

DOI: <https://doi.org/10.32782/2524-0072/D2026-86-221>

УДК 005.334

ІНТЕЛЕКТУАЛІЗАЦІЯ ПРОЦЕСІВ МОНІТОРИНГУ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ

INTELLIGENTISATION OF PROCESSES FOR MONITORING THE ECONOMIC SECURITY OF ENTERPRISES

Гайворонський Богдан Олександрович

аспірант,

Національний аерокосмічний університет «Харківський авіаційний інститут»

ORCID: <https://orcid.org/0009-0003-8856-9401>

Ревенко Даніїл Сергійович

доктор економічних наук, професор,

професор кафедри економіки та публічного управління,

Національний аерокосмічний університет «Харківський авіаційний інститут»

ORCID: <https://orcid.org/0000-0001-8125-1474>

Haivoronskyi Bohdan, Revenko Daniil

National Aerospace University «Kharkiv Aviation Institute»

У статті обґрунтовано теоретико-методичний підхід до формування архітектури системи інтелектуального моніторингу економічної безпеки підприємства. Розкрито сутність інтелектуалізації як еволюційного переходу від ретроспективної фіксації відхилень до створення проактивного когнітивного середовища. Запропоновано багаторівневу структуру архітектури, що включає модулі інтелектуальної конвергенції даних, цифрової симуляції через двійників, предиктивної діагностики та рециркуляції знань. Особливу увагу приділено принципам адаптивного синтезу та когнітивної автономності. Сформовано систему вимог до інтелектуального моніторингу та розроблено методіку оцінювання його ефективності на основі інтегрального індексу інтелектуальної резильєнтності, що враховує превентивність, адаптивну швидкість і когнітивну оптимізацію процесів.

Ключові слова: інтелектуальний моніторинг, цифрова трансформація, цифровізація, економічна безпека підприємства, архітектура системи моніторингу, цифровий двійник, адаптивний синтез, рециркуляція знань, превентивне управління ризиками, інтелектуальна резильєнтність, когнітивна автономність, машинне навчання.

The relevance of the research topic is determined by the rapid digitalisation of economic processes and the growing nonlinearity of risks, which render traditional monitoring methods ineffective and vulnerable. The aim of the article is to develop a theoretical and methodological approach to the formation of the architecture of an intelligent monitoring system for the economic security of an enterprise. The research methodology is based on a comprehensive combination of the systems approach, structural-logical modelling methods, and efficiency assessment techniques. An important component of the methodological framework is the development of an integral index of intellectual resilience, based on the synthesis of preventive, adaptive, and cognitive indicators of system performance efficiency. The obtained results consist in the formation of a unique five-level architecture of intelligent monitoring. The first level ensures intelligent data convergence through semantic gateways. The second level implements the function of an analytical core based on the enterprise's digital twin. The third level focuses on predictive diagnostics and the detection of weak danger signals. The fourth level provides decision-making support through interpretable artificial intelligence algorithms and a knowledge recirculation mechanism that ensures continuous self-learning of the system. The fifth level forms an autonomous security contour resistant to information attacks targeting internal monitoring algorithms. It has been proven that intellectualisation enables the transition from simple accounting functions to autonomous goal-setting functions, where each detected anomaly is transformed into a source of knowledge for improving the security contour. A system of specific requirements for the design of such systems has been substantiated. The practical value of the article lies in the possibility of directly implementing the developed architecture in enterprise activities in order to transform the economic security system into a strategic resource. The proposed assessment methodology based on the resilience index enables management to objectively determine the level of organisational protection and the effectiveness of investments in digital transformation. The implementation



of the developed approaches ensures the minimisation of losses and a significant reduction in the time required to adapt enterprise strategy to changes in the market environment.

Keywords: intelligent monitoring, digital transformation, digitalisation, corporate economic security, monitoring system architecture, digital twin, adaptive synthesis, knowledge recycling, preventive risk management, intelligent resilience, cognitive autonomy, machine learning.

Постановка проблеми. Динамічність економічного середовища, його безперервна трансформація та зростання нелінійності ризиків зумовлюють критичну вразливість і функціональну обмеженість традиційних систем моніторингу. Підходи орієнтовані, переважно, на фіксацію вже реалізованих відхилень втрачають здатність забезпечувати своєчасне реагування на приховані загрози, аномалії та дестабілізуючі процеси у діяльності підприємства. Унаслідок цього формується суперечність між потребою підприємств у превентивному захисті та недостатніми аналітичними й адаптивними можливостями існуючих інструментів моніторингу.

