоційного вигорання. За відсутності системної психологічної підтримки та гнучкої політики щодо режиму роботи це може призводити до зниження концентрації, зростання кількості помилок, конфліктів у колективах, прихованого саботажу або різкого падіння лояльності. У результаті зовнішня подія в макросередовищі через стан працівників трансформується у внутрішню загрозу для економічної безпеки підприємства.

Систематизація зовнішніх загроз через персонал наведена в таблиці 3.9.

Таблиця 3.9

Зовнішні загрози, що реалізуються через персонал промислового підприємства

Група загроз	Механізм реалізації через персонал	Потенційні наслідки для економічної безпеки	Критичні групи працівників
Соціальна інженерія	Обман, фішинг, підроблені звернення	Доступ до систем, витік даних, фінансові втрати	Офісний персонал, IT фахівці, диспетчери
Маніпуляції у соціальних мережах	Дезінформація, деструктивні наративи	Зниження довіри, внутрішні конфлікти, падіння лояльності	Усі групи персоналу
Юридичний та регуляторний тиск	Персоналізовані вимоги, позови, неформальний вплив	Невигідні рішення, вимушений витік інформації, репутаційні ризики	Керівники, відповідальні за звітність, юристи
Психологічні наслідки війни	Стрес, травматичний досвід, емоційне виснаження	Зростання помилок, конфлікти, абсентеїзм, підвищений ризик інцидентів	Працівники на небезпечних та відповідальних ділянках

Джерело: розроблено автором

Панель ключових індикаторів ризику як рання система попередження. Ключові індикатори ризику формують "сенсорний шар" моделі, який дає змогу перетворити абстрактні уявлення про загрози на вимірювані сигнали з конкретними порогами та правилами реагування. Панель індикаторів повинна охоплювати як кількісні, так і якісні показники, пов’язані з поведінкою персоналу, станом виробничих процесів та інформаційною безпекою.

До ключових індикаторів ризику, що сигналізують про проростання загроз з боку персоналу, належать:

- різке зростання кількості скарг, конфліктів та негативних звернень до HR служби;
- погіршення тональності внутрішнього зворотного зв’язку у опитуваннях, відкритих коментарях, корпоративних каналах комунікації;
- стрибки абсентеїзму, зростання кількості неявок, запізнень, незапланованих відгулів;

- відхилення у показниках браку продукції, частоти переробок, кількості аварійних зупинок;
- системні збої у дотриманні графіків технічного обслуговування та ремонту, перенесення критичних робіт без належного обґрунтування;
- збільшення кількості порушень правил охорони праці, інцидентів без травм, проте з потенційною небезпекою (так звані "майже аварії");
- зростання кількості інформаційних інцидентів, фіксація підозрілих входів, використання некорпоративних каналів для обміну даними.

Для управління цими індикаторами доцільно застосовувати диференційовані порогові значення і класифікацію за рівнями критичності. Приклад структурованої панелі подано в таблиці 3.10.

Таблиця 3.10

Приклад панелі ключових індикаторів ризику, пов'язаних з персоналом промислового підприємства

Індикатор	Опис індикатора	Джерело даних	Приклад порогів та інтерпретації
Частота скарг та конфліктів	Кількість формальних звернень та зафіксованих конфліктів за період	Система HR звернень, служба безпеки	+30 % до середнього рівня за 3 місяці сигнал про напруження в колективі
Тональність внутрішнього зворотного зв'язку	Частка негативних та нейтральних оцінок у опитуваннях та коментарях	Опитування, контент аналіз	Падіння середнього балу нижче 3,5 з 5 зона ризику комунікацій та довіри
Абсентеїзм	Частка незапланованих неявок та запізнень	Табелі обліку робочого часу, HR система	Перевищення норм на 20 % і більше сигнал про вигорання або протестну поведінку
Показники браку та переробок	Частка продукції, що потребує переробки	Виробнича звітність, система якості	Стійке зростання протягом трьох і більше періодів вказує на проблеми із залученістю або компетенціями
Виконання графіків технічного обслуговування та ремонту	Частка своєчасно виконаних робіт із ТО і ремонту	Система управління ремонтами	Зниження показника нижче 90 % сигнал про зростання операційного ризику
Інциденти з охорони праці	Кількість випадків порушення правил, "майже аварій"	Журнал охорони праці, служба безпеки	Зростання на 25 % і більше вказує на деградацію культури безпеки
Інформаційні інциденти	Кількість спроб несанкціонованого доступу, фішингових атак, підозрілих дій	Система інформаційної безпеки, IT служба	Зростання частоти інцидентів сигнал про вразливість до соціальної інженерії

Джерело: розроблено автором

Суміщення панелі індикаторів з індексом лояльності дозволяє виявляти критичні комбінації, наприклад низька лояльність при одночасному зростанні абсентеїзму, браку та конфліктів у конкретному цеху. Це дає змогу своєчасно ініціювати цільові втручання, перш ніж загрози матеріалізуються в серйозні економічні втрати.

Узагальнюючи, реєстр загроз з боку персоналу та пов’язана з ним панель ключових індикаторів ризику трансформують абстрактні уявлення про "людський чинник" у керовану систему сигналів, що може бути інтегрована в загальний контур управління економічною безпекою промислового підприємства.

Контур прийняття управлінських рішень на основі оцінювання лояльності та ризик індикаторів. Контур прийняття управлінських рішень є тим рівнем моделі, на якому результати оцінювання лояльності персоналу та дані реєстру загроз перетворюються на конкретні дії, плани та програми. Якщо індекс лояльності та ключові індикатори ризику залишаються лише аналітичною інформацією, не інтегрованою в управлінський цикл, їхній ефект для економічної безпеки є обмеженим. Тому завдання цього фрагменту Моделі полягає в описі логіки переходу від сигналів ризику до рішень, встановленні порогів та тригерів, визначенні відповідальних осіб і вписуванні всього контуру у загальну систему управління економічною безпекою промислового підприємства (рис. 3.3).

Логіка переходу від оцінювання до дій. Вихідними параметрами для контуру рішень є, з одного боку, інтегральний індекс лояльності персоналу L з його розподілом за підрозділами, професійними групами, змінами, з іншого боку, інтегральний індекс економічної безпеки S та набір ключових індикаторів ризику, пов’язаних з персоналом. На цьому рівні важливо не лише фіксувати абсолютні значення показників, але й відстежувати їхню динаміку, поєднання та просторовий розподіл по підприємству.

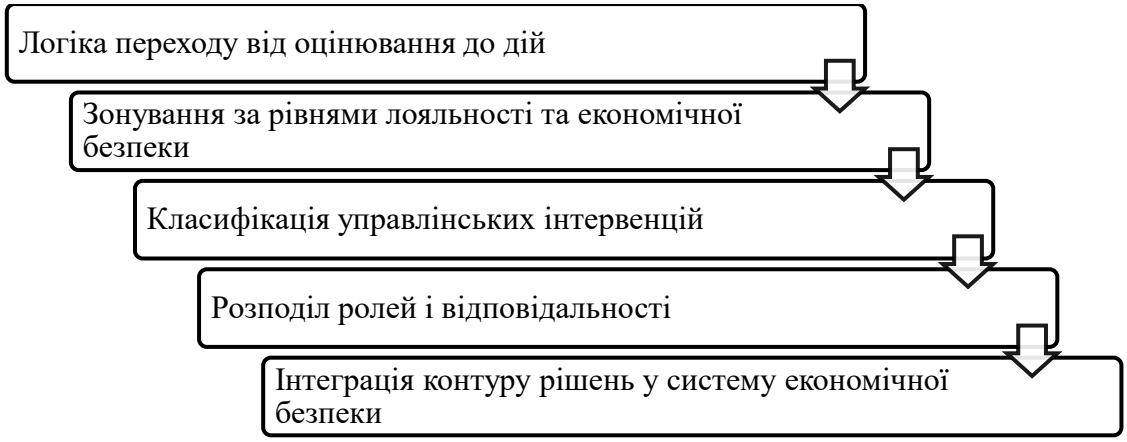

Рис. 3.3. Контур прийняття управлінських рішень на основі оцінювання лояльності та ризик індикаторів

Джерело: розроблено автором

Базова логіка моделі може бути представлена як послідовність кроків: виявлення відхилення показників від цільових значень, інтерпретація цього відхилення у контексті загроз з боку персоналу, вибір типу управлінської відповіді, планування набору конкретних заходів, призначення відповідальних осіб і встановлення термінів, подальший моніторинг ефекту. У такій конфігурації індекс лояльності виконує роль раннього маркера напруження в колективі, а ключові індикатори ризику та індекс S показують, де саме і в якій формі це напруження вже трансформується в операційні та фінансові проблеми.

Зонування за рівнями лояльності та економічної безпеки. Для того щоб перетворити сукупність числових показників на керовану систему рішень, доцільно запровадити шкали і зони ризику. Для індексу лояльності L, нормованого в інтервалі від 0 до 1, можна виділити чотири інтервали: низька лояльність ($L \leq 0{,}40$), вразлива лояльність (0,41-0,60), задовільна лояльність (0,61-0,80) та висока лояльність ($L > 0{,}80$). Аналогічно для індексу економічної безпеки S виділяються зони: критична, вразлива, задовільна та висока.

Комбінації цих зон формують матрицю управлінських режимів. Наприклад, ситуація низької лояльності та критичної економічної безпеки вимагатиме антикризової програми з жорсткими термінами і максимальною концентрацією ресурсів. Ситуація високої лояльності та задовільної чи високої економічної безпеки дає змогу зосередитися на підтримувальних та розвиткових заходах, зокрема на програмах розвитку компетентностей і наступництва. Важливо, що рішення приймаються не лише за сукупним значенням L і S по підприємству, але й за розрізами: цех, зміна, функціональна служба, лінія обладнання.

Для упорядкування рішень доцільно використовувати узагальнений формат матриці, наведений у таблиці 3.11.

Таблиця 3.11

Приклад матриці режимів управління за поєднанням рівнів лояльності та економічної безпеки

Рівень лояльності L	Рівень економічної безпеки S	Тип управлінського режиму	Загальна логіка дій
Низький	Критичний	Антикризова програма	Негайні інтервенції, стабілізація, концентрація ресурсів
	Вразливий	Програма відновлення	Усунення вузьких місць, посилення контролю
Вразливий	Вразливий	Комбінований режим	Паралельна робота з умовами праці та процесами
	Задовільний	Попереджувальні заходи	Профілактика падіння S, зміцнення довіри
Задовільний	Вразливий	Цільові операційні інтервенції	Переналаштування процесів, адресна робота з групами
	Задовільний, високий	Режим точкових поліпшень	Оптимізація, розвиток, посилення залученості
Високий	Задовільний, високий	Режим підтримки та розвитку	Підтримка культури, розвиток компетентностей

Джерело: розроблено автором

Практичне застосування цієї матриці передбачає, що для кожної комбінації L і S наперед визначається базовий набір заходів і стандартний пакет рішень, який потім адаптується до специфіки конкретного підприємства та підрозділу.

Класифікація управлінських інтервенцій. У моделі доцільно розрізняти щонайменше три рівні управлінських інтервенцій: швидкі, середньострокові та структурні. Швидкі інтервенції орієнтовані на негайне зниження напруження та ризику. До них належать, наприклад, коригування графіків змін за рахунок перерозподілу навантаження, оперативні комунікаційні кампанії з поясненням рішень керівництва, тимчасові програми матеріальної підтримки у кризових ситуаціях, посилення контролю за дотриманням процедур безпеки, оперативне реагування на скарги та конфлікти.

Середньострокові інтервенції пов’язані з переналаштуванням HR процесів і практик. Сюди належать програми розвитку лінійних керівників, упровадження або модернізація системи адаптації нових працівників, побудова систем наставництва, перегляд політики винагороди з урахуванням показників лояльності та безпеки, розширення каналів зворотного зв’язку, у тому числі анонімних. Такі заходи змінюють глибинні параметри середовища, але вимагають більше часу та ресурсів.

Структурні інтервенції спрямовані на зміну архітектури системи управління економічною безпекою з урахуванням людського чинника. Вони включають вбудовування показників лояльності та ключових індикаторів ризику, пов’язаних з персоналом, у карти ризиків підприємства, у систему планування та звітності, в моделі преміювання керівників, у регламенти роботи служби економічної безпеки, внутрішнього аудиту та кадрових служб. У такому випадку лояльність перестає бути "м’якою" характеристикою задоволеності і стає повноцінним елементом системи управління ризиками.

Розподіл ролей і відповідальності. Ще однією критичною умовою дієвості контуру рішень є чіткий розподіл ролей і відповідальності. Основними суб’єктами в моделі є вище керівництво підприємства, служба

економічної безпеки, HR підрозділ, керівники виробничих підрозділів, служби охорони праці, IT та служба інформаційної безпеки.

Вище керівництво визначає цільові значення для індикаторів лояльності та економічної безпеки, затверджує порогові значення для переходу між режимами управління, схвалює структурні інтервенції та контролює виконання програм. Служба економічної безпеки відповідає за підтримання реєстру загроз, аналіз панелі індикаторів ризику, координацію дій між підрозділами у випадку перетину порогів ризику та інтеграцію результатів у загальні карти ризиків підприємства.

HR підрозділ відповідає за регулярні вимірювання лояльності, організацію опитувань, інтерпретацію результатів, розроблення програм підтримки та залучення, а також за методичний супровід лінійних керівників. Керівники виробничих підрозділів несуть відповідальність за впровадження узгоджених заходів у своїх підрозділах, у тому числі за коригування графіків, організацію інструктажів, роботу з конфліктами, локальні програми підтримки персоналу у складних умовах.

Служба охорони праці та служба інформаційної безпеки забезпечують специфічні напрямки управління ризиками. Вони використовують дані про лояльність та індикатори ризику для планування превентивних заходів, навчальних програм, аудитів та перевірок, а також для встановлення додаткових контрольних процедур у найбільш вразливих точках.

Для формалізації розподілу ролей може бути використана матриця відповідальності, аналогічна до підходу RACI. У спрощеному вигляді така матриця може бути наведена в таблиці 3.12.

Чітка фіксація ролей знижує ризик ситуації, коли сигнали з панелі індикаторів залишаються без відповіді, оскільки кожний елемент контуру має визначеного власника, а кожний план дій супроводжується конкретними термінами та показниками результату.

Таблиця 3.12

Приклад матриці розподілу ролей у контурі рішень

Ключовий елемент контуру	Вище керівництво	Служба економічної безпеки	HR підрозділ	Керівники підрозділів	Служба охорони праці, інформаційної безпеки
Встановлення цільових значень L і S	Відповідальний	Консультативна роль	Консультативна роль	Консультативна роль	Консультативна роль
Підтримка реєстру загроз	Контроль	Відповідальний	Участь	Участь	Участь
Проведення вимірювань лояльності	Контроль	Консультативна роль	Відповідальний	Участь	Участь
Аналіз індикаторів ризику	Контроль	Відповідальний	Участь	Участь	Відповідальний у своїй сфері
Розроблення програм інтервенцій	Схвалення	Участь	Відповідальний	Участь	Участь
Впровадження заходів у підрозділах	Контроль	Моніторинг	Підтримка	Відповідальний	Підтримка

Джерело: розроблено автором

Інтеграція контуру рішень у систему економічної безпеки. Заключним елементом цього фрагмента моделі є вписування описаного контуру у загальну систему управління економічною безпекою промислового підприємства. Це означає, що дані про лояльність та ризики з боку персоналу повинні бути включені до регулярної звітності служби економічної безпеки, відображені в картах ризиків та матрицях ймовірності і впливу, у планах безперервності діяльності, у внутрішньому аудиті та в системі управління ризиками на рівні ради директорів або наглядової ради.

Узагальнюючи, контур прийняття управлінських рішень на основі результатів оцінювання лояльності та панелі ключових індикаторів ризику забезпечує практичну реалізацію моделі. Він дозволяє перетворити абстрактні оцінки "стану колективу" на конкретні дії, що знижують імовірність матеріалізації загроз з боку персоналу та посилюють здатність підприємства підтримувати прийнятний рівень економічної безпеки у умовах високої невизначеності.

3.3. Етичні, правові та організаційні аспекти використання результатів оцінювання лояльності персоналу для забезпечення економічної безпеки промислового підприємства

Валідація, перевірки стійкості та контроль якості даних є завершальним, але концептуально ключовим виміром моделі інтеграції результатів оцінювання лояльності персоналу в систему управління загрозами економічній безпеці промислового підприємства. Без формалізованих процедур перевірки надійності інструментів, робастності інтегрального індексу економічної безпеки та якості вхідних даних будь-яка, навіть математично витончена модель, перетворюється на джерело додаткової невизначеності для менеджменту. Тому контур валідації виконує функцію "захисного фільтра", який відсіює випадкові коливання, артефакти вимірювання та помилки даних, перш ніж результати будуть використані у процесі прийняття управлінських рішень.

Перший блок стосується надійності інструментів вимірювання лояльності персоналу. Для опитувальних шкал критичним є забезпечення внутрішньої узгодженості, стабільності в часі та відтворюваності результатів у різних хвилях дослідження. Внутрішня узгодженість оцінюється через коефіцієнт Кронбаха α для кожної підшкали лояльності (афективна, нормативна, інструментальна прихильність, поведінкові індикатори). Практичним порогом прийнятності є значення α не нижче 0,70, що свідчить про узгодженість тверджень всередині однієї латентної змінної. Тест–ретест надійність перевіряється шляхом повторного вимірювання вибіркової групи респондентів з інтервалом у кілька тижнів та розрахунку коефіцієнта кореляції між первинними та повторними оцінками індексу лояльності L. Якщо кореляція залишається стабільно високою, а середні значення не демонструють систематичного зсуву, можна вважати, що шкала є стійкою до випадкових коливань. Міжхвильова стабільність шкал

додатково оцінюється через порівняння розподілів індексу L за кілька періодів, з урахуванням зміни зовнішнього контексту. Це дозволяє відокремити реальні тренди у лояльності від змін, що є наслідком модифікації анкети або способу збору даних.

Другий блок охоплює робастність інтегрального індексу економічної безпеки підприємства S як агрегату кількісних та якісних показників. Оскільки S формується на основі нормованих індикаторів з різними вагами, необхідно перевірити, наскільки оцінки є чутливими до варіацій вагових коефіцієнтів, способів нормування та меж шкали інтерпретації. Для цього проводиться серія сенситивіті аналізів: у базовій специфікації, наприклад, співвідношення між кількісною та якісною складовими встановлюється як 0,70 до 0,30, після чого моделюються альтернативні конфігурації (0,60 до 0,40, 0,80 до 0,20) з перерахунком значень S для кожного підприємства. Порівнюються ранги та класифікація підприємств за рівнями "висока", "задовільна", "вразлива", "критична". Якщо при варіації ваг на ±10 відсоткових пунктів більшість підприємств зберігає свою категорію, а середнє відхилення S не перевищує наперед визначеного порогу (наприклад 0,03 пункту шкали), індекс можна вважати робастним до помірних змін у параметрах моделі.

Додатково застосовується бутстреп аналіз за підрозділами або часовими зрізами. Для цього з наявної бази спостережень випадковим чином формуються множинні псевдовибірки, для кожної з яких повторно розраховується індекс S. Отримані розподіли значень дозволяють оцінити довірчі інтервали для S, виявити "нестійкі" підприємства, індекс яких істотно змінюється при невеликій зміні складу даних, а також визначити, чи не є класифікація певних підприємств артефактом конкретної вибірки. Такий підхід особливо важливий для промислових компаній з неоднорідною структурою підрозділів, де локальні аномалії можуть суттєво впливати на загальну оцінку безпеки.