Відсутність інтегрованих механізмів самонавчання та інтелектуальної обробки даних у системах моніторингу економічної безпеки призводить до накопичення інформаційного шуму й перевантаження осіб, що приймають управлінські рішення. Це актуалізує проблему розробки архітектури інтелектуального моніторингу, здатної трансформувати різно-рідні масиви даних у випереджальні сценарії захисту та адаптивного реагування. Актуальність дослідження обумовлена необхідністю переходу від традиційних інформаційно-облікових функцій моніторингу до формування інтелектуалізованих когнітивних середовищ, спроможних автономно ідентифікувати вектори загроз, прогнозувати розвиток кризових ситуацій і підтримувати прийняття управлінських рішень у режимі реального часу.

Аналіз останніх досліджень і публікацій.

Аналіз наукового доробку свідчить про те, що фундамент сучасної теорії моніторингу організаційних систем було закладено у працях Галіцина В. К., Сулова О. П. та Самченко Н. К. [1], де автори детально структурували етапи спостереження та формування інформаційно-аналітичної бази для управлінських рішень. Проте традиційні підходи дедалі частіше стикаються з проблемою низької адаптивності. Зокрема, Кириленко О. В., Стогній Б. С. та Денисюк С. П. [2] наголошують на необхідності інтелектуального Smart-моніторингу, який би враховував складний взаємозв'язок економічного та інформаційного шарів.

Важливий внесок у розвиток когнітивних механізмів обробки даних зробили Голуб С. В. та Куницька С. Ю. [3], запропонувавши використання поліагентних функціоналів для видобутку інформації в умовах кризи, коли старі масиви даних втрачають репрезентативність. Продовжуючи цю лінію, Голуб С. В. та Остапюк В. В. [4] дослідили машинне навчання багат шарових моделей програмних агентів, що дозволяє виконувати завдання ідентифікації та прогнозування в нестабільних середовищах. Питання автоматичного оновлення таких моделей через адаптивний синтез розглянуто в роботі [5], що є критичним для систем, які функціонують у реальному часі.

Прикладні аспекти інтелектуалізації в різних галузях висвітлені у працях Кагарлицького Є. І. та Паршина М. М. [6], які інтегрували методи штучного інтелекту та комп'ютерного зору для аналізу сигналів, а також Лактінов І. С. та інші автори [7], що зосередилися на автоматизації агромоніторингу. Еколого-економічний контекст інтелектуальних систем досліджено Орехівською В., Сірик А. та Євтушенко О. [8], де акцентується увага на сталому розвитку.

Виділення невирішених раніше частин загальної проблеми. Незважаючи на значні результати, залишається невирішеною проблема формування єдиної адаптивної архітектури, яка б поєднувала цифрові двійники економічної безпеки з механізмами рециркуляції знань для забезпечення когнітивної автономності системи моніторингу економічної безпеки. Недостатньо вивченими є питання оцінювання специфічної резильєнтності таких інтелектуальних систем та їх здатності до самостійного цілепокладання без втручання оператора, що потребує розробки нових методичних підходів.

Формулювання цілей статті (постановка завдання). Метою статті є розробка теоретико-методичного підходу до формування архітектури системи інтелектуального моніторингу економічної безпеки підприємства.

Виклад основного матеріалу дослідження. Функціонування системи економічної безпеки підприємства все частіше

Таблиця 1

Специфікація вимог до системи інтелектуального моніторингу економічної безпеки підприємства

| Вимоги | Суть вимог та функціональне призначення | На що спрямована вимога в системі безпеки |
|---------------------------------|--|--|
| Адаптивний синтез | Автоматична перебудова алгоритмів оцінки при зміні даних або умов ринку | Гнучкість – здатність системи залишатись актуальною під час радикальних структурних змін |
| Інтелектуальний фільтр | Вилучення знань із шумів даних. Оцінка даних за змістовністю та репрезентативністю | Якість рішень – особа, що приймає рішення не перевантажена інформацією |
| Інтерпретованість | Вимога до прозорості алгоритмів. Система має надавати логічне обґрунтування, чому вона вважає певну подію загрозою | Довіра до рішень – особа, що приймає рішення повинна бачити логічний ланцюжок факторів, що призвели до загрози чи ризику |
| Когнітивна автономність | Система повинна самостійно ідентифікувати цілі моніторингу залежно від стратегічних пріоритетів підприємства | Цілепокладання – система сама розуміє, які показники стали критичними в конкретний момент, без команди оператора |
| Когнітивна ризик-орієнтованість | Здатність оцінювати широкий спектр загроз, ризиків і збитків (фінансові, репутаційні, екологічні, соціальні тощо). | Комплексність – безпека розглядається як багатовимірна стійкість (резильєнтність) |
| Прогностична здатність | Система повинна бути здатною прогнозувати ймовірність настання загроз | Превентивність – можливість зупинити загрозу на етапі її зародження |
| Рециркуляція знань | Постійне оновлення бази знань на основі досвіду подолання криз (збереження ефективних рішень) | Самонавчання системи – нова загроза з джерелом знань у майбутньому |
| Ситуаційність | Формування рекомендацій залежно від конкретного контексту ситуації | Ефективність – забезпечення точкових та своєчасних заходів |
| Стійкість до інформаційних атак | Вимога до захищеності самої системи і алгоритмів штучного інтелекту від маніпуляцій | Достовірність – унеможливлення ситуацій з фальшивими даними і приховання атак |
| Технологія цифрового двійника | Створення віртуальної моделі економічної безпеки підприємства, що працює в реальному часі синхронно з реальним підприємством | Точність прогнозу – дозволяє проводити стрес-тестування цифрового двійника без ризику для реальних ресурсів підприємства |

Джерело: сформовано на основі [1; 3–5; 9; 11; 12]

залежить від здатності своєчасно виявляти приховані загрози, аналізувати взаємозв'язки між факторами ризику та формувати обґрунтовані управлінські рішення. Існуючі підходи до моніторингу, спрямовані переважно на фіксацію ретроспективних відхилень, поступово втрачають свою ефективність через обмежені можливості адаптації, низький рівень прогностичності та недостатню швидкість аналітичної обробки інформації. Тому, актуальності набуває інтелектуалізація процесів моніторингу економічної безпеки підприємств, яка передбачає інтеграцію інструментів штучного

інтелекту, адаптивної аналітики, машинного навчання та цифрових механізмів підтримки прийняття рішень у єдину систему управління безпекою. Інтелектуалізація процесу моніторингу дозволяє перейти до проактивного управління ризиками, орієнтованого на прогнозування кризових явищ та раннє виявлення негативних факторів.

Під інтелектуалізацією процесів моніторингу економічної безпеки будемо розуміти спеціально організоване систематичне та автоматичне спостереження за станом економічної безпеки підприємства, яке поєднує

комплексну оцінку поточного стану об'єкта з його ретроспективним аналізом та прогнозуванням майбутньої поведінки [2]. Це еволюційний перехід від традиційного контролю, до створення інтелектуального середовища, яке формуватиме знання і контекст, виявити закономірності та передбачити розвиток подій.

При розгляді інтелектуалізації процесів моніторингу економічної безпеки і системи інтелектуального моніторингу треба зазначити, що це не тотожні поняття. Інтелектуалізацію процесів доцільно розглядати як еволюційний процес трансформації традиційної системи моніторингу у більш складну адаптивну систему, здатну до самонавчання, прогнозування та підтримки управлінських рішень. Інтелектуальний моніторинг представляє собою результат такої трансформації, тобто є новою сформованою системою, функціонування якої базується на використанні інтелектуальних технологій та аналітичних алгоритмів.

Можна виділити певну послідовність розвитку систем моніторингу економічної безпеки:

1. Етап традиційного моніторингу (фіксація показників та контроль відхилень).

2. Етап автоматизованого моніторингу (цифровізація процедур збору та обробки даних).

3. Етап інтелектуалізованого моніторингу (інтеграція аналітичних і адаптивних інструментів).

4. Етап інтелектуального моніторингу (автономна система прогнозування, аналізу та підтримки рішень).

Стадійність демонструє поступовий перехід від інформаційно-облікової функції моніторингу до формування когнітивної системи економічної безпеки, у межах якої дані перетворюються на основу для превентивного управління ризиками та стратегічної адаптації підприємства. В інтелектуальному моніторингу моделі штучного інтелекту та програмні агенти стають центральним ядром, яке перетворює різномірні масиви даних на осмислену аналітичну картину, готову для ухвалення рішень [6]. Замість звичайного запису та порівняння, такий моніторинг наділяється функціями цілепокладання, глибокого аналізування і навчання, контролінгу.