Третій вимір пов’язаний з прогностичною цінністю індексу S як інструменту раннього попередження про загрози економічній безпеці. Цей аспект виходить за межі описової аналітики і переводить модель у площину перевірки того, чи низькі значення S дійсно пов’язані з підвищеною ймовірністю негативних подій у майбутньому. Для цього формується панель даних, де для кожного підприємства фіксуються значення S у момент часу t, а також факти настання критичних подій у горизонті 1–3 квартали: значні простої виробництва, різке зростання плинності кадрів у критичних ролях, серйозні інциденти з охорони праці, суттєві фінансові відхилення, реалізація інформаційних або інсайдерських загроз. Далі будуються регресійні або логістичні моделі, які пов’язують ймовірність настання таких подій з рівнем S та його динамікою. Якщо виявляється статистично значущий зв’язок (наприклад, підприємства з S нижче 0,50 демонструють істотно вищу частоту кризових інцидентів у наступні періоди), індекс отримує підтвердження своєї прогностичної функції. Це дає змогу використовувати S не лише для ретроспективного аналізу, а і як базу для запуску превентивних програм, у тому числі спрямованих на роботу з лояльністю персоналу.

Четвертий блок стосується системного контролю якості даних, на яких базуються як індекс лояльності L, так і інтегральний індекс економічної безпеки S. Якість даних у цьому контексті включає щонайменше чотири виміри: повноту, узгодженість, відсутність дублювань та коректність часової прив’язки. Повнота передбачає, що для кожного підприємства і кожного періоду наявні всі ключові показники, необхідні для обчислення L і S, без систематичних прогалин у певних підрозділах або типах даних. Узгодженість означає використання єдиних довідників (номенклатури підрозділів, посад, типів інцидентів, категорій витрат), однакового формату одиниць виміру та однакових правил агрегування. Відсутність дублювань контролюється за допомогою автоматизованих

перевірок, які виявляють повторні записи щодо одних і тих самих подій або співробітників, що могли бути внесені з різних джерел. Часова коректність передбачає, що події прив’язані до конкретних дат або періодів, а також що не виникають "зсуви" між датами виникнення події, її реєстрації та включення до звітності, які можуть спотворити аналіз динаміки індикаторів.

Для практичної реалізації цих вимог доцільно використовувати стандартизований перелік перевірок, який може бути представлений у вигляді узагальнювальної таблиці 3.13.

Таблиця 3.13

Основні напрями валідації моделі та контролю якості даних

Напрям перевірки	Об’єкт контролю	Приклад процедур	Орієнтовні критерії прийнятності
Надійність інструментів вимірювання	Опитувальні шкали лояльності, індекс L	Розрахунок α Кронбаха, тест–ретест, аналіз розподілів за хвилями	α не нижче 0,70, відсутність систематичного зсуву середніх
Робастність інтегрального індексу S	Ваги, нормування, межі шкали, класифікація	Сенситивіті аналіз, зміна ваг на ±10 п.п., альтернативні схеми нормування, бутстреп	Стабільність ранжування, відхилення S в межах 0,02–0,03
Прогностична цінність	Зв’язок S з подальшими негативними подіями	Регресійні та логістичні моделі, аналіз частоти інцидентів у групах з різним S	Статистично значущі коефіцієнти, вища частота подій у групах з низьким S
Якість даних	Повнота, узгодженість, дублювання, часова прив’язка	Перевірки повноти полів, уніфікація довідників, алгоритми пошуку дублювань, зіставлення дат	Відсутність систематичних прогалин, мінімізація дублювань, коректні часові ряди

Джерело: розроблено автором

Сукупно ці процедури створюють "каркас довіри" до моделі, у межах якого результати інтеграції показників лояльності та індикаторів економічної безпеки можуть використовуватися як обґрунтована основа для управлінських рішень. Надійні та валідовані інструменти вимірювання гарантують, що індекс лояльності L відображає реальний стан ставлень персоналу, а не випадкові або методичні флуктуації. Робастність інтегрального індексу S забезпечує стійкість висновків до змін у параметрах моделі та вибірці даних. Прогностична цінність підтверджує, що низькі

значення S справді асоціюються з підвищеним ризиком кризових подій, отже, ранні сигнали на панелі показників мають практичний сенс. Нарешті, системний контроль якості даних знижує ймовірність того, що управлінські рішення прийматимуться на основі спотвореної або неповної інформації. У підсумку валідаційний контур перетворює модель з абстрактної аналітичної конструкції на відтворюваний, доказовий інструмент управління загрозами економічній безпеці промислового підприємства.

Етичні, правові та організаційні аспекти використання результатів оцінювання лояльності персоналу є критичним елементом моделі управління загрозами економічній безпеці промислового підприємства. Без чітких правил роботи з даними про працівників навіть технічно бездоганна система індикаторів може генерувати зворотний ефект у вигляді зниження довіри, зростання латентної напруги та формування додаткових ризиків, пов’язаних із персоналом. Тому контур етичного, правового та організаційного врегулювання повинен розглядатися як рівнозначний за важливістю елементу вимірювальних інструментів, аналітичних моделей та управлінських рішень.

По-перше, базовою передумовою є дотримання принципів добровільності та поінформованої згоди працівників. Будь-яке опитування щодо лояльності, задоволеності, стану психологічного благополуччя чи готовності залишатися в компанії повинно супроводжуватися чітким поясненням мети, змісту, способів оброблення та строків зберігання даних. Працівник має розуміти, що саме вимірюється, які категорії інформації будуть зібрані, хто матиме доступ до результатів та в якій формі вони використовуватимуться. При цьому модель має спиратися на принцип мінімізації: збираються лише ті дані, які є дійсно необхідними для оцінювання лояльності та пов’язаних ризиків, без надмірного втручання у приватне життя працівників або їхні переконання. Для цього доцільно застосовувати шаблони анкет, у яких кожен блок запитань відповідає

конкретній аналітичній задачі, та регулярно проводити ревізію змісту опитувальників.

По-друге, ключовим етичним та правовим принципом є анонімізація або, принаймні, надійна псевдонімізація індивідуальних відповідей. На операційному рівні це означає, що в системі зберігання даних результати опитувань прив'язуються до агрегованих груп (підрозділ, професійна категорія, зміна), а не до прізвищ. У разі, якщо технічно необхідно тимчасово зберігати ідентифікатори респондентів (наприклад, для панельного аналізу динаміки), вони мають бути відокремлені від основного масиву аналітичних даних, захищені та доступні у вкрай обмеженому режимі. Одночасно повинні діяти правила щодо мінімального розміру агрегованої групи: наприклад, результати не виводяться у звіті, якщо у підгрупі менше певної кількості працівників, щоб унеможливити неформальну ідентифікацію.

По-третє, необхідною умовою є запровадження формалізованої рольової моделі доступу до даних та журналу аудиту доступів. На практиці це означає, що для кожної категорії користувачів (вище керівництво, служба економічної безпеки, HR підрозділ, керівники підрозділів, служба охорони праці та служба інформаційної безпеки) визначаються рівні доступу: хто працює лише з агрегованими показниками, хто має доступ до розрізів за підрозділами, хто може бачити деталізацію за професійними групами, а хто не має доступу до жодних первинних даних. Усі операції з перегляду, експорту або модифікації масивів даних про лояльність та пов'язані ризики мають автоматично реєструватися в журналі аудиту, який регулярно переглядається уповноваженою особою. Це створює додатковий запобіжник проти зловживань та несанкціонованого використання інформації.

Для систематизації етичних та правових вимог до роботи з даними доцільно представити їх у вигляді таблиці 3.14, що слугує практичним орієнтиром для впровадження моделі.

Таблиця 3.14

Ключові принципи роботи з даними про лояльність персоналу та практичні механізми їх реалізації

Принцип	Зміст	Практичні механізми реалізації
Добровільність і поінформована згода	Працівник усвідомлено погоджується на участь в оцінюванні	Інформаційні повідомлення, окремі блоки згоди, можливість відмови
Мінімізація даних	Збираються лише необхідні для аналізу показники	Регулярний перегляд анкет, видалення надлишкових полів
Анонімізація та конфіденційність	Неможливість ідентифікації окремих респондентів	Агрегування, пороги для розміру груп, окреме зберігання ідентифікаторів
Рольовий доступ	Дані доступні лише тим, кому вони потрібні за функцією	Розмежування прав доступу, технічні профілі користувачів
Аудит доступів	Контроль усіх операцій з даними	Журнали доступу, регулярні перевірки, внутрішній аудит
Обмежені строки зберігання	Дані не зберігаються довше, ніж це необхідно	Політика ретенції, автоматичне видалення або архівація

Джерело: розроблено автором

Четвертою групою вимог є прозорість та недопущення карального використання результатів оцінювання. У моделі прямо закладається заборона застосовувати індивідуальні результати опитувань щодо лояльності як підставу для дисциплінарних стягнень, скорочень чи обмеження кар’єрних можливостей. Оцінювання має сприйматися працівниками як інструмент діагностики стану колективу та поліпшення умов праці, а не як форма прихованого контролю чи "тест на лояльність". Для цього необхідно послідовно демонструвати, що агреговані результати використовуються для запуску програм підтримки, модернізації процесів, поліпшення безпеки та комунікацій, а не для індивідуального покарання.

Важливою складовою є комунікаційний контур, який можна умовно описати як цикл "мета - інструменти - дії - ефекти". На початку кожної хвилі оцінювання працівникам повідомляються мета та очікувані результати: для

чого підприємство проводить опитування щодо лояльності, які проблеми прагне виявити, які аспекти умов праці, безпеки та комунікації планує покращити. Далі пояснюються інструменти: які саме запитання будуть ставитися, як працює система анонімізації, як агрегуються результати та яким чином вони інтегруються в панель індикаторів економічної безпеки. На наступному етапі, після опрацювання результатів, керівництво презентує працівникам перелік конкретних дій, які будуть здійснені у відповідь на виявлені проблеми. Нарешті, на завершальному етапі відбувається демонстрація ефектів: працівникам показують, які зміни вже запроваджено, як вони вплинули на умови праці, безпеку, організацію змін та інші аспекти. Регулярне проходження цього циклу підсилює довіру до системи оцінювання та робить її важливою складовою культури взаємної відповідальності.

Для візуалізації логіки такого циклу може використовуватися проста схема, яка одночасно слугує шаблоном для управлінських комунікацій:

1. "Мета": формулювання проблем та очікуваних покращень.
2. "Інструменти": опис методів вимірювання, джерел даних і гарантій конфіденційності.
3. "Дії": перелік програм, змін у процедурах, додаткових заходів підтримки.
4. "Ефекти": відстеження та комунікація результатів, у тому числі повторні вимірювання.

П’ятим блоком є організаційне вбудовування етичних, правових та процедурних вимог у регламенти підприємства. Це означає, що політика щодо оцінювання лояльності та її використання в системі управління загрозами економічній безпеці має бути закріплена в локальних нормативних актах: положенні про захист персональних даних, положенні про систему управління ризиками, регламентах роботи HR підрозділу, кодексі етики, інструкціях для керівників підрозділів. Кожен із цих

документів фіксує відповідний фрагмент моделі: від принципів збору та зберігання даних до правил інтерпретації результатів і вимог до комунікації з персоналом.

Узагальнено етичні, правові та організаційні аспекти можна розглядати як "метарівень" моделі, який визначає рамки допустимості та довіри. Якщо дані про лояльність збираються та використовуються в умовах прозорості, добровільності, конфіденційності та передбачуваності, система оцінювання та пов’язана з нею панель індикаторів економічної безпеки працюють як спільний інструмент працівників та керівництва для підвищення стійкості підприємства. Якщо ж ці умови не виконуються, модель ризикує перетворитися на джерело додаткових загроз, що суперечить її первинному призначенню.

Очікувані ефекти інтеграції результатів оцінювання лояльності персоналу в систему управління загрозами економічній безпеці промислового підприємства доцільно розглядати як перевірку практичної дієздатності моделі. Якщо попередні блоки моделі описують, як саме вимірюється лояльність, пов’язується з процесними та фінансовими показниками і вбудовується в контур прийняття рішень, то очікувані ефекти показують, чи трансформуються ці аналітичні дії у відчутні зміни рівня економічної безпеки. Йдеться не лише про формальне зростання інтегрального індексу економічної безпеки, а про реальне зменшення частоти інцидентів, стабілізацію виробництва, підвищення маржинальності та зниження вразливості підприємства до внутрішніх і зовнішніх шоків.

Перший блок очікуваних ефектів пов’язаний зі зниженням плинності персоналу і скороченням часу виходу працівників на цільовий рівень продуктивності у критичних змінах. У промислових компаніях саме плинність у вузлових професіях (машиністи, оператори технологічних ліній, енергетики, ремонтний персонал, фахівці чергових змін) створює найбільший ризик для економічної безпеки, оскільки кожне звільнення

породжує витрати на пошук, добір та адаптацію, а також тимчасово знижує стабільність випуску. Підвищення лояльності за рахунок правильно сконструйованих програм підтримки, прозорої комунікації і справедливої системи винагороди зменшує ймовірність добровільних звільнень, особливо серед досвідчених працівників. Одночасно зростає готовність персоналу до наставництва та внутрішнього навчання, що скорочує середній час виходу нових працівників на нормативний рівень продуктивності. На рівні економічної безпеки це означає меншу кількість вимушених простоїв через кадровий дефіцит, зниження витрат на понаднормову працю та аутсорсинг, більш плавну динаміку виробничих показників упродовж року. У результаті стабілізується кількісна складова інтегрального індексу економічної безпеки, зокрема підкомпоненти, пов’язані з операційною ефективністю та витратами на персонал.

Другий блок ефектів стосується зниження частки браку, кількості переробок і тривалості простоїв, що опосередковано покращує операційну маржу та грошові потоки. Лояльний персонал, як правило, більш схильний дотримуватися технологічних регламентів, процедур техніки безпеки і стандартів якості, а також вчасно сигналізувати про відхилення і приховані дефекти. Це зменшує ймовірність помилок, викликаних недбалим ставленням до роботи, знижує обсяг непродуктивних витрат на переробку, списання сировини та готової продукції, збільшує стабільність виконання виробничих планів. Крім того, підвищення лояльності і залученості підтримує культуру "раннього попередження", коли працівники не замовчують проблеми, а ініціюють їх обговорення до того, як вони переростуть у серйозні інциденти або тривалі простої. На фінансовому рівні це проявляється у вищій операційній маржі, кращій динаміці операційного грошового потоку та меншій волатильності показників прибутковості. В інтегральному індексі економічної безпеки посилюється блок, пов’язаний з

рентабельністю основної діяльності, надійністю виробничого процесу та ефективністю використання ресурсів.

Третій блок очікуваних ефектів пов’язаний із зниженням частоти інцидентів з охорони праці, виробничого травматизму та порушень вимог комплаєнсу. У промисловому середовищі, особливо за умов війни і дефіциту ресурсів, саме "людський чинник" нерідко стає причиною критичних подій. Лояльний персонал частіше дотримується правил, менше схильний до свідомого обходу процедур, відповідальніше ставиться до використання засобів індивідуального захисту, електробезпеки, протипожежних регламентів. Крім того, така група працівників, як правило, швидше повідомляє про порушення, що дозволяє запобігати ескалації ризиків. З точки зору комплаєнсу підвищення лояльності знижує мотивацію до корисливих чи опортуністичних дій, зменшує ризик участі в корупційних схемах, несанкціонованих операціях із активами, порушень етичного кодексу. Це прямо впливає на економічну безпеку через зменшення штрафів, компенсацій, судових витрат, витрат на ліквідацію наслідків аварій, а також через зниження репутаційних ризиків, які можуть призвести до втрати контрактів, доступу до фінансування або погіршення умов запозичень.

Четвертий блок стосується динаміки інтегрального індексу економічної безпеки підприємства і ризику виходу його значень за критичні порогові межі. Запропонована модель передбачає виділення принаймні трьох порогових зон: критична зона, де значення індексу економічної безпеки є нижчим за 0,50; вразлива зона, де індекс перебуває у діапазоні від 0,50 до 0,64; та зона задовільного або високого рівня економічної безпеки, де значення індексу перевищує 0,65. Підвищення лояльності персоналу через вищезазначені канали впливу (кадровий, операційний, безпековий, комплаєнс) зменшує ймовірність різких падінь індексу, пов’язаних з реалізацією внутрішніх загроз. В умовах турбулентного зовнішнього

середовища це означає, що навіть за наявності шоків ззовні (пошкодження інфраструктури, зміни регуляторних вимог, цінові коливання) підприємство має "людський запас міцності", який пом’якшує негативний сценарій. Внаслідок цього індекс економічної безпеки рідше опускається нижче порогів 0,65 та 0,50, а якщо це й відбувається, то на коротший час і з меншою глибиною падіння. Це підвищує прогнозованість діяльності, покращує сприйняття підприємства кредиторами, інвесторами та регуляторами, розширює простір для стратегічних рішень замість реактивного "гасіння пожеж".

Для систематизації очікуваних ефектів доцільно представити узагальнювальну схему, яка пов’язує основні напрями впливу лояльності персоналу з ключовими індикаторами економічної безпеки (табл. 3.15).

У підсумку очікувані ефекти демонструють, що інтеграція результатів оцінювання лояльності персоналу в систему управління загрозами економічній безпеці не є суто аналітичною процедурою. Вона безпосередньо спрямована на зміну поведінки, процесів і результатів діяльності підприємства та дозволяє перевести абстрактні показники лояльності у конкретні поліпшення виробничої, фінансової і безпекової динаміки. Це підсилює роль людського чинника як ресурсу економічної безпеки і створює сталіший фундамент для довгострокового розвитку промислового підприємства в умовах високої невизначеності.

Обмеження моделі. Оцінюючи модель інтеграції результатів оцінювання лояльності персоналу в систему управління загрозами економічній безпеці промислового підприємства, необхідно чітко зафіксувати її ключові обмеження. Це дає змогу коректно інтерпретувати отримані результати, уникати хибних причинно-наслідкових висновків і визначати напрями подальшого методологічного вдосконалення.

По-перше, модель за своєю природою частково ендогенна. Лояльність персоналу, ключові показники ефективності та рівень економічної безпеки взаємно впливають один на одного в динаміці.

Таблиця 3.15

Очікувані ефекти підвищення лояльності персоналу для економічної безпеки промислового підприємства

Напрям впливу лояльності	Канали передачі ефекту	Ключові індикатори економічної безпеки	Очікуваний результат для економічної безпеки
Стабілізація кадрового складу	Зниження плинності, скорочення часу адаптації, посилення наставництва	Частка звільнень у критичних ролях, середній час виходу на продуктивність, витрати на підбір та адаптацію	Стабільніший випуск, менші кадрові ризики, нижчі витрати на заміну персоналу
Зменшення браку і простоїв	Краще дотримання технологічних регламентів, своєчасні сигнали про відхилення	Частка браку, кількість переробок, тривалість простоїв, операційна маржа, операційний грошовий потік	Підвищення ефективності виробництва і рентабельності, зменшення непродуктивних витрат
Зниження інцидентів охорони праці та комплаєнсу	Дотримання правил безпеки, зменшення опортуністичної поведінки, своєчасні повідомлення про порушення	Частота виробничого травматизму, кількість порушень комплаєнсу, сума штрафів та компенсацій, кількість значущих інцидентів	Зменшення прямих збитків і судових витрат, нижчі репутаційні ризики, стабільніші умови діяльності
Стабілізація інтегрального індексу економічної безпеки	Послаблення впливу внутрішніх загроз, підвищення "людського запасу міцності"	Значення і динаміка інтегрального індексу економічної безпеки, частота перетину порогів 0,65 і 0,50	Менша ймовірність потрапляння у критичну зону, вищий рівень довіри з боку стейкхолдерів, розширення стратегічних можливостей

Джерело: розроблено автором

Підвищення лояльності сприяє покращенню операційних, фінансових і безпекових показників, що, у свою чергу, підсилює довіру працівників до підприємства і може додатково підвищувати їхню лояльність. У формальному вигляді це означає, що параметр еластичності β, який інтерпретується як наближене значення часткової похідної:

$$\beta \approx \frac{\partial S}{\partial L}, \qquad (3.26)$$

де S позначає інтегральний індекс економічної безпеки, а L інтегральний індекс лояльності, відображає не чистий причинний вплив, а змішаний ефект у системі з можливим зворотним зв’язком.