До основних характеристик інтелектуалізації процесів моніторингу можна віднести наступні [1–8]:

1. В сучасних умовах інтелектуальна система не може обмежуватися констатацією

поточних відхилень. Її ключовою характеристикою є здатність здійснювати *діагностування з ідентифікацією та прогнозуванням*. Використовуючи алгоритми машинного навчання, система моніторингу може аналізувати історичні та поточні дані, щоб розпізнавати ранні прояви загроз, аномалії чи кризові тенденції ще до моменту їх критичного прояву чи настання.

2. Інтелектуальні системи моніторингу не мають бути жорсткими математичними конструкціями, а повинні представляти живе алгоритмічне середовище, що реагує на динаміку об'єкта. Тому вони повинні бути здатними до *самоналаштування* – оптимізувати власні внутрішні параметри для мінімізації помилок та підвищення ефективності. Це може досягатися завдяки методам адаптивного синтезу, програмні агенти моніторингу можуть автоматично коригувати або повністю перебудовувати свої аналітичні моделі безпосередньо під час роботи, пристосовуючись до нових умов середовища чи зміни властивостей об'єкта.

3. Інтелектуальний моніторинг передбачає інтеграцію даних, що мають різну природу та походять із різних вимірів. Тому, *мульти-модальний підхід та синергія даних* дозволяє компенсувати слабкості одного каналу інформації можливостями іншого, створюючи багатовимірну і достовірну логіку поведінки об'єкта.

4. В інтелектуальному моніторингу цінність даних повинна вимірюватися не лише їх точністю, а й додатковими показниками: *репрезентативністю, змістовністю, достатністю та стійкістю*. Процедура розпізнавання ситуацій повинна відбуватись з оцінкою інформації на трьох рівнях: формально-структурному, змістовному та споживчому, що відповідає меті керування. Фактично, система моніторингу повинна здійснювати *інтелектуальний аналіз*, фокусуючись на вилученні корисних знань із загальної маси несуттєвих даних.

5. Інтелектуальний моніторинг виступає як специфічний інструмент «зворотного зв'язку» та невід'ємна складова технології управління. Він повинен забезпечувати *перехід від необроблених результатів до осмисленого рішення*, а саме формувати аналітичні довідки, перевіряти внутрішню логіку подій, оцінювати сценарії та генерувати рекомендації. Це забезпечує оперативне реагування на аномалії, дозволяє запобігати ризикам та підтримувати стабільний розвиток.

При проектуванні системи інтелектуального моніторингу економічної безпеки підприємства необхідно враховувати сукупність базових принципів, які визначають логіку її функціонування, аналітичні можливості та здатність до цілепокладання та контролю. До таких принципів доцільно віднести принципи [1–3; 7; 8]: адаптивного синтезу, безперервності, інформаційної взаємодії, інтегральної організації моніторингу, рециркуляції, превентивності, комплексності, самооновлення, інтегрованості, ситуаційності, прогностичності, когнітивності та ризик-орієнтованості. Дотримання цих принципів забезпечить формування гнучкої інтелектуальної системи моніторингу економічної безпеки підприємства, здатної до своєчасного виявлення загроз, прогнозування кризових явищ, аналізу складних взаємозв'язків та оперативного реагування на зміни внутрішнього і зовнішнього середовища підприємства.

Треба зауважити, що ефективність функціонування системи інтелектуального моніторингу економічної безпеки, а також інтелектуалізація його процесів значною мірою залежить від правильного сформованої архітектури самої системи. Тому необхідно визначити ключові вимоги до такої системи, які повинні враховуватися ще на етапі її проектування. Формування вимог покликано забезпечити функціональну цілісність системи, стійкість до інформаційних та економічних викликів, а також узгодженість між аналітичними, технологічними та управлінськими компонентами. При цьому вимоги повинні орієнтуватися на технічні характеристики, її здатність до самонавчання, оперативного реагування на аномалії, інтеграції різнорідних потоків інформації та підтримки стратегічного управління економічною безпекою підприємства. В таблиці 1 представлені ключові вимоги до системи інтелектуального моніторингу економічної безпеки підприємства.