Типова регресійна специфікація виду:

$$S_t = a + bL_{t-1} + cX_{t-1} + \varepsilon_t \qquad (3.27)$$

дає оцінку параметра b, який використовується як емпірична апроксимація β, однак навіть при лаговому включенні змінної лояльності повністю позбутися ендогенності неможливо.

На практиці це означає, що результати моделювання мають розглядатися як сценарні та умовні: вони показують, як могла б змінюватися економічна безпека за заданої траєкторії лояльності, за інших рівних умов, а не як беззаперечний доказ прямого причинного зв'язку. Для посилення доказовості бажаним є використання експериментального чи квазіекспериментального дизайну (наприклад, пілотні програми в окремих підрозділах з подальшим порівнянням з контрольною групою, метод "різниця в різницях", інструментальні змінні тощо).

По-друге, модель припускає, що коефіцієнт еластичності β, який відображає чутливість інтегрального індексу економічної безпеки до зміни лояльності, може бути узагальнений у межах сектора або групи підприємств. Насправді ж чутливість β істотно відрізняється між галузями з різною тривалістю виробничих циклів, структурою витрат і ступенем регуляторних обмежень. Для інфраструктурних компаній із довгими циклами, високою часткою регульованих тарифів і значною капіталомісткістю (наприклад, магістральний транспорт, енергетична передача, гідроенергетика) короткострокові зміни лояльності персоналу часто мають обмежений і лаговий вплив на фінансові результати, і, відповідно, на інтегральний індекс економічної безпеки. Натомість для підприємств з коротшими виробничими циклами, більш гнучкою структурою витрат і швидкою реакцією ринку (металургія, хімічне виробництво, гірничо-збагачувальні комбінати) локальні зміни в дисципліні, плинності кадрів та якості операцій можуть значно швидше трансформуватися у зміну маржі, оборотності та інцидентності, а отже, і в

зсув індексу економічної безпеки. Це означає, що β є не універсальною сталою, а параметром, який повинен калібруватися окремо для кожного підприємства або принаймні для однорідних груп підприємств з урахуванням галузевої специфіки, структури активів, частки регульованих доходів і ролі людського чинника у створенні доданої вартості.

По-третє, точність і надійність результатів моделі критично залежать від якості, повноти та періодичності даних. Інтегральний індекс лояльності формується на основі поєднання опитувальних джерел, поведінкових логів та операційних показників. Якщо опитування проводяться нерегулярно, із різною структурою питань або з низьким рівнем довіри працівників до анонімності, отримані оцінки лояльності можуть містити систематичні упередження. Аналогічно, якщо у кадрових та операційних системах відображені не всі інциденти (наприклад, частину не фіксують формально), або якщо показники плинності, браку та простоїв мають пропуски чи різну методику розрахунку по підрозділах, це знижує достовірність побудови як індексу лояльності, так і інтегрального індексу економічної безпеки. Важливо також враховувати періодичність даних: модель суттєво програє в чутливості, якщо оновлення ключових показників відбувається раз на рік при тому, що зміни в колективах і процесах відбуваються значно частіше.

Доцільно систематизувати основні обмеження моделі за трьома вимірами: концептуальним, методологічним і даних (табл. 3.16).

Таким чином, модель інтеграції результатів оцінювання лояльності в систему управління загрозами економічній безпеці промислового підприємства демонструє високу аналітичну та управлінську корисність, але її застосування потребує обережного ставлення до обмежень. Часткова ендогенність системи, неоднорідність чутливості в різних галузях та залежність від якості даних не скасовують практичної цінності моделі, проте вимагають від дослідника та управлінця свідомого використання

інструментів валідації, робастних перевірок і галузево специфічної калібровки.

Таблиця 3.16

Ключові обмеження моделі інтеграції лояльності в управління загрозами економічній безпеці

Вимір обмеження	Суть обмеження	Наслідки для інтерпретації результатів	Базові напрями пом'якшення
Концептуальний	Часткова ендогенність між лояльністю, ключовими показниками ефективності та економічною безпекою	Неможливість інтерпретувати β як чистий причинний ефект без додаткових припущень	Використання експериментальних та квазіекспериментальних підходів, чутливісний аналіз
Методологічний	Галузева і підприємницька диференціація чутливості β, різні лаги впливу	Обмежена можливість узагальнення результатів на всі типи підприємств	Секторальна калібровка, побудова окремих моделей для підгруп, урахування лагів
Обмеження даних	Неповнота, нерегулярність і варіативність якості даних про лояльність і ключові показники ефективності	Підвищений ризик зміщення оцінок індексів і параметра β, зниження точності прогнозів	Стандартизація показників, підвищення періодичності опитувань, аудит даних, єдине сховище

Джерело: розроблено автором

Лише за таких умов модель може слугувати не лише ілюстративним сценарним інструментом, але і надійною основою для прийняття рішень у сфері економічної безпеки.

Висновки до третього розділу

За результатами проведеного дослідження доцільно зробити наступні висновки.

1. Запропоновано авторську соціотехнічну модель інтеграції результатів оцінювання лояльності персоналу в систему управління загрозами економічній безпеці підприємства як єдиний контур прийняття рішень. Зробленотеоретичне обґрунтування лояльності як управлінськи значущої характеристики, що має афективний, нормативний та інструментальний виміри і проявляється у ставленні працівника до організації, норм, цілей та винагород. Виконано логічне пов'язання

лояльності з ризиками людського чинника, зокрема з імовірністю порушень процедур, зниженням дисципліни, зростанням конфліктності та появою поведінкових відхилень, які здатні трансформуватися у загрози для стабільності діяльності. Запропоновано інтерпретацію результатів оцінювання лояльності як інструменту профілактики та раннього попередження, а не як суто кадрового показника.

2. Запропоновано методичний підхід до операціоналізації лояльності на основі поєднання самооцінних шкал та поведінкових індикаторів, що підвищує валідність висновків і зменшує вплив суб'єктивних викривлень. Виконанонормування показників у єдину порівнювану шкалу та зроблено принципи зважування з урахуванням надійності джерел, стабільності метрик і їх стратегічної релевантності для економічної безпеки. Запропоновано структуру інтегрального показника лояльності як агрегату підіндексів прихильності та блоку поведінкових сигналів, що дозволяє одночасно фіксувати ціннісну орієнтацію і фактичні прояви у трудовій поведінці. Зроблено узгодження підходу до вимірювання з логікою практичного використання результатів у HR-процесах, ризик-менеджменті та управлінні змінами.

3. Виконано формування інтегрованого бачення економічної безпеки як індексу стану і спроможності системи підтримувати цільові параметри у фінансовому, процесному, виробничо-технологічному, інформаційному та управлінсько-комплаєнсному доменах. Запропоновано формалізацію зв'язку між індексом лояльності та інтегральним індексом економічної безпеки через систему індикаторів, що відображають як поточні результати, так і ризикові відхилення. Зроблено обґрунтування механізму впливу змін лояльності на показники діяльності через еластичності, порогові значення та оцінку чутливості, що дає можливість визначати, які зрушення лояльності є управлінськи критичними. Запропоновано використання

отриманих залежностей для пріоритизації ризиків та уточнення переліку заходів у програмах економічної безпеки.

4. Запропоновано математичний механізм інтеграції «лояльність, показники, індекс безпеки», який забезпечує відтворюваність розрахунків, прозорість вагових коефіцієнтів і можливість сценарного моделювання управлінських інтервенцій. Виконано визначення складу первинних показників і джерел даних, включно з опитуваннями, кадровою аналітикою, табелюванням та каналами зворотного зв'язку, що створює основу для регулярного моніторингу. Зроблено логіку перетворення різнорідних даних у порівнювані метрики та подальшої агрегації у підіндекси і інтегральні індекси без втрати управлінського змісту. Запропоновано підхід до перевірки стійкості результатів через повторюваність вимірювань і зіставлення з подійними показниками ризикових ситуацій.

5. Запропоновано поетапну процедуру впровадження моделі, що охоплює діагностику готовності даних і процесів, проєктування інструментів, пілотування, масштабування та інституціоналізацію у внутрішніх регламентах. Виконано розроблення процесної архітектури замкненого циклу управління, у якій результати оцінювання лояльності системно впливають на карти ризиків, реєстр загроз і програми управлінських дій у визначеній періодичності. Запропоновано деталізацію ключових управлінських кроків, включно з формуванням профілю лояльності, оновленням індикаторів, розрахунком індексів, ідентифікацією відхилень і запуском коригувальних заходів. Зроблено визначення етичних вимог і процедур якості даних, включно з інформованою згодою, знеособленням, рольовим доступом, журналюванням і забороною карального використання результатів, що забезпечує легітимність моделі та її розвиткову спрямованість.

6. За результатами проведених досліджень опубліковано одноосібний розділ у колективній монографії.

ВИСНОВКИ

В результаті проведеного дослідження було реалізовано поставлене наукове завдання, яке полягало в розробці інформаційно-аналітичного забезпечення оцінювання лояльності персоналу, здатного інтерпретувати її результати як ранні сигнали впливу деструктивних чинників на систему економічної безпеки промислових підприємств, що дозволить переводити аналітику в управлінські рішення. Нижче наведено детальні висновки за основними напрямами проведеного дослідження.

1. Вивчено теоретичні підходи до трактування поняття інформаційно-аналітичного забезпечення економічної безпеки суб'єктів господарювання як системи, що поєднує дані, методи їх обробки, організаційні ролі та регламенти використання результатів. Показано, що сучасне інформаційно-аналітичне забезпечення не зводиться до накопичення інформації або підготовки періодичних звітів, а виконує функцію перетворення відомостей про загрози, вразливості та можливості на керовані управлінські дії. Обґрунтовано, що результативність такого забезпечення визначається своєчасністю, відтворюваністю, порівнюваністю та підзвітністю прийнятих рішень, а також здатністю забезпечити зворотний зв'язок щодо ефективності втручань. Уточнено значення стандартизації показників, єдиного словника термінів та правил агрегації даних для забезпечення однаковості інтерпретації результатів різними підрозділами. Доведено, що логіка «моніторинг, аналіз, рішення, дія, навчання» є необхідною умовою перетворення аналітики на інструмент управління економічною безпекою в умовах нестабільності та швидких змін ризикового середовища.

2. Встановлено роль та місце управління персоналом у системі економічної безпеки промислових підприємств через обґрунтування людського чинника як системоутворювального елемента операційної стійкості та дисципліни виконання технологічних процедур. Показано, що

кадрові рішення впливають на рівень ризику не лише через укомплектованість штатів, а й через відповідність компетенцій критичним процесам, стабільність продуктивності, дотримання вимог охорони праці та комплаєнс-поведінку. Визначено, що управління персоналом має бути інтегрованим у контури економічної безпеки через узгодження індикаторів, формалізацію відповідальностей за дані та участь у процедурах реагування на ризикові відхилення. Обґрунтовано необхідність переходу від фрагментарного використання HR-метрик до системного застосування даних про персонал як ранніх сигналів ризику, що передують фінансовим втратам або операційним збоям. Доведено, що така інтеграція підсилює превентивність управління, оскільки дозволяє реагувати на зниження лояльності, напруженість у колективах та деградацію дисципліни до того, як ці явища трансформуються у аварійність, брак, простої або репутаційні втрати.

3. Досліджено сучасні підходи до оцінювання лояльності персоналу в контексті економічної безпеки, які передбачають поєднання психометричних інструментів і поведінкових даних для підвищення валідності вимірювання. Обґрунтовано, що лояльність доцільно інтерпретувати як багатовимірну характеристику, яка включає емоційну прихильність до організації, нормативну орієнтацію на дотримання правил та інструментальну оцінку доцільності співпраці. Показано, що в промисловому середовищі лояльність має не лише соціально-психологічний вимір, а й прямий операційний прояв через дисципліну, відповідальність, готовність дотримуватися процедур і підтримувати зміни. Встановлено, що оцінювання лояльності є особливо значущим як інструмент виявлення слабких сигналів ризику, зокрема схильності до порушення регламентів, ігнорування інструктажів, саботажу або небезпечної економії часу на критичних операціях. Підкреслено, що сучасні

підходи мають забезпечувати регулярність вимірювань, порівнюваність у часі та інтерпретованість результатів для управлінців різних рівнів.

4. Вивчено сучасний стан економічної безпеки промислових підприємств як комплексну категорію, що включає фінансову стійкість, операційну надійність, керованість процесів, інформаційну захищеність, технологічну дисципліну та дотримання нормативних вимог. Показано, що оцінювання економічної безпеки має бути орієнтованим на управлінське застосування, тобто передбачати не лише аналітичний висновок, а й визначення зон ризику та режимів реагування. Обґрунтовано доцільність використання інтегральних оцінок, які забезпечують порівнюваність між періодами та дозволяють відстежувати динаміку стійкості підприємства. Уточнено значення порогових значень і категорій інтерпретації, які переводять числовий результат у чіткі управлінські дії, відповідальність і часові горизонти реагування. Доведено, що для промислових підприємств важливо поєднувати фінансові й нефінансові ознаки уразливості, оскільки значна частина ризиків виникає на рівні процесів, дисципліни та людського чинника задовго до відображення проблем у фінансовій звітності.

5. Проаналізовано інструменти оцінювання лояльності персоналу та її вплив на економічну безпеку промислових підприємств із позиції можливості перетворення результатів вимірювання на конкретні управлінські рішення. Показано, що ізольоване використання анкет або разових опитувань не забезпечує достатньої практичної цінності, якщо немає механізму перевірки даних, нормування показників і порогової інтерпретації. Обґрунтовано, що лояльність впливає на економічну безпеку через зміну ймовірності інцидентів, якісних відхилень, простоїв, порушень правил безпеки праці та комплаєнс-ризиків, що у підсумку формує фінансові наслідки. Визначено, що найпродуктивнішим є підхід, за якого результати оцінювання лояльності інтегруються в систему показників ризику і доповнюються даними про плинність, прогули, участь у навчанні,

дисциплінарні випадки та інші поведінкові сигнали. Показано, що така інтеграція створює підстави для раннього попередження та адресних інтервенцій, спрямованих на критичні групи, процеси або підрозділи з найбільшою чутливістю до людського чинника.

6. Ідентифіковано внутрішні та зовнішні загрози економічній безпеці промислових підприємств з боку персоналу, враховуючи механізми їх виникнення, реалізації та наслідки для підприємства. До внутрішніх загроз віднесено порушення технологічної дисципліни, ігнорування регламентів охорони праці, зниження відповідальності, прихований опір змінам, конфліктність і деградацію командної взаємодії. До зовнішніх загроз, що реалізуються через персонал, віднесено соціальну інженерію, схиляння до неправомірних дій, витоки інформації, провокування інцидентів і використання вразливостей поведінки працівників. Показано, що низька лояльність виступає фактором посилення як внутрішніх, так і зовнішніх загроз, оскільки знижує готовність дотримуватися правил і підвищує сприйнятливість до зовнішнього впливу. Обґрунтовано необхідність систематизації загроз у межах реєстру ризиків та встановлення для них індикаторів, порогів, власників ризику та стандартних планів реагування.

7. Розроблено модель інтеграції результатів оцінювання лояльності персоналу в систему забезпечення економічної безпеки промислового підприємства як єдиний контур прийняття рішень. Модель передбачає послідовний перехід від збору первинних даних до формування індикаторів і узагальненого показника, далі до порівняння з порогами та ідентифікації ризикових відхилень. Обґрунтовано, що кожне відхилення має бути пов’язане з конкретною управлінською інтервенцією, відповідальним підрозділом і часовим горизонтом реагування, що забезпечує підзвітність і керованість. Показано, що модель підтримує сценарний підхід, оскільки дозволяє оцінювати потенційний ефект програм підвищення лояльності на ключові процесні та фінансові метрики. Доведено, що інтеграція лояльності

у контур економічної безпеки підсилює превентивність управління, оскільки зменшує часовий лаг між появою слабких сигналів і запуском коригувальних дій.

8. Розроблено процесну архітектуру моделі інтеграції результатів оцінювання лояльності в систему забезпечення економічної безпеки як безперервний, регламентований цикл. Визначено етапи планування вимірювань, збирання даних, їх перевірки та очищення, нормування, розрахунку індикаторів, інтерпретації, ескалації та прийняття управлінських рішень. Передбачено механізм зворотного зв'язку, за яким результати інтервенцій оцінюються повторними вимірюваннями, а параметри індикаторів, ваг і порогів можуть коригуватися на основі фактичного ефекту. Обґрунтовано необхідність інтеграції архітектури з практиками внутрішнього контролю, ризик-менеджменту та управління змінами для уникнення дублювання функцій і підвищення узгодженості рішень. Показано, що процесна архітектура забезпечує можливість масштабування на рівні підрозділів і підприємства загалом, а також створює основу для цифрового впровадження через дашборди та регламентовану управлінську звітність.

9. Визначено вимоги до етичних, правових та організаційних аспектів використання результатів оцінювання лояльності персоналу як необхідну умову легітимності, довіри та стійкості інформаційно-аналітичної системи. Обґрунтовано потребу у правовій визначеності мети збору та обробки даних, мінімізації чутливих даних і дотриманні принципу пропорційності, щоб уникнути надмірного втручання в приватність працівників. Встановлено необхідність прозорого інформування персоналу про інструменти оцінювання, правила доступу й використання результатів, а також про механізми захисту та оскарження у разі порушень. Визначено організаційні вимоги щодо розмежування доступу за ролями, журналювання операцій, контролю якості даних і підзвітності рішень, що

ґрунтуються на результатах оцінювання. Підкреслено принцип недопущення карального використання індивідуальних результатів і пріоритет застосування оцінювання для профілактики ризиків, розвитку компетенцій, поліпшення умов праці та зміцнення організаційної довіри.

10. Запропоновані підходи сприятимуть підвищенню ефективності управління персоналом у промислових підприємствах, зменшенню ризиків людського чинника та посиленню якості стратегічного планування кадрових і організаційних ресурсів. Їх застосування забезпечує системне перетворення даних про лояльність персоналу на управлінські рішення в контурі економічної безпеки, що підвищує превентивність реагування на загрози та знижує ймовірність операційних і фінансових втрат. Це підтверджує, що інформаційно-аналітичне забезпечення оцінювання лояльності персоналу є ключовим інструментом системи забезпечення економічної безпеки, який підтримує довгострокову стійкість виробничих процесів і конкурентоспроможність підприємства в умовах нестабільного бізнес-середовища.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Altman, E. I. (1968). Financial ratios, discriminant analysis and the prediction of corporate bankruptcy. *The Journal of Finance, 23*(4), 589–609. https://doi.org/10.2307/2978933
2. Angrave, D., Charlwood, A., Kirkpatrick, I., Lawrence, M., & Stuart, M. (2016). HR and analytics: Why HR is set to fail the big data challenge. *Human Resource Management Journal, 26*(1), 1–11. https://doi.org/10.1111/1748-8583.12090
3. Armbrust, M., Ghodsi, A., Xin, R., & Zaharia, M. (2021). Lakehouse: A new generation of data analytics architectures. In *Proceedings of CIDR 2021*. https://www.cidrdb.org/cidr2021/papers/cidr2021_paper17.pdf
4. Armstrong, M. (2014). *Armstrong's handbook of human resource management practice* (13th ed.). Kogan Page. https://www.koganpage.com/
5. AuditBoard. (2024). How to develop key risk indicators (KRIs) to fortify your business. https://auditboard.com/blog/how-to-develop-key-risk-indicators-kris-to-fortify-business
6. Bakker, A. B., & Demerouti, E. (2007). The Job Demands–Resources model: State of the art. *Journal of Managerial Psychology, 22*(3), 309–328. https://doi.org/10.1108/02683940710733115
7. Barabási, A.-L. (2002). *Linked: The new science of networks*. Perseus Publishing.
8. Baranovskyi, O. I. (1999). Financial Security: Monograph. Phoenix.
9. Baranovskyi, O. I. (2004). Financial Security in Ukraine: Assessment Methodology and Provision Mechanisms. KNUTE.
10. Barocas, S., & Selbst, A. D. (2016). Big data's disparate impact. *California Law Review, 104*(3), 671–732. https://doi.org/10.15779/Z38BG31
11. Beaver, W. H. (1966). Financial ratios as predictors of failure. *Journal of Accounting Research, 4*, 71–111. https://doi.org/10.2307/2490171

12. Becker, B. E., & Huselid, M. A. (2001). *The HR scorecard: Linking people, strategy, and performance*. Harvard Business School Press. https://www.hbs.edu/
13. Becker, H. S. (1960). Notes on the concept of commitment. *American Journal of Sociology, 66*(1), 32–40. https://doi.org/10.1086/222820
14. Beer, M., Spector, B., Lawrence, P. R., Mills, D. Q., & Walton, R. E. (1984). *Managing human assets*. Free Press.
15. Blau, P. M. (1964). *Exchange and power in social life*. Wiley.
16. Bondarouk, T., & Ruël, H. (2009). Electronic human resource management: Challenges in the digital era. *The International Journal of Human Resource Management, 20*(3), 505–514. https://doi.org/10.1080/09585190802707235
17. Borgatti, S. P. (2005). Centrality and network flow. *Social Networks, 27*(1), 55–71. https://doi.org/10.1016/j.socnet.2004.11.008
18. Borgatti, S. P., & Everett, M. G. (2006). A graph-theoretic perspective on centrality. *Social Networks, 28*(4), 466–484. https://doi.org/10.1016/j.socnet.2005.11.005
19. Boudreau, J. W., & Ramstad, P. M. (2007). *Beyond HR: The new science of human capital*. Harvard Business Press.
20. Boxall, P., & Purcell, J. (2003). *Strategy and human resource management*. Palgrave Macmillan.
21. Burt, R. S. (1992). *Structural holes: The social structure of competition*. Harvard University Press.
22. Burt, R. S. (2004). Structural holes and good ideas. *American Journal of Sociology, 110*(2), 349–399. https://doi.org/10.1086/421787
23. Campion, M. A., Fink, A. A., Ruggeberg, B. J., Carr, L., Phillips, G. M., & Odman, R. B. (2011). Doing competencies well: Best practices in competency modeling. *Personnel Psychology, 64*(1), 225–262. https://doi.org/10.1111/j.1744-6570.2010.01207.x

24. Cappelli, D., Moore, A., Trzeciak, R., & Shimeall, T. (2006–2013). *The CERT guide to insider threats*. Addison-Wesley.
25. Charnes, A., Cooper, W. W., & Rhodes, E. (1978). Measuring the efficiency of decision making units. *European Journal of Operational Research, 2*(6), 429–444. https://doi.org/10.1016/0377-2217(78)90138-8
26. Cheng, Y., Boey, K. W., & Hui, W. (2003). The validity of the three-component model of organizational commitment in a Chinese context. *Acta Psychologica, 114*(3), 285–300. https://doi.org/10.1016/S0001-6918(03)00076-9
27. Christian, M. S., Garza, A. S., & Slaughter, J. E. (2011). Work engagement: A quantitative review and test of its relations with task and contextual performance. *Personnel Psychology, 64*(1), 89–136. https://doi.org/10.1111/j.1744-6570.2010.01203.x
28. CISA. (2021). Insider threat mitigation guide. https://www.cisa.gov/sites/default/files/2022-11/Insider%20Threat%20Mitigation%20Guide_Final_508.pdf
29. Colquitt, J. A. (2001). On the dimensionality of organizational justice: A construct validation of a measure. *Journal of Applied Psychology, 86*(3), 386–400. https://doi.org/10.1037/0021-9010.86.3.386
30. Committee of Sponsoring Organizations of the Treadway Commission. (2017). *Enterprise risk management: Integrating with strategy and performance*. https://www.coso.org/Pages/erm.aspx
31. Corbett-Davies, S., & Goel, S. (2018). The measure and mismeasure of fairness: A critical review of fair machine learning. *arXiv*. https://arxiv.org/abs/1808.00023
32. Cross, R., & Parker, A. (2004). *The hidden power of social networks*. Harvard Business School Press.

33. Dabirian, A., Kietzmann, J., & Diba, H. (2017). A great place to work!? Understanding crowdsourced employer branding. *Business Horizons, 60*(2), 197–205. https://doi.org/10.1016/j.bushor.2016.11.005
34. DAMA International. (2017). *DAMA-DMBOK: Data management body of knowledge* (2nd ed.). Technics Publications. https://technicspub.com/dmbok/
35. Danyuk, V. M., Kolot, A. M., & Sukov, H. S. (2013). *Управління персоналом*. КНЕУ.
36. Davenport, T. H., Harris, J., & Shapiro, J. (2010). Competing on talent analytics. *Harvard Business Review, 88*(10), 52–58. https://hbr.org/2010/10/competing-on-talent-analytics
37. Dessler, G. (2005). *Human resource management* (10th ed.). Prentice Hall.
38. Dwork, C., Hardt, M., Pitassi, T., Reingold, O., & Zemel, R. (2012). Fairness through awareness. In *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference* (pp. 214–226). https://doi.org/10.1145/2090236.2090255
39. Edmondson, A. C. (1999). Psychological safety and learning behavior in work teams. *Administrative Science Quarterly, 44*(2), 350–383. https://doi.org/10.2307/2666999
40. Eisenberger, R., Armeli, S., Rexwinkel, B., Lynch, P., & Rhoades, L. (2001). Reciprocation of perceived organizational support. *Journal of Applied Psychology, 86*(1), 42–51. https://doi.org/10.1037/0021-9010.86.1.42
41. Fan, W., & Yan, Z. (2010). Factors affecting response rates of the web survey: A systematic review. *Computers in Human Behavior, 26*(2), 132–139. https://doi.org/10.1016/j.chb.2009.10.015
42. Flanagan, J. C. (1954). The critical incident technique. *Psychological Bulletin, 51*(4), 327–358. https://doi.org/10.1037/h0061470

43. Freeman, L. C. (1979). Centrality in social networks: Conceptual clarification. *Social Networks, 1*, 215–239. https://doi.org/10.1016/0378-8733(78)90021-7
44. Gebru, T., Morgenstern, J., Vecchione, B., Vaughan, J. W., Wallach, H., Daumé III, H., & Crawford, K. (2021). Datasheets for datasets. *Communications of the ACM, 64*(12), 86–92. https://doi.org/10.1145/3458723
45. Gill, P., Stewart, K., Treasure, E., & Chadwick, B. (2008). Methods of data collection in qualitative research: Interviews and focus groups. *British Dental Journal, 204*(6), 291–295. https://doi.org/10.1038/bdj.2008.192
46. Granovetter, M. (1973). The strength of weak ties. *American Journal of Sociology, 78*(6), 1360–1380. https://doi.org/10.1086/225469
47. Hardt, M., Price, E., & Srebro, N. (2016). Equality of opportunity in supervised learning. In *Advances in Neural Information Processing Systems* (pp. 3315–3323). https://proceedings.neurips.cc/
48. Harry, M., & Schroeder, R. (2000). *Six Sigma: The breakthrough management strategy revolutionizing the world's top corporations*. Doubleday.
49. Harter, J. K., Schmidt, F. L., & Hayes, T. L. (2002). Business-unit-level relationship between employee satisfaction, employee engagement, and business outcomes. *Journal of Applied Psychology, 87*(2), 268–279. https://doi.org/10.1037/0021-9010.87.2.268
50. Heskett, J. L., Sasser, W. E., Jr., & Schlesinger, L. A. (1997). *The service profit chain*. Free Press.
51. High-Level Expert Group on AI. (2019). *Ethics guidelines for trustworthy AI*. European Commission. https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai
52. Hollnagel, E. (2011). *Resilience engineering in practice: A guidebook*. CRC Press.

53. Holtom, B. C., Mitchell, T. R., Lee, T. W., & Eberly, M. B. (2008). Turnover and retention research. *Academy of Management Annals, 2*(1), 231–274. https://doi.org/10.5465/19416520802211552
54. Huett, L., & Gun, P. H. (дані не уточнено). (Як наведено у твоєму переліку).
55. Hwang, C.-L., & Yoon, K. (1981). *Multiple attribute decision making: Methods and applications*. Springer. https://doi.org/10.1007/978-3-642-48318-9
56. Ianioglo, A., Polajeva, T., & Parmacli, D. (2015). Economic security of enterprise and the system of its ensuring. In *Contemporary Issues in Business, Management and Education 2015* (pp. 1–8). VGTU Press. https://doi.org/10.3846/cibme.2015.05
57. Ibarra, H. (1993). Network centrality, power, and innovation involvement. *Academy of Management Journal, 36*(3), 471–501. https://doi.org/10.2307/256589
58. International Organization for Standardization / International Electrotechnical Commission. (2022). ISO/IEC 27001:2022 Information security management systems: Requirements. https://www.iso.org/standard/82875.html
59. International Organization for Standardization / International Electrotechnical Commission. (2022). ISO/IEC 27002:2022 Information security controls. https://www.iso.org/standard/75652.html
60. International Organization for Standardization / International Electrotechnical Commission. (2019). ISO/IEC 27701:2019 Privacy information management. https://www.iso.org/standard/71670.html
61. International Organization for Standardization / International Electrotechnical Commission. (2023). ISO/IEC 23894:2023 Artificial intelligence: Guidance on risk management. https://www.iso.org/standard/77304.htm

62. International Organization for Standardization. (2018). ISO 19011:2018 Guidelines for auditing management systems. https://www.iso.org/standard/70017.html
63. International Organization for Standardization. (2018). ISO 30414:2018 Human resource management: Guidelines for internal and external human capital reporting. https://www.iso.org/standard/69338.html
64. International Organization for Standardization. (2018). ISO 31000:2018 Risk management: Guidelines. https://www.iso.org/standard/65694.html
65. International Organization for Standardization. (2018). ISO 45001:2018 Occupational health and safety management systems: Requirements with guidance for use. https://www.iso.org/standard/63787.html
66. International Organization for Standardization. (2019). ISO 22301:2019 Security and resilience: Business continuity management systems: Requirements. https://www.iso.org/standard/75106.html
67. International Organization for Standardization. (2021). ISO 37002:2021 Whistleblowing management systems: Guidelines. https://www.iso.org/standard/65035.html
68. International Organization for Standardization. (2021). ISO 37301:2021 Compliance management systems: Requirements with guidance for use. https://www.iso.org/standard/75080.html
69. Jackson, M. C., Mansingh, G., & McAuley, J. (2001). Information technology and knowledge management. In *Handbook on knowledge management* (pp. 517–531). Springer.
70. Jain, P., Venkataraman, S., et al. (2023). Analyzing and comparing lakehouse storage systems. In *Proceedings of CIDR 2023*. https://www.cidrdb.org/cidr2023/
71. Jüttner, U. (2005). Supply chain risk management. *The International Journal of Logistics Management, 16*(1), 120–141. https://doi.org/10.1108/09574090510617385

72. Kahn, W. A. (1990). Psychological conditions of personal engagement and disengagement at work. *Academy of Management Journal, 33*(4), 692–724. https://doi.org/10.2307/256287
73. Kaplan, R. S., & Norton, D. P. (1992). The balanced scorecard: Measures that drive performance. *Harvard Business Review, 70*(1), 71–79. https://hbr.org/1992/01/the-balanced-scorecard-measures-that-drive-performance-2
74. Kaplan, R. S., & Norton, D. P. (1996). *The balanced scorecard: Translating strategy into action*. Harvard Business School Press.
75. Kleinberg, J., Mullainathan, S., & Raghavan, M. (2017). Inherent trade-offs in the fair determination of risk scores. In *Proceedings of ITCS 2017*. https://doi.org/10.4230/LIPIcs.ITCS.2017.43
76. Krackhardt, D. (1992). The strength of strong ties. In N. Nohria & R. Eccles (Eds.), *Networks and organizations* (pp. 216–239). Harvard Business School Press.
77. Kroll, J. A., et al. (2017). Accountable algorithms. *University of Pennsylvania Law Review, 165*(3), 633–705. https://scholarship.law.upenn.edu/penn_law_review/vol165/iss3/3/
78. Kuvaas, B. (2016). Performance appraisal satisfaction and employee outcomes. *The International Journal of Human Resource Management, 27*(1), 36–53. https://doi.org/10.1080/09585192.2015.1079278
79. Latora, V., & Marchiori, M. (2001). Efficient behavior of small-world networks. *Physical Review Letters, 87*(19), 198701. https://doi.org/10.1103/PhysRevLett.87.198701
80. Levenson, A. (2018). *Strategic analytics: Advances and impacts in human resources management*. Berrett-Koehler.
81. Lipton, Z. C. (2018). The mythos of model interpretability. *Communications of the ACM, 61*(10), 36–43. https://doi.org/10.1145/3233231

82. Lundberg, S. M., & Lee, S.-I. (2017). A unified approach to interpreting model predictions. In *Advances in Neural Information Processing Systems*. https://proceedings.neurips.cc/
83. Macey, W. H., & Schneider, B. (2008). The meaning of employee engagement. *Industrial and Organizational Psychology, 1*(1), 3–30. https://doi.org/10.1111/j.1754-9434.2007.00002.x
84. Mael, F., & Ashforth, B. E. (1992). Alumni and their alma mater. *Journal of Organizational Behavior, 13*(2), 103–123. https://doi.org/10.1002/job.4030130202
85. Marler, J. H., & Boudreau, J. W. (2017). An evidence-based review of HR analytics. *The International Journal of Human Resource Management, 28*(1), 3–26. https://doi.org/10.1080/09585192.2016.1244699
86. Maslach, C., Schaufeli, W. B., & Leiter, M. P. (2001). Job burnout. *Annual Review of Psychology, 52*, 397–422. https://doi.org/10.1146/annurev.psych.52.1.397
87. Men, L. R. (2014). Strategic internal communication. *Management Communication Quarterly, 28*(2), 264–284. https://doi.org/10.1177/0893318914524536
88. MetricStream. (2026). Key risk indicators (KRIs): A complete guide. https://www.metricstream.com/insights/Key-Risk-indicators-ERM.htm
89. Meyer, J. P., & Allen, N. J. (1991). A three-component conceptualization of organizational commitment. *Human Resource Management Review, 1*(1), 61–89. https://doi.org/10.1016/1053-4822(91)90011-Z
90. Meyer, J. P., & Allen, N. J. (1997). *Commitment in the workplace: Theory, research, and application*. Sage.
91. Meyer, J. P., & Herscovitch, L. (2001). Commitment in the workplace: Toward a general model. *Human Resource Management Review, 11*(3), 299–326. https://doi.org/10.1016/S1053-4822(00)00053-X

92. Mitchell, M., Wu, S., Zaldivar, A., et al. (2019). Model cards for model reporting. In *Proceedings of FAT* 2019* (pp. 220–229). https://doi.org/10.1145/3287560.3287596
93. Molnar, C. (2019). *Interpretable machine learning*. https://christophm.github.io/interpretable-ml-book/
94. Montgomery, D. C. (2012). *Introduction to statistical quality control* (7th ed.). Wiley.
95. Mowday, R. T., Porter, L. W., & Steers, R. M. (1982). *Employee–organization linkages*. Academic Press.
96. National Institute of Standards and Technology. (2020). *Security and privacy controls for information systems and organizations (SP 800-53 Rev. 5)*. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
97. National Institute of Standards and Technology. (2023). *AI Risk Management Framework (AI RMF 1.0)*. https://www.nist.gov/itl/ai-risk-management-framework
98. Neal, A., & Griffin, M. A. (2006). A study of the lagged relationships among safety climate, safety motivation, safety behavior, and accidents. *Journal of Applied Psychology, 91*(4), 946–953. https://doi.org/10.1037/0021-9010.91.4.946
99. Near, J. P., & Miceli, M. P. (1985). Organizational dissidence: The case of whistle-blowing. *Journal of Business Ethics, 4*(1), 1–16. https://doi.org/10.1007/BF00382668
100. Newman, M. E. J. (2003). The structure and function of complex networks. *SIAM Review, 45*(2), 167–256. https://doi.org/10.1137/S003614450342480
101. Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.
102. Noe, R. A., Hollenbeck, J. R., Gerhart, B., & Wright, P. M. (2017). *Fundamentals of human resource management* (7th ed.). McGraw-Hill Education.

103. Nunnally, J. C., & Bernstein, I. H. (1994). *Psychometric theory* (3rd ed.). McGraw-Hill.
104. Opsahl, T., Agneessens, F., & Skvoretz, J. (2010). Node centrality in weighted networks. *Social Networks, 32*(3), 245–251. https://doi.org/10.1016/j.socnet.2010.03.006
105. Organ, D. W. (1988). *Organizational citizenship behavior: The good soldier syndrome*. Lexington Books.
106. Paulhus, D. L. (1991). Measurement and control of response bias. In J. P. Robinson, P. R. Shaver, & L. S. Wrightsman (Eds.), *Measures of personality and social psychological attitudes* (pp. 17–59). Academic Press.
107. Pfeffer, J. (1998). *The human equation: Building profits by putting people first*. Harvard Business School Press.
108. Podsakoff, P. M., Podsakoff, N. P., MacKenzie, S. B., Maynes, T., & Spoelma, T. (2014). Consequences of unit-level organizational citizenship behaviors. *Annual Review of Organizational Psychology and Organizational Behavior, 1*, 599–622. https://doi.org/10.1146/annurev-orgpsych-031413-091314
109. Pratt, M. G. (1998). To be or not to be? Central questions in organizational identification. In D. A. Whetten & P. Godfrey (Eds.), *Identity in organizations* (pp. 171–207). Sage.
110. Primorac, T., Kozina, T., & Turčić, I. (2018). Economic security of enterprises. *Poslovna izvrsnost / Business Excellence, 12*(2), 167–175. https://doi.org/10.22598/pi-be/2018.12.2.167
111. Pushak, Y., Lagodiienko, V., Basiurkina, N., Nemchenko, V., & Lagodiienko, N. (2021). Formation the system for assessing the economic security of enterprise in the agricultural sector. *Business: Theory and Practice, 22*(1), 80–90. https://doi.org/10.3846/btp.2021.13013
112. Rabotin, Y. (2022). The essence of economic security and the principles of its ensuring. *Revista Română de Statistică – Supliment*, (8), 37–42.

https://www.revistadestatistica.ro/supliment/wp-content/uploads/2022/09/RRSS_02EN_08_2022.pdf

113. Reagans, R., & Zuckerman, E. (2001). Networks, diversity, and productivity. *Organization Science, 12*(4), 502–517. https://doi.org/10.1287/orsc.12.4.502.10639
114. Reason, J. (1997). *Managing the risks of organizational accidents*. Ashgate.
115. Reichheld, F. F. (2003). The one number you need to grow. *Harvard Business Review, 81*(12), 46–54. https://hbr.org/2003/12/the-one-number-you-need-to-grow
116. Richards, N. M., & Hartzog, W. (2015). Privacy's blueprint. *Harvard Law Review, 128*(7), 1307–1360. https://harvardlawreview.org/
117. Riketta, M. (2005). Organizational identification: A meta-analysis. *Journal of Vocational Behavior, 66*(2), 358–384. https://doi.org/10.1016/j.jvb.2004.05.005
118. Rothwell, W. J. (2010). *Effective succession planning* (4th ed.). AMACOM.
119. Rousseau, D. M. (1995). *Psychological contracts in organizations*. Sage.
120. Saaty, T. L. (1980). *The analytic hierarchy process: Planning, priority setting, resource allocation*. McGraw-Hill.
121. Saks, A. M. (2006). Antecedents and consequences of employee engagement. *Journal of Managerial Psychology, 21*(7), 600–619. https://doi.org/10.1108/02683940610690169
122. Samoilenko, A., Britchenko, I., Levchenko, N., Lošonczi, P., Bilichenko, O., & Bodnar, I. (2023). Economic security system for a company in the conditions of digital transformations. *WSEAS Transactions on Business and Economics, 20*, 57–67. https://doi.org/10.37394/232032.2023.1.5
123. Schaufeli, W. B. (2017). Applying the Job Demands–Resources model: A "how to" guide to increase work engagement. *Organizational Dynamics, 46*(2), 120–132. https://doi.org/10.1016/j.orgdyn.2017.04.008

124. Schaufeli, W. B., & Bakker, A. B. (2004). *UWES manual*. Utrecht University.
125. Schaufeli, W. B., & Bakker, A. B. (2010). Defining and measuring work engagement. In A. B. Bakker & M. P. Leiter (Eds.), *Work engagement* (pp. 10–24). Psychology Press.
126. Schein, E. H. (2010). *Organizational culture and leadership* (4th ed.). Jossey-Bass.
127. Shippmann, J. S., Ash, R. A., Battista, M., et al. (2000). The practice of competency modeling. *Personnel Psychology, 53*(3), 703–740. https://doi.org/10.1111/j.1744-6570.2000.tb00220.x
128. Smelik, R. (2020). Economic security of the organisation: Financial component management. *Financial Law Review, 18*(2), 33–48. https://ejournals.eu/en/journal_article_files/full_text/018ecedd-e93c-7152-92b6-dcad97024366/download
129. Smith, P. C., & Kendall, L. M. (1963). Retranslation of expectations. *Journal of Applied Psychology, 47*(2), 149–155. https://doi.org/10.1037/h0041858
130. Solove, D. J. (2021). *Breached! Why data security law fails and how to improve it*. Oxford University Press.
131. Spencer, L. M., & Spencer, S. M. (1993). *Competence at work: Models for superior performance*. Wiley.
132. Thomson Reuters. (2025). Key risk indicators (KRIs): An overview. https://legal.thomsonreuters.com/blog/key-risk-indicators-kris-an-overview/
133. Ulrich, D., & Brockbank, W. (2005). *The HR value proposition*. Harvard Business School Press.
134. Wasserman, S., & Faust, K. (1994). *Social network analysis: Methods and applications*. Cambridge University Press.