Як можна бачити з таблиці 1, система інтелектуального моніторингу повинна забезпечити виконання наступних прикладних задач: раннє виявлення аномалій і загроз; автоматично генерувати сценарій захисту; здійснювати безперервний аудит та семантичний аналіз зовнішнього середовища.

Визначення ключових вимог до інтелектуальної системи моніторингу економічної безпеки підприємства створює основу для формування її архітектури. Сукупність вимог визначає логіку побудови системи, структуру взаємодії її компонентів, механізми обробки

даних та принципи підтримки управлінських рішень. У зв'язку з цим проектування архітектури інтелектуального моніторингу слід розглядати як процес трансформації визначених вимог у цілісну багаторівневу систему. Архітектурна модель має забезпечувати узгодженість та функціональність як єдине інтелектуальне середовище управління економічною безпекою підприємства: аналітичні алгоритми, цифрові агенти, механізми машинного навчання та інструменти підтримки прийняття рішень.

Треба зазначити, що архітектура системи інтелектуального моніторингу економічної безпеки повинна розглядатися як динамічне когнітивне середовище, що функціонує за принципом безперервного інтелектуального циклу. Її структура базується на багаторівневому підході, де кожен рівень реалізує конкретні принципи та вимоги, забезпечуючи перехід від простого збору даних до автономного цілепокладання. Розглянемо кожен рівень системи, що пропонується.

Модуль 1. Рівень інтелектуальної конвергенції даних (забезпечує принципи інформаційної взаємодії та інтегрованості). Цей рівень відповідає за безперервний видобуток інформації з різнорідних джерел. Тут реалізується вимога до «інтелектуального фільтра», який очищує вхідний потік від «інформаційного шуму». Завдяки принципу інтегральної організації, дані не просто накопичуються, а проходять крізь семантичні шлюзи, де оцінюється їх змістовність та репрезентативність для цілей безпеки.

Модуль 2. Аналітичне ядро та цифрова симуляція. Центральним елементом архітектури системи інтелектуального моніторингу є цифровий двійник економічної безпеки. Це віртуальна копія бізнес-процесів, яка працює синхронно з реальним підприємством. Адаптивний синтез дозволяє аналітичному ядру автоматично змінювати вагові коефіцієнти моделі оцінювання рівня економічної безпеки та ризиків при зміні ринкової кон'юнктури. На цьому рівні моделюються сценарії та проводиться стрес-тестування без загрози для реальних ресурсів, що відповідає принципу ситуаційності.

Модуль 3. Рівень предиктивної діагностики та когнітивного аналізу. В основі цього модуля лежить принцип ризик-орієнтованості. Система не чекає на настання критичної події, а використовує свою прогностичну здатність для виявлення слабких сигналів загроз. Вимога до когнітивної ризик-орієнто-

ваності дозволяє системі одночасно аналізувати фінансові, репутаційні, екологічні та інші вектори, формуючи цілісну картину стійкості (резильєнтності) підприємства.

Модуль 4. Рівень інтелектуальної підтримки рішень та рециркуляції знань (забезпечує вимоги превентивності та самонавчання системи). Це рівень взаємодії «система – особа, що приймає рішення». Архітектура передбачає обов'язкову інтерпретованість, тобто система не просто видає сигнал про небезпеку, а будує логічний ланцюжок факторів. Завдяки принципу рециркуляції, кожне прийняте рішення та його результат повертаються в

систему, оновлюючи базу знань. Вимога до когнітивної автономності дозволяє системі самостійно коригувати вектори моніторингу, якщо вона ідентифікує нові стратегічні пріоритети підприємства, забезпечуючи повну превентивність управління.

Модуль 5. Захисний контур (забезпечує стійкість до інформаційних атак та самооновлення). Оскільки система є критично важливою для виживання бізнесу, її архітектура містить вбудований контур безпеки. Він реалізує вимогу стійкості до інформаційних атак, захищаючи алгоритми машинного навчання від маніпуляцій. Принцип самооновлення гаран-

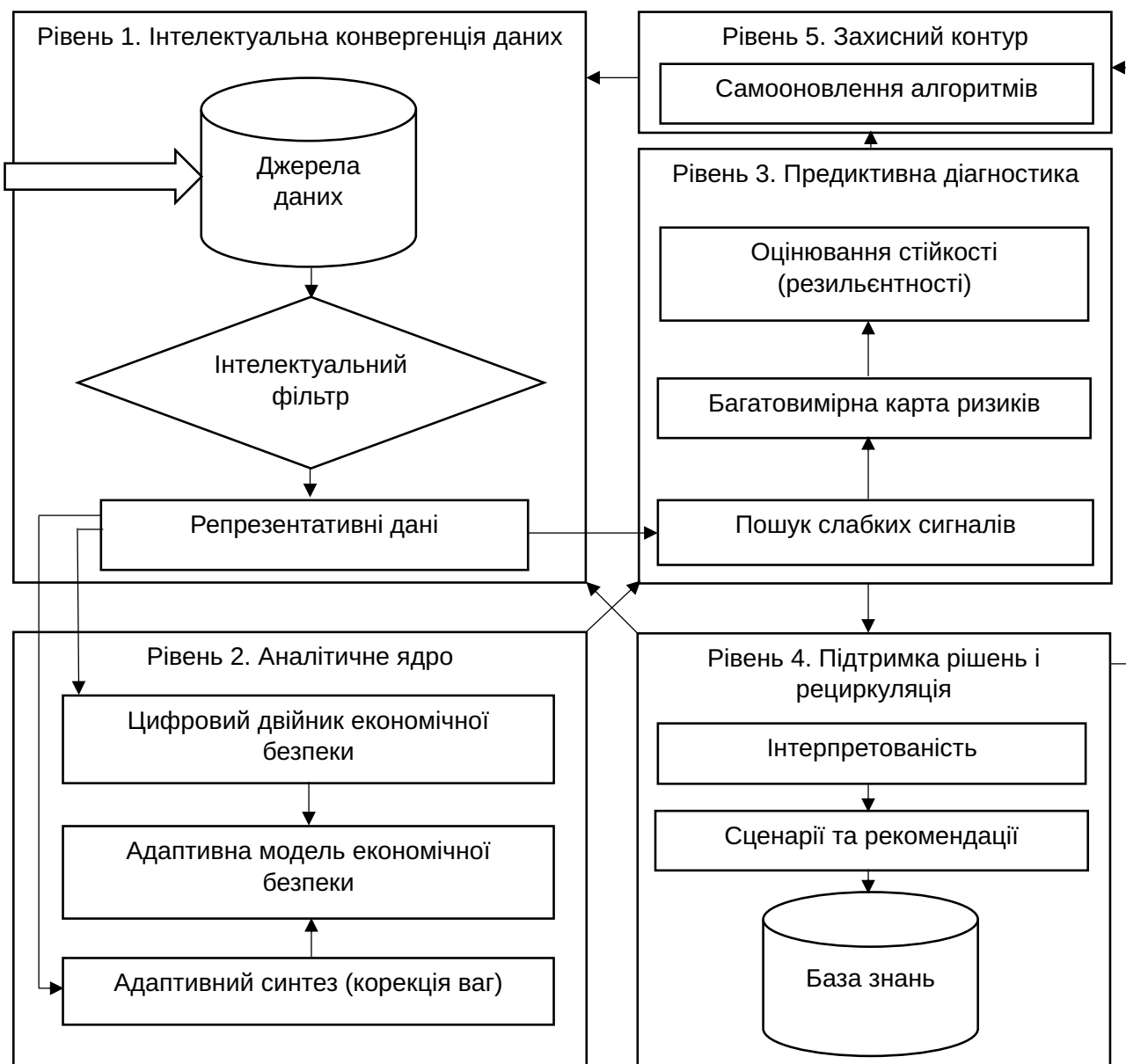


Рис. 1. Архітектура та структурна побудова системи інтелектуального моніторингу економічної безпеки підприємства

Джерело: сформовано авторами

тує, що захисні механізми системи еволюціонують швидше за методи кібератак.

Сформована за такими принципами архітектура перетворює моніторинг із сервісної функції на стратегічний актив. Узгодженість між технологічним та управлінським рівнями забезпечує функціональну цілісність всієї системи економічної безпеки. Така структура дозволяє підприємству реагувати на зміни та здійснювати стратегічну адаптацію, перетворюючи кожну виявлену загрозу на джерело інтелектуального розвитку організації. На рисунку 1 подану схему сформованої архітектури та структурної побудови системи інтелектуального моніторингу економічної безпеки підприємства.