135. Watson, T. J. (2010). Critical social science, pragmatism and the realities of HRM. *The International Journal of Human Resource Management, 21*(6), 915–931. https://doi.org/10.1080/09585191003729387
136. Wilton, N. (2013). *An introduction to human resource management* (2nd ed.). Sage.
137. Wright, P. M., & McMahan, G. C. (1992). Theoretical perspectives for strategic human resource management. *Journal of Management, 18*(2), 295–320. https://doi.org/10.1177/014920639201800205
138. Yuzue, N. (2025). Defining economic security through literature review. *Frontiers in Political Science*. https://www.frontiersin.org/journals/political-science
139. Zadeh, L. A. (1965). Fuzzy sets. *Information and Control, 8*(3), 338–353. https://doi.org/10.1016/S0019-9958(65)90241-X
140. Zlobin K. (2024). Information and analytical support and tools for assessing employee loyalty in enterprises. *Economics, Finance and Management Review.* № 2(18), P. 60–72. DOI: https://doi.org/10.36690/2674-5208-2024-2-60-72.
141. Zlobin K. (2023). Personnel well-being as a component of the social policy of the company. *Relationship between public administration and business entities management:* book of abstracts (November 24, 2023). Estonia. https://conf.scnchub.com/index.php/RPABM/RPABM-2023/paper/view/600/83
142. Zlobin K. (2024). The impact of involving employees in decision-making on increasing the loyalty of the company's personnel. International Conference on Corporation Management: book of abstracts (April 26, 2024). Estonia. https://conf.scnchub.com/index.php/ICCM/ICCM-2024/paper/view/740/208
143. Zlobin, K. (2025). Model of Integration of Loyalty Assessment Results into the Threat Management System of the Economic Security of an

Industrial Enterprise. In P. Kolisnichenko (Ed.),Insider threats and security in corporations.274p. (pp. 181–203). Scientific Center of Innovative Research. DOI: https://doi.org/10.36690/ITSC-181-203.

144. Акімов, В. В., & Фурса, В. А. (2012). Організація економічної безпеки на українських підприємствах. Вісник Національного технічного університету «ХПІ», (5), 11–16.
145. Алькема, В., & Діденко, В. (2024). Цифровізація інформаційно-аналітичного забезпечення управління інноваційною діяльністю, інноваційним розвитком підприємств. Вчені записки Університету «КРОК», 3(75), 85–92. https://doi.org/10.31732/2663-2209-2024-75-85-92.
146. Алькема, В. Г., & Сумець, О. М. (2025). Інтегрована модель комунікативного управління персоналом ІТ-компаній в умовах кадрових ризиків. Економіка та суспільство, (75). https://doi.org/10.32782/2524-0072/2025-75-16.
147. Алькема, В. Г., Літвін, Н. М., & Кириченко, О. С. (2015). Економічна безпека інноваційного підприємства (навчальний посібник). Університет економіки та права «КРОК». https://dspace.krok.edu.ua/handle/krok/79.
148. Архипенко, С. М., & Іванова, А. В. (2021). Інформаційно-аналітичне забезпечення системи управління економічною безпекою промислового підприємства. *Економічний форум*, (3), 6–14. https://econforum.duan.edu.ua/images/PDF/2021/3.pdf.
149. Архипенко, Т. А., & Іванова, М. І. (2021). Систематизація визначень поняття «економічна безпека підприємства». *Нобелівський вісник*, 1(14), 7–12. https://acadrev.duan.edu.ua/images/PDF/2010/2/5.pdf
150. Баланда, А. Л. (2011). Інформаційно-аналітичне забезпечення економічної безпеки суб'єктів підприємницької діяльності: стан та

перспективи розвитку. *Управління проектами та розвиток виробництва*, 1(37), 150–155.

151. Бєлоус, Н. Д. (2012). Теоретичне узагальнення складових та факторів формування економічної безпеки підприємств. *Збірник наукових праць ВНАУ*, 1(56), 3, 73–83.
152. Бондаренко, О. С. (2018). Інформаційно-аналітичне забезпечення управління фінансовими ресурсами суб'єктів господарювання. *Економіка та держава*, (6), 21–24.
153. Варенко В. М. (2014). Інформаційно-аналітична діяльність : навч. посіб. К. : Університет Україна. 417 с.
154. Васильців, Т. Г. (2008). Економічна безпека підприємництва України: стратегія та механізми зміцнення (монографія). Львів: Арал. 384 с.
155. Волощук, Л. О., Філиппова, С. В., & Черкасова, С. О. (2015). Економічна безпека підприємств реального сектору економіки в умовах вартісно-орієнтованого управління (монографія). *Одеський національний політехнічний університет*. 196 с.
156. Воронюк, Є. В. (2021). Інформаційно-аналітичне забезпечення як елемент організаційного забезпечення економічної безпеки підприємницької діяльності. *Вісник СумДУ*, (1), 47–55. https://journals.snu.edu.ua/
157. Гаркуша, В. О., & Єршова, Н. Ю. (2018). Теоретичні та методичні підходи до організаційного забезпечення економічної безпеки підприємства. *Економіка і суспільство*, (18), 333–339. https://economyandsociety.in.ua/
158. Гаркуша, В., & Єршова, Н. (2021). Систематизація наукових поглядів щодо сутності поняття «економічна безпека підприємства». *Економіка та суспільство*, (28). https://doi.org/10.32782/2524-0072/2021-28-34
159. Гончарова, М. Л. (2014). Застосування ситуаційно-адаптивного підходу до формування системи економічної безпеки вітчизняних підприємств.

Науковий вісник Херсонського державного університету, 6(2), 141–144.

160. Гриценко, М. Р. (2003). Економічна безпека банківської системи України. *Вісник Національного банку України*, (4), 27–28.
161. Денисов, А. І. (2014). Економічна безпека держави: завдання господарсько-правового забезпечення. *Вісник Національного університету «Юридична академія України імені Ярослава Мудрого»*, (2), 197–206.
162. Дидик, А. М. (Ред.). (2019). Економічна безпека підприємства (підручник). Національний університет «Львівська політехніка»; ТзОВ «Видавнича група “Бухгалтери України”». https://fpk.in.ua/images/biblioteka/3fmb_finan/Ekonomichna-bezpeka-pidpryyemstva_pidruchnyk.pdf.
163. Дуб, Б. С. (2016). Система економічної безпеки підприємства: поняття та структура. *Управління проектами та розвиток виробництва*, 4(60), 5–18.
164. Єршова, Н. Ю. (2018). Удосконалення обліково-аналітичного забезпечення економічної безпеки підприємства. У *Матеріалах 7-ї міжнародної науково-практичної інтернет-конференції «Інновації в обліково-аналітичному забезпеченні та управлінні фінансово-економічною безпекою…»* (с. 116–119). http://repository.kpi.kharkov.ua/handle/KhPI-Press/38847.
165. Захаров, О. І. (2003). Інформаційна безпека в системі стратегічного керування підприємством. *Проблеми інформатизації та управління*, (8), 80–85.
166. Зачосова, Н. В. (2011). Кадровий менеджмент у системі економічної та фінансової безпеки комерційного банку. *Сучасна економіка*, (5), 14–25.
167. Зачосова, Н. В. (2016). Формування системи економічної безпеки фінансових установ (монографія). ПП Чабаненко. 375 с.

168. Злобін, К. (2025). Сучасні підходи до оцінювання лояльності персоналу в контексті економічної безпеки. *Актуальні проблеми економіки*, (10(292)), 172–181. https://doi.org/10.32752/1993-6788-2025-1-292-172-181.
169. Злобін, К. (2024). Вплив війни в Україні на лояльність персоналу підприємств до роботодавців. *Вчені записки Університету «КРОК»,* 2(74), 217–227. https://doi.org/10.31732/2663-2209-2024-74-217-227.
170. Злобін, К., Літвін, Н., & Бурлакова, І. (2023). Вплив програм wellbeing на продуктивність та лояльність персоналу. *Вчені записки Університету «КРОК»*, 1(69), 162–170. https://doi.org/10.31732/2663-2209-2022-69-162-170.
171. Злобін, К. В. (2024). Вплив лояльності персоналу на довгострокове стратегічне планування компанії. У *Сучасний менеджмент організації: витоки, реалії та перспективи розвитку*: тези доповідей IV наукової конференції (18 квітня 2024 р.). Університет «КРОК». https://conf.krok.edu.ua/MMO/MMO-2024/paper/view/2235.
172. Злобін, К. В. (2024). Ідентифікація ризиків економічної безпеки через персонал. У Держава, регіони, підприємництво: інформаційні, суспільно-правові, соціально-економічні аспекти розвитку: тези доповідей VI міжнародної конференції (5–6 грудня 2024 р.). Університет «КРОК». https://conf.krok.edu.ua/SRE/SRE-2024/paper/view/2638.
173. Ібрагімов, Е. Е. (2015). Теоретичні підходи до виокремлення складових системи економічної безпеки підприємства. *Науковий вісник Міжнародного гуманітарного університету*, (11), 94–96.
174. Кавун, С. В. (2014). Економічна безпека підприємств. Інформаційний аспект (монографія). Щедра садиба плюс. 312 с.

175. Кавун, С. В. (n.d.). Концепція інформаційно-аналітичного забезпечення системи економічної безпеки підприємства. *Управління проектами та розвиток виробництва*, (20).
176. Кириченко, О. А., & Коробчинський, О. Л. (2009). Нормативно-правове регулювання системи економічної безпеки підприємства. *Інвестиції: практика та досвід*, (12), 31–34.
177. Кириченко, О. А., & Сідак, В. С. (2008). Проблеми управління економічною безпекою суб'єктів господарювання (монографія). УЕП «КРОК». 401с.
178. Кириченко, О. (2025). Інформаційно-аналітичні, репутаційні, цифрові, технологічні аспекти управління системою економічної безпеки підприємств, банківських установ, їх вплив та оцінювання. *Вчені записки Університету «КРОК»*, 1(77), 203–210. https://doi.org/10.31732/2663-2209-2025-77-203-210.
179. Кириченко, О. С. (2017). Класифікація загроз економічної безпеки української промисловості. *Вчені записки Університету «КРОК»*, (48), 38–47.
180. Кириченко, А. А., & Кім, Ю. Г. (2008). Методологічні основи економічної безпеки суб'єктів господарювання в трансформаційній економіці. *Актуальні проблеми економіки*, 12(90), 53–65.
181. Козаченко, Г. В., Понамарьов, В. П., & Ляшенко, О. М. (2003). Економічна безпека підприємства: сутність та механізм забезпечення (монографія). Лібра.
182. Козаченко, Г., & Пономарьов, В. (2001). Економічна безпека підприємств: сутність і передумови формування. У *Теорія та практика управління у трансформаційний період* (Т. 3, с. 3–7). Донецьк.
183. Кондратьєв, Б. О., & Єршова, Н. Ю. (2020). Інформаційне забезпечення управління діяльністю підприємства: теоретичні та практичні аспекти удосконалення. У *Матеріалах міжнародної науково-практичної*

конференції «Модернізація економіки…» (с. 418–419). http://repository.kpi.kharkov.ua/bitstream/KhPI-Press/48071/1/Kondratiev_Informatsiine_zabezpechennia_2020.pdf

184. Копитко, М. І. (2013). Аналіз теоретичних підходів до визначення поняття та складових елементів системи економічної безпеки підприємств. *Науковий вісник Херсонського державного університету*, (3), 59–64
185. Корчевська, Л. О. (2012). Системні принципи економічної безпеки підприємства. *Економіка Кр*иму, 1(38), 242–245.
186. Крамаренко, К., & Вінниченко, О. (2024). Інформаційно-аналітичне забезпечення управління фінансово-економічною безпекою суб'єктів господарювання. *Сталий розвиток економіки*, (3(50)), 344–349.
187. Кузіна, Р. В. (2015). Транспарентність корпоративної звітності як основа її формування. *Науковий вісник Херсонського державного університету*, (12), 193–197.
188. Кургуженкова, Л. А. (2015). Економічна безпека підприємства: сутність та чинники формування її відповідного рівня. *Економіка та суспільство,* (1), 31–34. https://economyandsociety.in.ua/journals/1_ukr/06.pdf
189. Лазаришина, І. Д., & Оренчин, О. В. (2012). Джерела інформаційно-аналітичного забезпечення економічної безпеки підприємства. *Вісник економіки транспорту і промисловості*, (38), 62–65.
190. Малащенко, В. (2011). Економічна безпека підприємства як чинник ефективного корпоративного управління. *Вісник Національної академії державного управління при Президентові України*, (3), 283–291.
191. Мельник, С. І. (2009). Економічна безпека банків в умовах фінансової кризи. *Науковий вісник Львівського державного університету внутрішніх справ*, (2), 278–287.

192. Мігус, І. П., & Андрієнко, В. М. (2014). Структура та основні елементи системи забезпечення економічної безпеки при управлінні безпекою праці на будівельних підприємствах. *Бізнес Інформ*, (10), 213-219.
193. Шульга І.П. (2010). Економічна безпека емісійної діяльності акціонерних товариств. Черкаси: МАКЛАУТ. 425 с.
194. Мігус, І. П. (2012). *Кадрова безпека суб'єктів господарської діяльності: менеджмент інсайдерами* (монографія). МАКЛАУТ.
195. Мігус, І. П. (2018). Створення системи управління кадровою безпекою на підприємстві. *Вчені записки Університету «КРОК»*, (4(52)), 213–221. https://doi.org/10.31732/2663-2209-2018-52-213-221
196. Мігус, І. П., Лаптєв С.М. (2011). Необхідність розмежування понять «загроза» та «ризик» при діагностиці економічної безпеки суб'єктів господарювання. Електронне наукове фахове видання «Ефективна економіка». *Режим доступу: http://www.economy.nayka.com.ua*.
197. Мігус, І. П., & Черненко, С. А. (2013). Оцінка лояльності персоналу в контексті забезпечення економічної безпеки підприємства. *Агросвіт*, (11), 24–27.
198. Мігус, І. П., Худолій, Л. М., Денисенко, М. П., & Міхно, С. П. (2012). *Корпоративне управління в системі економічної безпеки акціонерних товариств України* (монографія). Маклаут.
199. Мішин, О. Ю., & Мішина, С. В. (2012). Сутність поняття «економічна безпека підприємства». *Вісник економіки транспорту і промисловості,* (38), 86–92.
200. Наумова, О., & Копил, А. (2024). Корпоративне волонтерство як інструмент управління лояльністю стейкхолдерів організації. *Вчені записки Університету «КРОК»*, (4(76), 145–154. https://doi.org/10.31732/2663-2209-2024-76-146-154

201. Небава, М. І., & Міронова, Ю. В. (2017). *Економічна безпека підприємства* (навчальний посібник). ВНТУ. https://pdf.lib.vntu.edu.ua/books/2024/Nebava_2017_73.pdf
202. Новикова, О. Ф. (2006). Економічна безпека: концептуальне визначення та механізм забезпечення. ПАН України, Інститут економіки промисловості. 407 с.
203. Онищенко, С. В., & Глушко, А. Д. (2023). Інформаційно-аналітичне забезпечення фінансової безпеки підприємств у сучасних умовах. *Науковий вісник ОНЕУ*, 7–8(308–309), 135–154.
204. Орлик, О. (2017). Концептуальні підходи щодо визначення поняття «економічна безпека підприємства». *Сталий розвиток економіки*, 2(35), 105–110. https://www.economdevelopment.in.ua/index.php/journal/article/view/281
205. Отенко, І. П., Іващенко, Г. А., & Воронков, Д. К. (2012). Економічна безпека підприємства (навчальний посібник). ХНЕУ. 256 с.
206. Павлов, О. І. (2011). Основи інформаційно-аналітичної діяльності (навчальний посібник). Астропринт. 240 с.
207. Пархоменко, О. В. (2006). Інформаційно-аналітичне забезпечення процесу прийняття рішень в системі науково-технічної інформації (дисертація кандидата економічних наук, 08.02.02). Київ. 211 с.
208. Позднишев, Є. В. (2007). Інформаційно-аналітичне забезпечення безпеки підприємництва (методи та їх застосування) (Кн. 1). Видавець Позднишев. 89 с.
209. Позднишев, Є. В., Чергенець, Е. В., & Зайцев, А. В. (2007). Інформаційно-аналітичне забезпечення безпеки підприємництва (збір та пошук інформації) (Кн. 2). Видавець Позднишев. 74 с.
210. Позднишев, Є. В. (2007). Інформаційно-аналітичне забезпечення безпеки підприємництва (методи та їх застосування) (Кн. 1). Видавець Позднишев. 89 с.

211. Пригунов, П. Я. & Квашук, Д. М. (2015). Інформаційно-аналітичне забезпечення підприємницької діяльності в сфері економічної безпеки. *Ефективна економіка*. http://www.economy.nayka.com.ua/?op=1&z=4247.
212. Пушак, Я. М., та ін. (2021). Індикаторний підхід у галузевій безпеці агросектору. *Економіка АПК*.
213. Рудніченко, Є. М. (2013). Аналіз нормативного забезпечення системи економічної безпеки підприємств. *Вісник Хмельницького національного університету*, 5(1), 133–140.
214. Сисоліна, Н. П. (2014). *Економічна безпека підприємства*. ХНУРЕ. https://core.ac.uk/
215. Сорока, Р. С., & Сорока, М. П. (2012). Значення інформаційно-аналітичної діяльності в забезпеченні економічної безпеки підприємства. *Науковий вісник НЛТУ України*, 22(13), 317–322.
216. Президент України. (2021, 28 грудня). Стратегія інформаційної безпеки (Указ Президента України № 685/2021). https://www.president.gov.ua/documents/6852021-41069
217. Уразалієв, Р. М., & Васильців, Т. Г. (2011). Узагальнення концептуальних основ економічної безпеки підприємств. *Науковий вісник НЛТУ України*, 21(2), 153–158.
218. Харченко, В. В. (2011). Підходи до трактувань інформаційного забезпечення. *Науковий вісник Національного університету біоресурсів і природокористування України*, 168(3), 145–148.
219. Хвальчик, І. Л., & Волощук, Л. О. (2020). Сутність інформаційно-аналітичного забезпечення управління. *Економіка: реалії часу*, 1(47), 84–90. https://economics.opu.ua/files/archive/2020/No1/84.pdf
220. Худолій, Л. М. (2011). Складові економічної безпеки суб'єктів господарської діяльності. *Ефективна економіка*. http://www.economy.nayka.com.ua/?op=1&z=455.