Процес розробки та впровадження системи інтелектуального моніторингу економічної безпеки підприємства являє собою складну науково-технологічну задачу, що виходить за межі класичного програмування та вимагає глибокої інтеграції когнітивних методів аналізу. На початковому етапі розробки увага повинна приділятися створенню алгоритмічного фундаменту, здатного до адаптивного синтезу, що дозволяє системі самостійно конструювати логіку оцінки залежно від мінливості зовнішнього середовища. Розвиток системи моніторингу передбачає поступове нарощування її аналітичних потужностей через навчання на великих масивах даних, в цьому процесі акцент повинен бути зроблений на налаштуванні інтелектуальних фільтрів. Ці фільтри є критично важливими для відсікання інформаційного шуму та виокремлення змістовних індикаторів, що забезпечує високу якість подальших управлінських рішень і запобігає перевантаженню аналітиків нерелевантною інформацією.

Процес функціонування системи у реальному часі базується на постійній взаємодії між цифровим двійником економічної безпеки та реальними бізнес-процесами підприємства. Це формує умови для безперервного стрес-тестування та симуляції різних сценаріїв розвитку подій без ризику для реальних ресурсів. По мірі розвитку система набуває здатності до когнітивної автономності, коли вона повинна почати самостійно ідентифікувати нові вектори загроз. Така прогностична здатність трансформує моніторинг із механізму фіксації на інструмент стратегічного випередження. Результатами когнітивного аналізу є конкретні цифри і семантичний розгляд контексту ситуації, що підвищує точність діагностики у складних умовах.

Робота з інтелектуальною системою моніторингу вимагає від осіб, що приймають рішення нового рівня довіри до технологій штучного інтелекту. Система повинна формувати кінцевий висновок і розгортати для фахівця зрозумілий логічний ланцюг факторів і причинно-наслідкових зв'язків, що призвели до конкретного сигналу тривоги. Найважливішим етапом життєвого циклу системи моніторингу є рециркуляція знань – постійне самонавчання алгоритмів на конкретних випадках і ситуаціях. Це забезпечує еволюційний розвиток архітектури, через досвід подолання криз та інтеграцію і оновлення моделі прогнозування.

Впровадження інтелектуальної системи моніторингу економічної безпеки підприємства потребує постійного оцінювання результативності її функціонування, оскільки технологічно складна система не гарантує автоматичного підвищення якості управління безпекою. Ефективність інтелектуального моніторингу повинна визначатися швидкістю обробки інформації, обсягом аналітичних даних, здатністю системи своєчасно виявляти загрози, мінімізувати ймовірність помилкових рішень та забезпечувати адаптацію до змін середовища.

Для оцінювання ефективності роботи, системи інтелектуального моніторингу економічної безпеки підприємства, пропонується розраховувати інтегральний індекс інтелектуальної резильєнтності системи, який визначає спроможність системи моніторингу трансформувати вхідні дані у стратегічну стійкість підприємства. Модель цього індексу можна представити як функцію трьох показників:

$$IR = v_1 IP + v_2 SP + v_3 CO, \quad (1)$$

де v_n – вагові коефіцієнти при кожному показнику;

IP – показник превентивного запобігання;

SP – показник адаптивної швидкості;

CO – показник когнітивної оптимізації.

Показник превентивного запобігання оцінює економічну ефективність прогностичної здатності системи (наскільки ефективно працює «проактивний» режим моніторингу порівняно з ретроспективним):

$$IP = \frac{L_p}{L_T}, \quad (2)$$

де L_p – вартість збитків, яким вдалося запобігти завдяки ранньому виявленню загроз;

L_T – загальна оціночна вартість виявлених ризиків за звітний період.

Показник адаптивної швидкості реакції системи вимірює технологічну гнучкість системи на нову аномалію (загрозу):

$$SP = 1 - \frac{T_d + T_a}{T_c}, \quad (3)$$

де T_d – час на детекцію, розраховується як різниця між часовою міткою виникнення аномалії та моментом її класифікації як загрози;

T_a – час на адаптацію, є інтервалом від моменту ідентифікації загрози до повного завершення перебудови аналітичної моделі;

T_c – критичний час, максимально допустимий час, протягом якого загроза може вплинути на підприємство.