221. Цікановська, Н. А. (2013). Інтерпретація понять «виклик», «небезпека», «загроза» та «ризик» у теорії фінансової безпеки. *Фінансовий простір*, (3), 110–114.
222. Шинкар С. М. (2018). Організаційно-економічний механізм забезпечення економічної безпеки промислових підприємств : Кандидат економічних наук : спец.. 21.04.02 - Економічна безпека суб'єктів господарської діяльності : дата захисту 2018-12-11; Статус: Захищена; Українська академія друкарства. Львів, 0418U005145.
223. Шульга, І. П. (2010). Економічна безпека підприємства як економічна категорія. *Академічний огляд*, 2(33), 37–44. https://acadrev.duan.edu.ua/images/PDF/2010/2/5.pdf
224. Шемаєва, Л. Г. та Мігус, І. П. та Шемаєв, В. М. та Шемаєв, В. В. та Мельник, Л. М. (2020). Застосування моделі наскрізної оптимізації фінансових і матеріальних потоків у механізмі забезпечення фінансової безпеки на підприємствах оборонної промисловості. *Фінансово-кредитна діяльність: проблеми теорії та практики.* 2(33), 400–410. https://doi.org/10.18371/fcaptp.v2i33.207078.

ДОДАТОК А

etg.ua незалежний провайдер енергії

Печерський район, вулиця
Івана Мазепи, 6
Київ, Україна, 01010
info@etg.ua

+380 (44) 337-74-28
центральний офіс
+380 (44) 390-99-89
контакт-центр

Вхід на сайт
etg.ua

вих. № 345/КП від 27.11.2025

ДОВІДКА
про впровадження результатів дисертаційного дослідження на тему «Інформаційно-аналітичне забезпечення оцінювання лояльності персоналу в системі економічної безпеки промислових підприємств» аспіранта кафедри управлінських технологій ВНЗ «Університет економіки та права «КРОК» за спеціальністю 073 «Менеджмент» Злобіна Кирила Васильовича

Керівництво Товариство з обмеженою відповідальністю «ЕНЕРДЖІ ТРЕЙД ГРУП», далі за текстом ТОВ «ЕНЕРДЖІ ТРЕЙД ГРУП», розглянувши матеріали дисертаційного дослідження Злобіна К.В., підтверджує практичну значущість отриманих результатів та доцільність їх використання у системі управління економічною безпекою підприємства.

У діяльність ТОВ «ЕНЕРДЖІ ТРЕЙД ГРУП» впроваджено методичні положення оцінювання стану економічної безпеки підприємства на основі інтегрального індексу, що формується як зважене поєднання кількісного та якісного блоків. У межах впровадження забезпечено використання відкритих джерел даних, а саме річної або квартальної фінансової звітності, аудиторського звіту та приміток, що підвищує відтворюваність розрахунків і придатність результатів для порівняння в часі. Окремо застосовано підхід до врахування якісних ознак, що зчитуються з аудиторського звіту та приміток, зокрема щодо думки аудитора, ковенантів і графіка погашень, юридичних і регуляторних ризиків, клієнтського та кредитного ризику, операційної безперервності та якості фінансового розкриття. Для управлінського використання в організації запроваджено інтерпретацію результатів за єдиною шкалою категорій економічної безпеки з прив'язкою до мінімальних умов та типових управлінських дій, а також із визначеною частотою перегляду результатів. Результати оцінювання інтегровано в регулярні аналітичні матеріали для керівництва, включно з моніторингом сигналів раннього попередження і формуванням пріоритетів управлінських заходів.

Впровадження результатів дослідження забезпечило підвищення обґрунтованості управлінських рішень щодо рівня економічної безпеки, та уніфікацію підходів до інтерпретації ризикових станів. Запропоновані положення рекомендовано до подальшого використання в ТОВ «ЕНЕРДЖІ ТРЕЙД ГРУП» та можуть бути адаптовані для інших підприємств відповідної галузі.

Директор ТОВ «ЕНЕРДЖІ ТРЕЙД ГРУП» _____ Євген ФРАНЧИК

ЄДРПОУ: 36716332; ІПН 367163326584 п/р № UA193204780000026000924417793

ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ
«ПАУЕР ДЕВЕЛОПМЕНТ»
01010, місто Київ, вулиця Мазепи Івана, будинок 6
ЄДРПОУ 45408714
тел.+38 044 3377428

вих. 54 від 05.12.2025

ДОВІДКА
про впровадження результатів дисертаційного дослідження на тему «Інформаційно-аналітичне забезпечення оцінювання лояльності персоналу в системі економічної безпеки промислових підприємств» аспіранта кафедри управлінських технологій ВНЗ «Університет економіки та права «КРОК» за спеціальністю 073«Менеджмент» Злобіна Кирила Васильовича

Керівництво Товариство з обмеженою відповідальністю «ПАУЕР ДЕВЕЛОПМЕНТ», далі за текстом ТОВ «ПАУЕР ДЕВЕЛОПМЕНТ», розглянувши матеріали дисертаційного дослідження Злобіна К.В., підтверджує практичну значущість отриманих результатів та доцільність їх використання у системі управління економічною безпекою підприємства і кадровими ризиками.

У діяльність ТОВ «ПАУЕР ДЕВЕЛОПМЕНТ» впроваджено рекомендації щодо оцінювання лояльності персоналу як чинника стабільності операцій і зниження ризиків, із застосуванням комбінування кількісних та якісних інструментів. У практиці роботи ТОВ «ПАУЕР ДЕВЕЛОПМЕНТ» використано стандартизовані опитування та анкети, аналіз показників плинності кадрів і відсутностей, інтерв'ю та фокус-групи, а також контент-аналіз внутрішніх каналів зворотного зв'язку з подальшим відображенням результатів у аналітичних панелях. Отримані результати застосовуються для уточнення кадрових ризиків у профілі економічної безпеки, для планування заходів утримання критичних компетенцій та для підвищення узгодженості рішень між HR-функцією і функцією економічної безпеки.

Впровадження результатів дослідження забезпечило підвищення обґрунтованості управлінських рішень щодо рівня кадрової безпеки, уніфікацію підходів до інтерпретації ризикових станів та посилення доказової бази кадрових рішень у частині управління лояльністю персоналу. Запропоновані положення рекомендовано до подальшого використання в практиці ТОВ «ПАУЕР ДЕВЕЛОПМЕНТ» та можуть бути адаптовані для інших підприємств відповідної галузі.

Директор ТОВ «ПАУЕР ДЕВЕЛОПМЕНТ» _____ Святослав БАЗИЛЕВСЬКИЙ

М.П.

RISK CONTROL
ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ
"РИЗИК КОНТРОЛЬ" (ЕГРПОУ 43833882)

Україна, 0830, Київська обл., Бориспільський р-н, місто Бориспіль, вул. Старокняжицька, буд. 1, офіс 272-273. тел. +38(097)-110-86-39, +38(095)-466-22-05. www.risk-control.com.ua, E-mail: info@risk-control.com.ua.

Вих. 3012/1-25
від 30.12.2025 р.

ДОВІДКА
про впровадження результатів дисертаційного дослідження на тему «Інформаційно-аналітичне забезпечення оцінювання лояльності персоналу в системі економічної безпеки промислових підприємств» аспіранта кафедри управлінських технологій ВНЗ «Університет економіки та права «КРОК» за спеціальністю 073«Менеджмент» Злобіна Кирила Васильовича

Керівництво компанії ТОВ «РИЗИК КОНТРОЛЬ» розглянувши матеріали дисертаційного дослідження Злобіна К.В. на тему «Інформаційно-аналітичне забезпечення оцінювання лояльності персоналу в системі економічної безпеки промислових підприємств», підтверджує доцільність їх використання в контексті оцінювання економічної безпеки підприємств у процесах скринінгу, моніторингу та управлінського реагування.

Доцільність застосування обґрунтовується тим, що в дисертації сформовано цілісний підхід до оцінювання економічної безпеки як керованого процесу, що спирається на інформаційно-аналітичне забезпечення та практичні індикатори.

У дослідженні запропоновано інтегральний індекс економічної безпеки S, який поєднує кількісну та якісну оцінку, що дозволяє враховувати як фінансові результати, так і якість розкриття інформації та сигнали ризику з аудиторського звіту. Запропонована методика орієнтована на відкриті джерела даних і тому придатна для практичного застосування на підприємствах та для зовнішнього порівняльного аналізу.

Для управлінського використання запропоновано шкалу інтерпретації значень індексу S з категоріями стану економічної безпеки та прив'язкою до базових управлінських дій і частоти перегляду результатів, що перетворює розрахунок на інструмент прийняття рішень. Додатково враховано кадровий чинник через оцінювання лояльності персоналу як елементу ризикового профілю підприємства, що підвищує повноту діагностики економічної безпеки.

В ході вивчення матеріалів Злобіна К.В., встановлено, що результати дисертаційного дослідження та запропоновані методики, дозволяють підвищити ефективність всіх функціональних складових економічної безпеки промислових підприємств, що дає змогу їх використання в аналітичній та консалтинговій діяльності компанії ТОВ «РИЗИК КОНТРОЛЬ».

Директор ТОВ «РИЗИК КОНТРОЛЬ» Віктор КОРЖЕВСЬКИЙ

ДОДАТОК Б

Додаток Б.1

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА

Публікації, в яких опубліковані основні наукові результати дисертації:

1. Злобін К. (2025). Сучасні підходи до оцінювання лояльності персоналу в контексті економічної безпеки. Актуальні проблеми економіки. № 10 (292), жовтень, 2025. DOI: 10.32752/1993-6788-2025-1-292-172-181
2. Zlobin, K. (2025). Model of Integration of Loyalty Assessment Results into the Threat Management System of the Economic Security of an Industrial Enterprise. In P. Kolisnichenko (Ed.),Insider threats and security in corporations.274p. (pp. 181–203). Scientific Center of Innovative Research. DOI: https://doi.org/10.36690/ITSC-181-203
3. Злобін К. Вплив війни в Україні на лояльність персоналу підприємств до роботодавців / К. Злобін // Вчені записки Університету "КРОК". - 2024. - № 2(74), С. 217–227. – DOI: https://doi.org/10.31732/2663-2209-2024-74-217-227.
4. Zlobin K. Information and analytical support and tools for assessing employee loyalty in enterprises / K. Zlobin // Economics, Finance and Management Review. - 2024. - № 2(18), P. 60–72. – DOI: https://doi.org/10.36690/2674-5208-2024-2-60-72.
5. Злобін К. Вплив програм wellbeing на продуктивність та лояльність персоналу / К. Злобін, Н. Літвін, І. Бурлакова // Вчені записки Університету "КРОК". - 2023. - № 1(69), С. 162–170. – DOI: https://doi.org/10.31732/2663-2209-2022-69-162-170.

Публікації, які засвідчують апробацію матеріалів дисертації:

1. Zlobin K. The impact of involving employees in decision-making on increasing the loyalty of the company's personnel/ K. Zlobin // International Conference on Corporation Management: abstracts of reports of a 4th International Conference (April 26, 2024). - Estonia, 2024 https://conf.scnchub.com/index.php/ICCM/ICCM-2024/paper/view/740/208
2. Злобін К.В. Ідентифікація ризиків економічної безпеки через персонал. / К.В. Злобін // Держава, регіони, підприємництво: інформаційні, суспільно-правові, соціально-економічні аспекти розвитку: тези доповідей VI Міжнародної конференції (грудень 5-6, 2024). - Київ: Університет "КРОК", 2024. https://conf.krok.edu.ua/SRE/SRE-2024/paper/view/2638
3. Злобін К.В. Вплив лояльності персоналу на довгострокове стратегічне планування компанії / К.В. Злобін // Сучасний менеджмент організації: витоки, реалії та перспективи розвитку: тези доповідей IV Наукової конференції (18 квітня 2024 р.). - Київ: Університет "КРОК", 2024. https://conf.krok.edu.ua/MMO/MMO-2024/paper/view/2235
4. Zlobin K. Personnel well-being as a component of the social policy of the company / K. Zlobin // Relationship between public administration and business entities management: abstracts of reports of a 3nd International Conference (November 24, 2023). - Estonia, 2023. https://conf.scnchub.com/index.php/RPABM/RPABM-2023/paper/view/600/83

Додаток Б.2

ВІДОМОСТІ ПРО АПРОБАЦІЮ РЕЗУЛЬТАТІВ ДИСЕРТАЦІЇ

- Міжнародна науково-практична конференція «4th International Conference on corporation management» (2024, заочна форма участі);
- Міжнародна науково-практична конференція «Relationship between public administration and business entities managemen» (2023, заочна форма участі);
- Держава, регіони, підприємництво: інформаційні, суспільно-правові, соціально-економічні аспекти розвитку (2024, очна форма участі);
- International Conference on Corporation Management (2020, участь онлайн);
- Науково-практична конференція «Сучасний менеджмент організації: витоки, реалії та перспективи розвитку» (2024, очна форма участі).

Додаток В

Таблиця В.1

Основні трактуванні поняття «економічна безпека підприємства»

№	Автор(и), рік	Ключова ідея	Коментар/критика
1	Козаченко Г.В., Пономарьов В.П., Ляшенко О.М. (2003)	ЕБП як бінарна конструкція: стан захищеності інтересів + механізм забезпечення; інтересоцентричність.	Міцний інституційний каркас; потрібні сучасні KRI/EWI та правила data governance.
2	Сисоліна Н.М. (2014)	ЕБП як система управлінських заходів зі стійкістю й розвитком як результатом; процесний цикл.	Переконлива процесність; бракує карти даних і порогів ризику.
3	Небава М.І., Міронова Ю.В. (2017)	ЕБП як управлінська підсистема: діагностика загроз, інтегральна оцінка; ролі, регламенти, документування.	Сильна рамка; посилити цифрову частину ІАЗ і інтеграцію з ERP/MES/SCM/HRIS.
4	Дідик О. (ред.) (2020)	Навчально-методичний каркас мікрорівня безпеки; уніфікація понять, структур загроз, принципів.	Корисна «карта місцевості»; бракує глибини в аналітиці та data governance.
5	КНТЕУ (2021)	ЕБП як система мобілізації ресурсів задля стійкості; підзвітність витрат на безпеку.	Ресурсна дисципліна важлива; потрібні випереджальні індикатори та сценарії.
6	Кургузенкова Н.М. (2015)	ЕБП як стан і спроможність нейтралізації дестабілізаторів; акцент на capability.	Влучна оптика; необхідна чітка метризація через KRI/EWI.
7	Дуб Б.С. (2016)	Системний підхід: принципи, функції, декомпозиція підсистем, розподіл відповідальності.	Кістяк системи; без потокових індикаторів і BI-панелей ризик декларативності.
8	Шульга О.В. (2010)	Інституційний ракурс: ЕБП як система економічних відносин захисту інтересів.	Легітимність і підзвітність; кількісні ризик-метрики розкриті стисло.
9	Орлик С.В. (2017)	Фінансове ядро ЕБП (ліквідність, платоспроможність, рентабельність) з прив’язкою до P&L/CF.	Фінансовий фокус сильний; бракує HR/операційних та інформаційних складових.
10	Панченко В.В. (2017)	ЕБП як управлінський напрям у логіці стейкхолдерів і процесів; імплементація у системи менеджменту.	Переконливо; слід формалізувати ролі даних, SLA аналітики та пороги ескалації.
11	Шмалій О.В. (2019)	ЕБП як комплексна здатність інтегрувати ризики й ресурси (рух до резилієнсу).	Є інтегральність; потрібні галузеві KRI та перевірки стабільності індексів.
12	Меліхова Т.О. (2018)	ЕБП як організаційно-контрольна система для ефективності та розвитку.	Контроль дисциплінує; без предиктивної аналітики можливе запізнення реакцій.
13	Архипенко О., Іванова Т. (2021)	Систематизація еволюції дефініцій ЕБ/ІАЗ; теоретичний базис.	Корисно для теорії; цифрові ризики, етика даних і XAI потребують розширення.
14	Шинкар І.В. (2020)	ЕБП як безперервний процес із критеріями оцінювання; узгоджено з ERM.	Процесність глибока; додати моделі зрілості ІАЗ і тригери KRI/EWI.
15	Пушак Я.Я. та ін. (2021)	Галузева індикаторна система ІАЗ для агросектору з інтегральною оцінкою.	Предметність висока; для інших галузей потрібна адаптація індикаторів.

№	Автор(и), рік	Ключова ідея	Коментар/критика
16	Алькема В.Г. (2024)	Управлінсько-методологічні засади ЕБП; інституціоналізація процесів та стандартизація інформаційних потоків.	Посилений управлінський контур; додати вимоги до якості/лінійності даних і формальні KRI/EWI.
17	Кириченко О.С. (2008-2009)	Концепція управління системою ЕБ і цифровізація ІАЗ (інфраструктура, автоматизація, захист, big data).	Релевантно; потрібні власники індикаторів, пороги/частоти та контроль стабільності моделей.
18	Лаптєв С.М. (2012)	Організаційно-економічні механізми ЕБП і підготовка рішень на основі аналітики.	Механізми продумані; варто посилити ХАІ і політики приватності для HR/поведінкових даних.
19	Зачосова Н.В. (2016)	Фінансово-страховий вимір ЕБП: інтеграція у загальну архітектуру безпеки.	Сильний фінансовий/комплаєнс-акцент; зшити з OT/SCADA-даними та нефінансовими KRI.
20	Андрієнко В.М. (2014)	Методики оцінювання рівня ЕБП і системи показників у зв’язку з управлінськими циклами.	Індикаторна логіка виважена; потрібні сценарні пороги, ескалації та перевірка стабільності.

Джерело: систематизовано автором на основі [145-224]

Таблиця В.2

Основні трактуванні поняття «інформаційно-аналітичне забезпечення економічної безпеки підприємства»

№	Автор, рік	Парафраз	Коментар/критика
1	Кавун, 2016	ІАЗ ЕБ як цілісна система збирання, обробки й інтерпретації даних для ідентифікації загроз і підтримки рішень.	Системно; бракує сучасної архітектури (lakehouse) і потокових EWI/KRI.
2	Воронюк, 2021	ІАЗ як організаційний елемент: потоки інформації, показники, правила доступу та відповідальність.	Чітка регламентація; потрібні формалізовані EWI/KRI й пороги ескалації.
3	Крамаренко, 2024	ІАЗ як BI/DSS-методи, що перетворюють внутрішні/зовнішні дані на сигнали ризику для превентивних дій.	Техно-сильний; додати XAI та етичні обмеження для HR-даних.
4	Небава & Міронова, 2017	Управлінська підсистема моніторингу, діагностики та інтегральної оцінки рівня безпеки.	Логіка переконлива; посилити якість/трасованість і інтеграцію з ERP/MES/SCM/HRIS.
5	Дуб, 2016	Системний контур принципів, функцій і ролей (risk owner, аналітик, аудитор).	Карта корисна; без потокових індикаторів і data governance ризик декларативності.
6	Онищенко & Глушко, 2023	Фінансова грань ІАЗ: процедури/метрики (KRI, LCR, DSCR), що зшивають облік, аналіз і контроль.	Добра фінансова деталізація; інтегрувати OT/IT-ризики й нефінансові тригери.
7	Краєвський, 2020	Обліково-аналітична база для вимірювання рівня безпеки через систему показників і звітності.	Сильна P&L/CF-прив'язка; додати випереджальні індикатори та сценарії.
8	Мішчук та ін., 2021	Галузева карта даних (гірнича справа) для моніторингу економічної безпеки.	Висока предметність; потрібна методична уніфікація для інших галузей.
9	Мігус, 2013	HR-вимір: опитувальні та поведінкові дані лояльності як вхід у контур безпеки.	Валідно; додати приватність/етику та XAI-пояснюваність.
10	Архипенко & Іванова, 2021	ІАЗ як еволюційний конструкт інституцій, механізмів і метрик забезпечення безпеки.	Історіографічно корисно; цифрові ризики та governance стисло.
11	Єфіменко, 2024	ІАЗ лояльності: структуровані метрики прихильності, інтегровані в ризик-контур.	Логічно; додати поведінкові логи та етичні запобіжники.
12	Дідик (ред.), 2020	Стандартизоване понятійне поле й процедури для однорідності оцінок безпеки.	Фундамент є; потрібні цифрові SLA та моніторинг дрейфу даних.
13	Шинкар, 2020	Процесно-критеріальна конструкція: критерії рівня безпеки, що живляться даними моніторингу.	Добре; додати зрілість ІАЗ і пороги ескалації.
14	Пушак та ін., 2021	Галузева індикаторна система ІАЗ для агросектору (якість, врожайність, ризики ланцюгів).	Сильно для агро; генералізація потребує адаптації індикаторів.
15	Захаров, 2019	ЕБ і система ЕБ як пов'язані, але відмінні; модель суб'єктів безпеки; ІАЗ як основа виявлення загроз і порогового контролю.	Сильна інституційна рамка; додати сучасний data governance, потокові EWI/KRI та XAI-валідації.
16	Гнилицька, 2012	Обліково-аналітична парадигма ІАЗ: стандартизація управлінської інформації, контроль якості даних, побудова показників для моніторингу.	Міцна база метризації; розширити на OT/IoT, формалізувати пороги/ескалації та політики приватності.

№	Автор, рік	Парафраз	Коментар/критика
17	Кириченко, 2012	Концепт управління системою ЕБ; акцент на цифрових технологіях ІАЗ, інфраструктурі даних та автоматизації збору/оброблення.	Релевантно; уточнити вимоги до KRI/EWI (власники/пороги/частоти) і лінійність даних, тест стабільності моделей.
17	COSO, 2017	Блок «інформація–комунікація–звітність» як ядро ІАЗ в ERM для ризик-рішень.	Базові принципи; для індустрії додати OT/IoT-джерела.
18	ISO 31000, 2018	Структурована інформаційна підтримка ідентифікації, аналізу, оцінки та моніторингу ризиків.	Універсально; необхідна локальна метризація EWI/KRI.
19	ISO/IEC 27001, 2022	Дані для менеджменту інформаційних ризиків: контроли, аудит, поліпшення.	Фокус ІБ; зв’язати з економічними KPI та ЕБ-панелями.
20	DAMA-DMBOK, 2017	Data governance, якість і метадані як основа довірчої аналітики ІАЗ.	Ідеальна «прошивка»; доменні KRI визначати локально.
21	Hollnagel та ін., 2011/2017	Індикатори резилієнсу: anticipate–monitor–respond–learn як сенсорика ІАЗ.	Концептуально сильно; потрібні промислові проксі-метрики.
22	Armbrust та ін., 2021	Lakehouse як платформа ІАЗ для уніфікації DWH/Lake і продвинутої аналітики.	Технічно переконливо; додати XAI й чіткі правила доступу.
23	Jain та ін., 2023	Керовані сховища (Delta/Hudi/Iceberg) для відтворюваної аналітики ризику.	Ядро сильне; потрібні управлінські SLA та ролі.
24	NC State ERM Initiative, n.d.	Система EWI/KRI з порогами та заздалегідь визначеними діями.	Прикладно; формалізувати ескалації та власників даних.
25	AuditBoard, 2024	Методика побудови KRI: релевантність, пороги, валідація, частота.	Практично; обмежена академічна верифікація.
26	Thomson Reuters, 2025	Оглядова рамка KRI: типи (leading/lagging), частота, власники.	Корисно; потребує локальної адаптації під процеси.
27	Deloitte, 2020–2024	Операційні ризик-панелі з інтеграцією джерел і сценаріями реагування.	Best-practice; у науці позначати межі корпоративних гайдів.
28	CERT/SEI (Collins та ін.), 2016	Поведінкові індикатори інсайдерських загроз і кейс-аналітика як елемент ІАЗ.	Важливо для HR/ІБ; додати етичні/приватнісні протоколи.
29	Meyer & Allen, 1991	Метрики організаційної прихильності як вхід до ризик-панелей ЕБ.	Класика HR; потрібна локальна валідизація/адаптація.
30	Jüttner, 2005	Розвідка ланцюгів постачання та KRI SCM у мережевому вимірі.	Релевантно для промисловості; додати OT-сенсори/телеметрію.
31	MetricStream, 2025	GRC-оркестрація: карта ризиків, KRI, події та контрольні тести в єдиній системі.	Зручний шаблон; академічна нейтральність помірна.

Джерело: систематизовано автором на основі [145-224]

Таблиця В.3

Основні трактуванні поняття «управління персоналом»

№	Автор (APA)	Формула визначення (парафраз)	Ключовий акцент / підхід
1	Balabanova, L. V., & Sardak, O. V.	Функція менеджменту, що як система підсистем (планування, добір, розвиток, оцінювання, мотивація) забезпечує досягнення цілей.	Адміністративно-функціональний; системний
2	Krushelnytska, O. V., & Melnychuk, D. P.	Наука і практика керування людьми через політики, процедури і моделі для організаційної результативності.	Процесно-нормативний; стратегічний
3	Khmil, F. I.	Управлінська діяльність із формування, розвитку та використання трудового потенціалу організації.	Функціональний; трудовий потенціал
4	Danyuk, V. M., Kolot, A. M., et al.	Підсистема загального менеджменту: регламенти, ролі й процеси, узгоджені зі стратегією та соціально-трудовою політикою.	Стратегічний; стейкхолдерський
5	Nykyforenko, V. H.	Перехід від адмін-схем до модельованих процесів організації кадрової роботи для керованості й вимірності.	Процесний; керованість
6	Shubalyi, O. M., Rud, N. T., Hordiychuk, A. I., et al.	Методологічно окреслена рамка: планування, формування/розвиток, рух/утримання, оцінювання, мотивація, умови праці.	Процесно-регламентний
7	Oliinyk, S. U.	Система концептів і механізмів менеджменту «людського чинника» з акцентом на узгодженість політик і розвиток компетенцій.	Концептуально-методологічний; компетентнісний
8	Hurbyk, Yu. Yu., & Bahunts, O. S.	Складова загального менеджменту з шістьма базовими елементами: методологія, політика, залучення, оцінка, розміщення/мотивація, навчання.	Комплексний; процесний
9	Vynohradskyi, M. D.	Соціосистемне управління персоналом із фокусом на суб’єктність працівника та компетентнісні виміри.	Соціосистемний; компетентнісний
10	Djakiv, O. P., et al.	Організація кадрової роботи для формування, розвитку, мотивації, оцінювання й утримання персоналу.	Процесний; утримання
11	Hnylytska, L. V.	УП спирається на обліково-аналітичну підтримку рішень: стандартизація даних, показники результативності, контроль якості інформації.	Аналітично-цифровий; data-driven
12	Voroniuk, Ye. V.	Елемент організації підприємницької діяльності з інформаційно-аналітичною підтримкою кадрових рішень.	Аналітичний; прикладний
13	Armstrong, M.	Стратегічний, інтегрований і узгоджений підхід до зайнятості, розвитку та добробуту людей в організаціях.	Стратегічний; інтегрований HRM
14	Boxall, P., & Purcell, J.	Сукупність діяльностей із управління трудовими відносинами у фірмі як цілісна система практик.	ER/стейкхолдерський; системний
15	Watson, T. J.	Управлінське використання зусиль, знань, здібностей і відданої поведінки в обміні зайнятістю.	Поведінковий; критична перспектива

№	Автор (APA)	Формула визначення (парафраз)	Ключовий акцент / підхід
16	Dessler, G.	Політики та практики добору, навчання, винагород і оцінювання як «людський вимір» менеджменту.	Процедурний; функціональний
17	Mathis, R. L., & Jackson, J. H.	Комплекс політик/процедур щодо залучення, розвитку, оцінки та винагород, зорієнтований на результативність і комплаєнс.	Процесно-нормативний
18	Storey, J.	Відмінні підходи HRM (soft/hard) для формування конкурентних переваг через залучення та компетентність.	Стратегічний; soft/hard HRM
19	Wright, P. M., & McMahan, G. C.	Зв'язування HR-практик зі стратегією через поведінкові, кібернетичні, агентські та RBV-перспективи.	Стратегічний HRM; RBV
20	Beer, M., Spector, B., Lawrence, P., Mills, D. Q., & Walton, R. E.	HRM як поліцентричне поле політик і практик із балансом інтересів стейкхолдерів та часових горизонтів.	Гарвардська модель; стейкхолдерський
21	Wilton, N.	HRM як «парасольковий» термін управління трудовими відносинами з фокусом на бізнес-партнерстві й цінності.	Бізнес-партнерство; аналітика
22	Bratton, J., & Gold, J.	Теорія і практика HRM як інтеграція структурних, культурних і агентних чинників у праці.	Соціотехнічний; критичний
23	Torrington, D., Hall, L., & Taylor, S.	Інструментальна рамка практик HRM у циклі «залучити-розвинути-утримати».	Функціональний; процесний
24	Ulrich, D., & Brockbank, W.	HR як архітектор цінності та бізнес-партнер, що поєднує людей, стратегію, процеси.	Стратегічний; value-based
25	Guest, D. E.	Модель HRM і продуктивності: узгодження цілей, інтеграція практик, організаційні результати.	Performance-oriented; інтеграція
26	Schuler, R. S., & Jackson, S. E.	Стратегічний HRM: узгодження HR-практик із конкурентною стратегією (cost/quality/innovation).	Стратегічний; контингентність
27	Pfeffer, J.	«High-commitment» HRM як джерело стійких переваг через залучення та довіру.	High-commitment; RBV
28	Delery, J. E., & Doty, D. H.	Типології HRM і зв'язок із ефективністю: універсалізм, контингентність, конфігурації.	Теоретична типологія; стратегічний
29	Becker, B. E., & Huselid, M. A.	«HR Scorecard»: вимірювання внеску HR у стратегію й результати бізнесу.	Аналітичний; performance
30	Noe, R. A., Hollenbeck, J. R., Gerhart, B., & Wright, P. M.	HRM як інтегрований цикл практик, що перетворює людський капітал на стійку результативність.	Інтегрований; людський капітал

Джерело: систематизовано автором на основі [1-145]

Таблиця В.4

Узагальнення сучасних підходів до оцінювання персоналу в контексті економічної безпеки

№	Підхід	Сутність (коротко)	Об’єкт / мета	Методи / дані (ключові)	Приклади EWI	Приклади KRI	Governance / етика	Типові ризики	Кроки впровадження (стисло)	Ілюстративний ефект
1	Компетентнісний і результативний	Зіставлення профілів компетентностей критичних ролей із результативністю процесів та ризик-метриками	Критичні ролі (OT/SCADA, енергетика, технологи); мета – зменшення людських відхилень, браку, простоїв	Job analysis, карти компетенцій, BARS/спостереження, робочі проби/симуляції, сертифікації HSE/ІБ; дані: HRIS/LMS, QMS, MES/SCADA, SPC	Прострочені допуски; «просідання» тестів; дрібні відхилення параметрів; дисбаланс компетенцій у зміні	Scrap rate; FPY; OEE; години простоїв з кадрових причин; інциденти через дефіцит навичок	Паспорти індикаторів; прозорі критерії; аудит недискримінаційності	Формалізм; «метрики без процесу»; відрив HR-оцінки від виробництва	Профілювання ролей → мінімальний набір компетенцій/допусків → зв’язування з KPI/OKR → регулярна переатестація → пороги та playbooks	−35% браку; −28% простоїв після закриття «дірки» в сертифікаціях
2	Процесно-нормативний (life-cycle)	Дзеркальне накладання контролів на J-M-L: до/під час/після найму	Усі етапи життєвого циклу працівника; мета – запобігання інсайдерським інцидентам, помилкам доступу	Checklists J-M-L; RBAC/ABAC; SoD; критичні ролі; IAM/SIEM-логи; HRIS	Прострочені скринінги; «висячі» доступи; затримки деактивацій; аномальні запити на підвищення прав	Порушення SoD; частка запізнілих деактивацій; інсайдерські інциденти; повторні кейси	RACI HR/IT/ІБ/бізнес; SLA/OLA; журнали ескалацій	«Паперова відповідність»; розриви HR↔IT/ІБ; відсутність часових норм	Інвентаризація контролів → шаблони → автоматизація J-M-L → доступ-рев’ю → тестування SLA (table-top)	Зниження часу деактивації 48→4 год; −60% інцидентів доступу
3	Ризик-орієнтований і галузевий	Вбудовування оцінювання у ERM-цикл, сценарії впливу людського чинника	Ролі/процеси з високою експозицією; мета – зменшення резидуального ризику	Карти ризиків, bow-tie, heat-maps; FMEA/HIRA; stress-тести; реєстри ризиків; OT/HSE-дані	Тренди near-miss; зростання понаднормових у критичних змінах; «розігрів» SPC-карт	Індекс інцидентів/200 тис. год; резидуальний ризик; MTTR після помилок персоналу	Комітети ризиків; квартальні рев’ю карт; прив’язка до бюджетів та BCM	Надмірна агрегованість без дій; ігнорування поведінкових драйверів	Мапа HR-KPI ↔ KRI; сценарні матриці змін/дільниць; канбан контролів; ROI контрзаходів	Переналаштування графіків → −45% простоїв із кадрових причин
4	Аналітичний (data-driven) і предиктивний	HR-аналітика, предиктивні моделі та XAI для ранніх попереджень і керованих втручань	Конверсія розрізнених HR/LMS/HSE/OT/IT-логів у попереджувальні сигнали	DWH/Lakehouse; feature store; часові ряди/класифікації; SHAP/LIME; моніторинг дрейфу; кореляція HR-подій з SIEM/OT	Індекс втоми; аномалії доступу (час/локація); «просідання» дисципліни тренінгів; ранні патерни відтоку	MTTD/MTTR; % хибних спрацювань; частка інцидентів, попереджених EWI; втрати від помилок	Data governance; аудит справедливості; DPIA/PIA; журнал рішень	«Чорні скриньки»; спуріозні зв’язки; зсуви вибірки; проксі-дискримінація	Каталог даних/паспорт метрик → пілоти з XAI → пороги/playbooks → MLOps (дрейф/ретрейн) → ex-post ефективність	Модель «втоми» → −18% дефектів; −22% MTTR
5	Поведінковий та інтегративний (лояльність/залученість)	Поєднання опитувальних шкал прихильності з поведінковими даними та результативністю	«М’які» ризики: вигорання, ерозія культури безпеки, девіантна поведінка	Pulse-опитування; культурні індекси; HSE-події; журнали порушень; табелювання; CFA/α	Падіння залученості у критичних змінах; комбо понаднормові+абсентеїзм; часті near-miss	Дисциплінарні кейси; плинність у критичних ролях; страйкові дні; HSE-інциденти	Анонімність/псевдонімізація; «just culture»; заборона репресивного використання	Соцбажаність відповідей; «втома» від опитувань; редукція до одного індексу	Календар pulse → інтеграція з логами → гіпотези інтервенцій → перевірка до/після (CBA)	Перекроювання графіків + лідерські сесії → −30% HSE-порушень

№	Підхід	Сутність (коротко)	Об’єкт / мета	Методи / дані (ключові)	Приклади EWI	Приклади KRI	Governance / етика	Типові ризики	Кроки впровадження (стисло)	Ілюстративний ефект
6	Організаційний аналіз мереж (ONA) і соціальна надійність	Картографування внутрішніх мереж для виявлення «одиничних точок відмови» знань і координації	Експертні вузли, перетини процесів/змін, власники високих доступів	Centrality/betweenness; карти компетенцій; анонімізовані комунікаційні метадані; протоколи зміни	Надмірна централізація на одній особі; черги на консультації; падіння дублювання навичок	Mean time to competency; частка ролей без резерву; інциденти через втрату експертизи	Межі приватності (метадані, не контент); добровільність; анти-«соцскоринг»	Стигматизація «вузлів»; помилки через неповні дані; плутання ризику з координацією	Інвентаризація критичних знань → ONA-картування → плани наступництва/менторство → контроль дублювання	Shadowing + подвійне закріплення → −33% часу відновлення
7	Етичний і комплаєнс-орієнтований	Легітимність, пропорційність і пояснюваність оцінювання; мінімізація даних і антидискримінація	Підвищення довіри та правової стійкості; уникнення «чорних скриньок»	DPIA/PIA; RBAC/ABAC; speak-up/whistleblowing; аудит упереджень; журнали рішень; ретенція	Скарги/апеляції; сигнали упередженості; інциденти приватності	Скасовані кейси через процедурні помилки; суми штрафів/претензій; частка рішень без пояснення	Ролі DPO/CISO; комітети етики даних; аудити відповідності; етика аналітики	«Гіпер-комплаєнс»; декларативні кодекси без нагляду	Рамки приватності/етики → паспорти показників з XAI-вимогами → канали викривачів → fairness-аудити → огляди ретенції	+40% ранніх повідомлень; −25% правових ескалацій

Примітка: EWI – випереджальні індикатори; KRI – ключові ризик-показники.

Джерело: систематизовано автором на основі [145-224]

Таблиця В.5

Сучасні підходи до трактування поняття «лояльність персоналу»

№	Підхід	Стисле визначення лояльності	Ключові джерела (APA)
1	Атитюдний (commitment)	Стійкий психологічний зв'язок із організацією (афективний, нормативний, інструментальний)	Meyer & Allen (1991, 1997); Mowday, Porter, & Steers (1982)
2	Поведінково-адміністративний	Стабільні проорганізаційні дії (дисципліна, дотримання процедур, участь у навчанні)	Organ (1988); Podsakoff et al. (2009)
3	Обмінний/довіри	Лояльність як результат взаємності, підтримки й справедливості	Blau (1964); Eisenberger et al. (2001); Colquitt (2001); Rousseau (1995)
4	Ідентифікаційно-ціннісний	Лояльність як ототожнення з цілями й цінностями організації	Mael & Ashforth (1992); Pratt (1998); Riketta (2005)
5	Калькулятивний (side-bet)	Утримання через «ставки» та високі витрати виходу	Becker (1960)
6	Залучення (engagement)	Енергетично-когнітивна включеність у роботу як «операційна лояльність»	Kahn (1990); Schaufeli & Bakker (2010); Saks (2006); Harter et al. (2002)
7	Мультифокусна/ безпекова	Лояльність до різних фокусів + благонадійність у доступах/повідомленнях	Meyer & Herscovitch (2001); NIST (2020); ISO/IEC 27002 (2022)
8	Сервіс-профіт/цінність	Лояльність працівників як ланка до якості, задоволеності клієнтів і прибутку	Heskett, Sasser, & Schlesinger (1997)
9	Етична/критична	Лояльність як доброчесність і готовність до «speak-up», а не «сліпа відданість»	Near & Miceli (1985); ISO 37002 (2021)
10	Культурно-інституційна	Лояльність як функція культури справедливості й психологічної безпеки	Schein (2010); Edmondson (1999)
11	Індексно-композитна	Агрегований індекс (атитюди + поведінка + мережі) для панелей ризику	ISO 30414 (2018); AHP/entropy-weighting (методично)
12	Українська прикладна	Лояльність як компонент HR-ризиків/ЕБП (індикатори навчання, плинність, EWI/KRI)	Balabanova & Sardak (2011); Migus (2013); Yefimenko (2024)

Джерело: систематизовано автором на основі [1-145]

Таблиця В.6

Сучасні сім підходів до оцінювання лояльності персоналу в контексті економічної безпеки

Назва підходу	Сутність	Методологія (інструменти, дані, показники)	Автори (APA)
Атитюдний (commitment-based)	Лояльність як організаційна прихильність: афективна, нормативна та інструментальна (continuance).	Опитувальники та шкали прихильності: OCQ; трикомпонентна модель TCM (ACS/NCS/CCS); підтверджувальний факторний аналіз; оцінка надійності/інваріантності; за потреби – проксі (UWES, Gallup Q12, eNPS) з валідацією.	Meyer, J. P., & Allen, N. J. (1991, 1997); Mowday, R. T., Porter, L. W., & Steers, R. M. (1982).
Поведінково-адміністративний (behavioral trace)	Лояльність як стабільні патерни дотримання правил і проорганізаційних дій (OCB), що відбиваються в операціях.	Журнали HRIS/LMS/HSE/OT/IT; процес-майнінг; контрольні карти, аномалії; перетворення цифрових слідів у EWI/KRI (відвідування тренінгів, дисципліна доступів, «near miss», реакція на відхилення).	Organ, D. W. (1988); Podsakoff, N. P., Whiting, S. W., Podsakoff, P. M., & Blume, B. D. (2009).
Обмінний/довіри (social exchange)	Лояльність як результат взаємності «організація ↔ працівник» через підтримку та справедливість; ерозія – наслідок порушення психологічного контракту.	Шкали POS (сприйнята організаційна підтримка), організаційної справедливості (Colquitt), порушення контракту; SEM/медіаційні моделі; моніторинг драйверів та наслідків (плинність, девіації).	Blau, P. (1964); Rousseau, D. M. (1995); Eisenberger, R., Armeli, S., Rexwinkel, B., Lynch, P. D., & Rhoades, L. (2001); Colquitt, J. A. (2001).
Ідентифікаційно-ціннісний	Лояльність як ототожнення з цілями/символами організації та ціннісна конгруентність; потенційний ризик «групового мислення».	OIQ (Mael–Ashforth), опитування ціннісної відповідності; мережеві/крос-рівневі моделі; перевірка зв’язку з кооперацією та стрес-резистентністю.	Mael, F. A., & Ashforth, B. E. (1992); Pratt, M. G. (1998); Riketta, M. (2005).
Калькулятивний (side-bet)	Лояльність зумовлена «ставками» працівника (специфічний людський капітал, пільги, пенсійні плани), що підвищують витрати виходу.	Оцінка switching costs; моделі виживання/ризику звільнення; аналіз специфічного людського капіталу; інтеграція з HR-аналітикою утримання.	Becker, H. S. (1960).
Залучення як «операційна лояльність» (engagement)	Енергетично-когнітивна включеність у роботу та організацію як	UWES; Gallup Q12; багаторівневі моделі зв’язку з результативністю/безпекою	Kahn, W. A. (1990); Harter, J. K., Schmidt, F. L., & Hayes, T. L. (2002); Saks, A. M.

Назва підходу	Сутність	Методологія (інструменти, дані, показники)	Автори (APA)
	практичний сурогат лояльності, пов’язаний із якістю та безпекою.	(OEE, defect rate, інциденти HSE); вимоги до валідизації показників.	(2006); Schaufeli, W. B., & Bakker, A. B. (2010).
Мультифокусна та безпекова лояльність	Лояльність має кілька фокусів (до організації, керівника, команди, професії) і безпековий вимір (благонадійність, дотримання доступів, speak-up).	Шкали commitment-to-targets; показники personnel/security compliance; EWI/KRI для JML-процесів, RBAC/SoD; програми whistleblowing та «just culture»; узгодження з NIST/ISO-контролями.	Meyer, J. P., & Herscovitch, L. (2001); NIST (2020); ISO/IEC 27002 (2022).

Примітка: EWI – випереджальні індикатори; KRI – ключові ризик-показники; HRIS/LMS/HSE/OT/IT – відповідні інформаційні системи кадрового, навчального, охорони праці, операційного та IT-контурів; JML – joiner–mover–leaver; RBAC/SoD – рольове керування доступом/сегрегація обов’язків.

Джерело: систематизовано автором на основі [1-145]

Додаток Д

Таблиця Д.1

Ключові індикатори економічної безпеки: пояснення та вимірювання

Сфера	Показник	Як вимірювати (формула/одиниці)	Тип	Напрямок	Пояснення (зв'язок з ЕБП)	Джерело даних	Періодичність
Фінанси	Коефіцієнт покриття (Current ratio)	Оборотні активи / Поточні зобов'язання	T	Вище – краще (до розумної межі)	Запас ліквідності для погашення короткострокових зобов'язань і підтримання безперервності	Баланс	Місяць/кв.
	Маржа операц. грошового потоку	CFO / Виручка, %	T	Вище – краще	Якість прибутку й здатність самофінансувати операції в стресі	Звіт про РГК	Місяць/кв.
	Борг/EBITDA	Валовий борг / EBITDA	T	Нижче – краще	Ковенантна стійкість; ризик рефінансування	Фінзвітність, договори	Кв.
	Частка простроченої ДЗ >90 днів	Простр. ДЗ>90 / Заг. ДЗ, %	L	Нижче – краще	Кредитний ризик контрагентів; загроза касових розривів	ERP/облік	Місяць
Виробництво Ланцюги постачань і ринок	OEE (заг. ефективність обладнання)	Доступність×Продуктивність×Якість, %	T	Вище – краще	Інтегральна операційна стійкість; чутливість до збоїв	MES/SCADA	Тижд./міс.
	Завантаження потужностей	Факт. випуск / Потенціал, %	L	Оптимум (70–90%)	Ризик простоїв/перевантажень, що впливає на витрати й резерви	MES/план-факт	Тижд./міс.
	Рівень браку	Неконд. продукція / Випуск, %	T	Нижче – краще	Витрати на переробку, ризик рекламацій і штрафів	QC/QA	Тижд./міс.
	MTTR критичних активів	Середній час ремонту, год	L	Нижче – краще	Швидкість відновлення; впливає на RTO виробництва	CMMS/EAM	Місяць

Сфера	Показник	Як вимірювати (формула/одиниці)	Тип	Напрямок	Пояснення (зв’язок з ЕБП)	Джерело даних	Періодичність
	Концентрація постачальників (HHI)	Σ частка_i² (за обсягом/вартістю)	L	Нижче – краще	Диверсифікація ризику зривів постачання	Закупівлі/ERP	Кв.
	TTR постачання (Time to Recover)	Дні до відновлення критичної номенклатури	L	Нижче – краще	Визначає запас міцності складу й план безперервності	SCM/контракти	Кв./півр.
	Портфель замовлень (місяці покриття)	Backlog / Середньоміс. випуск	L	Вище – краще (до межі)	Видимість попиту і стабільність грошових потоків	CRM/ERP	Місяць
	Частка експорту з високим георизиком	Виручка «ризикових» ринків / Заг. виручка, %	L	Нижче – краще	Чутливість до санкцій/логістики/валюти	Продажі/ERM	Кв.
ІКТ / інформаційна безпека	Критичні IT-інциденти	К-сть рівня «High/Critical» за період	L	Нижче – краще	Безперервність ERP/MES; ризик простою й витоку даних	SIEM/ITSM	Тижд./міс.
	Досягнутий RTO (тести BCP/DRP)	Середній час відновлення, год	L	Нижче – краще	Фактична відновлюваність критичних систем	DR-тести/звіт	Кв./півр.
	RPO (втрата даних у разі аварії)	Години/хвилини	L	Нижче – краще	Ліміт незворотної втрати транзакцій/даних	DR-план/тести	Кв./півр.
	Відмовостійкість критичних систем	% систем із активним резервуванням	L	Вище – краще	Ймовірність безперервної роботи під час збоїв	IT-арх./CMDB	Кв.
Персонал і HSE	Плинність ключових кадрів	Звільнення ключ. ролей / Серед. чисельн., %	L	Нижче – краще	Збереження критичних компетенцій; ризик деградації процесів	HRIS	Місяць/кв.
	Покриття наступництва	% критичних ролей із планом заміщення	L	Вище – краще	Операційна стійкість до кадрових шоків	HR/кадровий резерв	Кв.
	LTIFR	Травми з втратою працездатності / 1 млн люд-год	T	Нижче – краще	Безпека виробництва; ризик зупинок і штрафів	HSE/охор. праці	Місяць/кв.
	Абсентеїзм	Втрачені робочі дні / Планові, %	L	Нижче – краще	Ранній сигнал проблем у колективах/умовах праці	HRIS	Місяць
Екологія та енергія	Енергоємність продукції	кВт·год на одиницю/тонну	T	Нижче – краще	Вартість і чутливість до енергошоків	EMS/ланц. енергії	Місяць
	Викиди CO_2e	т CO_2e / т продукції	T	Нижче – краще	Регуляторний і репутаційний ризики, «вуглецеві» мита	Екооблік/MRV	Кв./півр.

Сфера	Показник	Як вимірювати (формула/одиниці)	Тип	Напрямок	Пояснення (зв’язок з ЕБП)	Джерело даних	Періодичність
	Частка «зеленої» енергії	ВДЕ у споживанні, %	L	Вище – краще	Хедж проти цінових/регуляторних шоків	Енергопостачальник	Кв.
	Екоштрафи/претензії	Сума за період, грн/валюта	T	Нижче – краще	Правові та фінансові наслідки інцидентів	Юрдеп/HSE	Кв./рік
Інновації та інтелектуальна власність	Нові продукти у виручці	Частка виручки від продуктів <3 років, %	L	Вище – краще	Довгострокова конкурентоспроможність і стійкість маржі	Продажі/BI	Кв./півр.
	R&D-інтенсивність	R&D / Виручка, %	L	Вище – краще	Потенціал технологічного оновлення та енергоефективності	Фінплан/бюджет	Кв./рік
	Активний портфель ІВ	К-сть чинних патентів/ліцензій	L	Вище – краще	Захист технологічних ніш; монетизація	Юр/ІВ-реєстри	Півр./рік
	Time-to-Market	Дні «ідея → запуск»	L	Нижче – краще	Організаційна гнучкість і здатність реагувати на шоки попиту	PMO/PLM	Кв./рік

*Скорочення: **L** – випереджальний (leading) індикатор; **T** – запізнілий (lagging). «Напрямок» вказує, який бік зміни є сприятливим для безпеки.*
Джерело: систематизовано автором

Таблиця Д.2

Анкета

Шановні експерти, просимо вас встановити вагові коефіцієнта окремо для кількісних та якісних показників оцінювання стану економічної безпеки підприємства

	Назва показника	Питома вага
Кількісний показник		
Q1	Поточна ліквідність	
Q2	Покриття відсотків	
Q3	Чистий борг/EBITDA	
Q4	Маржа операц. грош. потоку	
Q5	EBITDA-маржа	
Q6	Оборотність активів	
Q7	DSO – дні дебіторки	
Q8	CAPEX/Амортизація	
	Разом Q	
Якісний показник		
QL1	Думка аудитора	
QL2	Ковенанти та графік погашень	
QL3	Юридичні/регуляторні ризики	
QL4	Кредитний та клієнтський ризик	
QL5	Операційна безперервність (BCP/наслідки шоків)	
QL6	Фінансова прозорість/якість розкриття	
	Разом QL	

Таблиця Д.3

Перелік промислових підприємств

Компанія	Галузь	Де шукати звітність
АТ «Укрзалізниця»	Транспорт, інфраструктура	Розділ «Фінансова звітність» на сайті компанії.
ПрАТ «НЕК “Укренерго”»	Енергетика, передача	«Financial reports» на сайті Укренерго; також публікації для інвесторів/біржові повідомлення.
АТ «Укргідроенерго»	Енергетика, генерація	Інвесторський розділ: «Фінансова звітність».
ПАТ «Центренерго»	Енергетика, генерація	«Фінансова звітність» на сайті компанії (історія) та архіви рішень/звітів.
АТ «Укрнафта»	Нафта й газ	Сторінка для інвесторів/протоколи та звіти.
ПАТ «АрселорМіттал Кривий Ріг»	Металургія	«Регулярна інформація / Річні звіти» на сайті компанії; є фінзвітність та аудиторські звіти.
АТ «Запоріжсталь» (ПАТ)	Металургія	Окремий розділ для акціонерів на сайті комбінату; також агрегатори відкритих даних (XLSX).
ПрАТ «Полтавський ГЗК» (Ferrexpo Poltava Mining)	Залізорудна сировина	На сайті підприємства – окрема та консолідована звітність (доступні PDF/ZIP).
ПАТ «Сумихімпром»	Хімічна промисловість	Розділ «Звітність емітента / Річна фінзвітність» на офіційному сайті.
АТ «Дніпроазот»	Хімічна промисловість	Розділ «Інформація для акціонерів» та відкриті дані з файлами фінзвітності (XLSX).

Джерело: систематизовано автором

Додаток Д.4

Результати перевірки методики оцінювання стану економічної безпеки промислових підприємств (S)

Логіка перевірки охоплює валідність, надійність, стійкість, калібрування та придатність до управління – із чіткими тестами, метриками й порогами «склав/не склав».

1) Мета та обсяг верифікації

Мета. Довести, що індекс S коректно відбиває ризик-профіль підприємства, стабільний до технічних виборів (нормування/ваги), відтворюваний різними аналітиками та корисний для прийняття рішень.
Обсяг. Дані 2020–2024 рр., не менше 8–10 підприємств на сектор; джерела – фінзвіт, аудиторський звіт, примітки (IFRS/НП(С)БО).

2) Перевірки даних (Data QA/QC)

- ***Заповненість*** кількісних показників (θ): частка наявних Q1–Q8 ≥ **0,90** (мінімум 0,80).
- ***Узгодженість:*** баланс ↔ Звіт про фінрезультати ↔ РГК (контрольні співвідношення, наприклад, EBITDA=EBIT+амортизація).
- ***Дефляція/валюта:*** за потреби – приведення грошових рядів до постійних цін; FX-розклад боргу.
- ***Аномалії:*** політика винзорування (1–99 перцентилі) + журнал винятків.

3) Конструктна валідність (чи міряємо те, що потрібно)

3.1. Факторна структура кількісних метрик.

- ***Тест:*** PCA/фактор-аналіз для Q1–Q8.
- ***Критерії:*** 2–3 латентні фактори (ліквідність/платоспроможність; маржа/грошові потоки; ефективність/оборотність) пояснюють ≥ 60% дисперсії; навантаження відповідають економічній інтуїції (наприклад, Q2, Q3, Q4, Q5 – один кластер).

3.2. Конвергентна/дискримінантна перевірка.

- ρ_Spearman між S_{quant} і «твердими» індикаторами ризику (відсоткове покриття, DSCR, CFO-margin) ≥ 0,50; з «несумісними» – помірні або низькі.

3.3. Якісний блок.

- Очікуваний зв'язок: гірші аудиторські висновки/ковенанти → нижчі S_{qual} (ρ_Spearman ≤ –0,40 із наявністю модифікованих думок/попереджень про безперервність).

4) Критеріальна валідність (ex post наслідки)

4.1. Визначення подій «ризику»:

- велике скорочення виробництва/тривала зупинка, суттєві руйнування активів, дефолт/реструктуризація боргу, модифікована думка аудитора щодо GC, різка втрата ліквідності.

4.2. Backtesting «раннього сигналу».

- Правило: *тригер ризику* –S<0,50 або S∈[0,50;0,64] + наявність gatekeeper (Q2=0, Q3=0, QL2≤1, QL5≤1).
- Оцінка: ROC-AUC ≥ 0,75 для передбачення подій у вікні 1–3 квартали наперед; Precision-Recall (для рідкісних подій) – area ≥ 0,40.
- Калібрування порогів: якщо частка *false negatives* > 25%, переглянути пороги 0,50/0,650,50/0,65 або ваги 70/30.

5) Надійність і відтворюваність

5.1. Інтерпретаторська узгодженість якісних оцінок.

- Два незалежні аналітики виставляють QL1–QL6 за примітками/аудиторським звітом.
- Метрика: Cohen's κ по кожному QL ≥ 0,70; середній κ ≥ 0,75 – «добре», ≥ 0,80 – «дуже добре».

5.2. Повторюваність кількісних розрахунків.

- Перерахунок іншою особою/скриптом → середнє абсолютне відхилення $S_{quant} \leq 0{,}01$.

5.3. Audit trail:

- Повний паспорт джерел і формул, контрольні суми датасетів; журнал змін версій порогів/ваг.

6) Стійкість (robustness) до методичних виборів

6.1. Нормування:

- Порівняти базову дискретну шкалу з альтернативою (лінійне min–max у секторах).
- Критерій: Kendall's τ між рейтингами S ≥ 0,80.

6.2. Ваги 70/30 та всередині блоків.

- Бутстреп по підприємствах/роках → SD(S) при варіації ваг ±10 п.п. ≤ 0,03; ранги топ-3/бот-3 стабільні у ≥ 80% ітерацій.

6.3. Gatekeepers та ε-смуга.

- Аналіз граничних спостережень (|S – поріг| < 0,01): частка «перекласифікацій» при вимкненому гістерезисі ≤ 15%; з гістерезисом – ≤ **5%**.

7) Калібрування шкали та справедливість між секторами

- **Секторальні коригування** порогів окремих Q-показників (Q2, Q3, Q6) на ±10–20% тестувати в перекристалізації ROC-AUC; очікуване покращення AUC ≥ 0,03 без втрати інтерпретованості.
- ***Міжсекторна неупередженість:*** середній S не має систематично занижуватись для окремого сектору після коригувань; тест MANOVA або Jonckheere–Terpstra – відсутність упередженого зсуву (p>0,10).

8) Придатність до управління (decision usefulness)

- ***Тригери дій*** жорстко прив'язані до категорій:
  S≥0,80 - підтримка; 0,65–0,79 - точкові поліпшення; 0,50–0,64 - програма відновлення; <0,50 - антикризова програма.
- ***SLA оглядів*** q/q на операційному рівні; щомісячний комітет ризиків для «жовтих/червоних» випадків; річний перегляд секторальних порогів.
- ***Відслідковуваність наслідків:*** міра виконання планів дій (on-time %) у «жовтій/червоній» зонах ≥ **80%** – умова «склав».

9) Узагальнений чек-лист «склав/не склав»

Блок	Метрика/тест	Поріг «склав»
Дані	Заповненість θ	≥ 0,90 (мін. 0,80)
Конструкт	PCA: пояснена дисперсія	≥ 60%
Конструкт	$\rho S_{quant,core}$	≥ 0,50
Конструкт	$\rho S_{qual,red\ flags}$	≤ –0,40
Критеріальна	ROC-AUC (1–3 кв. наперед)	≥ 0,75
Надійність	Cohen's κ (QL середній)	≥ 0,75
Стійкість	Kendall's τ (нормування)	≥ 0,80
Стійкість	SD(S) при зсуві ваг ±10 п.п.	≤ 0,03
Гістерезис	«перекласифікації» біля порогів	≤ 5%
Управління	Виконання планів дій у «жовтій/червоній»	≥ 80%

10) Обмеження й застереження

- ***Фінансоцентричність:*** без внутрішніх операційних KPI методика чутливіша до бухгалтерських ефектів (імпейрменти, одноразові резерви).
- ***Якісні оцінки:*** залежать від повноти розкриття в примітках; контроль через подвійне рецензування (κ).
- ***Подійні «шоки»:*** раптові руйнування/блекаути можуть різко змінити профіль; саме тому збережено gatekeepers та гістерезис.

11) Практичний протокол запуску

1. Зібрати фіндані/примітки 2020–2024, застосувати QA/QC.
2. Розрахувати S_{quant}, S_{qual}, S, первинні категорії.
3. Накласти фільтр даних, gatekeepers, гістерезис → остаточні категорії.
4. Провести PCA/кореляції, κ для QL, чутливість нормувань/ваги.
5. Backtesting із вікном 1–3 кв.; оцінити ROC-AUC/PR-AUC, відкоригувати пороги/ваги.
6. Затвердити пороги та регламент оновлення; оформити audit trail.

Висновок перевірки. Методика – методологічно валідна й управлінсько придатна, за умови дотримання контрольних порогів:

- достатньої заповненості даних, узгодженості якісних оцінок ($\kappa \geq 0{,}75$),
- стійкості до альтернативних нормувань ($\tau \geq 0{,}80$) і прийнятної предиктивної здатності щодо кризових подій ($AUC \geq 0{,}75$).

Найбільший приріст якості дають системна перевірка «червоних прапорів», застосування гістерезису та щорічна секторальна калібровка порогів. У такій конфігурації індекс S надійно транслює публічні дані у чіткі, дієві рішення для менеджменту та наглядових рад.