Показник когнітивної оптимізації визначає ефективність заміщення інтелектуальної праці алгоритмами (відсоток ресурсів, вивільнених завдяки роботі системи):

$$CO = \frac{C_t - C_i}{C_t}, \quad (4)$$

де C_t – витрати на традиційний моніторинг;

C_i – операційні витрати на підтримку системи інтелектуального моніторингу.

Запропонований методичний підхід до формування системи інтелектуального моніторингу економічної безпеки підприємства дозволяє переосмислити роль інформаційно-аналітичних процесів у забезпеченні корпоративної стійкості. Перехід від пасивної фіксації збитків до активного моделювання майбутнього стану підприємства за допомогою цифрових двійників та алгоритмів самонавчання створює фундамент для нової парадигми безпеки. Впровадження інтелектуального моніторингу, підкріплене об'єктивним вимірюванням когнітивної, адаптивної та превентивної ефективності, трансформує сис-

тему економічної безпеки з витратної статті бюджету на високотехнологічний стратегічний ресурс.

Висновки. Розвиток концепції інтелектуалізації моніторингу економічної безпеки підтверджує, що в сучасних умовах цифрової трансформації є ключовим чинником забезпечення стратегічної стійкості підприємства. Проведений аналіз свідчить про перехід до багаторівневої архітектури, що поєднує цифрові двійники, механізми адаптивного синтезу та рециркуляцію знань, дозволяє подолати обмеження традиційних ретроспективних підходів. Запропонована модель інтелектуальної системи не лише автоматизує збір даних, а й формує когнітивне середовище, здатне до автономного цілепокладання та самонавчання. Це забезпечує превентивне реагування на аномалії та трансформацію ризиків у джерело досвіду. Оцінювання ефективності впровадження такої системи через інтегральний індекс інтелектуальної резильєнтності дозволяє об'єктивно виміряти когнітивний, адаптивний та економічний внесок технологій у безпековий контур підприємства.

Подальші перспективи досліджень у цьому напрямку пов'язані розробкою методів протидії складним інформаційним атакам на самі алгоритми моніторингу, що потребує посилення «захисного контуру» архітектури. Окрім того, перспективним є розширення мультимодального підходу через інтеграцію неструктурованих великих даних, що дозволить поглибити прогностичну здатність цифрових двійників.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Галіцин В. К., Суслов О. П., Самченко Н. К. Концептуальні засади моніторингу. *Бізнес Інформ*. 2013. № 9. С. 330–335.
2. Кириленко О. В., Стогній Б. С., Денисюк С. П., Сопель М. Ф. Smart-моніторинг електроенергетичних систем. *Технічна електродинаміка*. 2024. № 5. С. 48–62. DOI: <https://doi.org/10.15407/techned2024.05.048>.
3. Голуб С. В., Куницька С. Ю. Поліагентні функціонали в інформаційних технологіях інтелектуального моніторингу. *Математические машины и системы*. 2020. № 4. С. 11–19.
4. Голуб С. В., Остапюк В. В. Машинне навчання багатозарових моделей моніторингового програмного агента. *Математичні машини і системи*. 2025. № 2. С. 76–95. DOI: <https://doi.org/10.34121/1028-9763-2025-2-76-95>.
5. Остапюк В. В., Голуб С. В. Концептуальні підходи до адаптивного синтезу моделей для задач інтелектуального моніторингу. *Інформаційні технології та комп'ютерне моделювання: матеріали Міжнародної науково-практичної конференції*. м. Івано-Франківськ, 20–23 травня 2025 р. С. 142–143.
6. Кагарлицький Є., Паршин М. Інтелектуальні системи моніторингу та аналізу сигналів і зображень на основі методів штучного інтелекту. *Дослідження та інновації*. 2025. № 1 (5 (8)). С. 89–94.
7. Лактіонов І. С., Гнатушенко В. В., Каштан В. Ю., Дяченко Г. Г. Інтелектуальні інформаційні та комп'ютерні технології збору та аналізу даних агромоніторингу : монографія. Дніпро : НТУ «ДП», 2025. 235 с.

8. Орешківська В., Сірик А. Теоретичні аспекти формування складових інтелектуальної інформаційно-аналітичної системи з еколого-економічного моніторингу на підприємствах харчової промисловості в контексті сталого розвитку. Вибрані матеріали IV Міжнародної конференції з європейських аспектів сталого розвитку (20–21 жовтня 2022 р., м. Київ). Київ : НУХТ, 2022. 187 с.

9. Калінеску Т. В., Ревенко Д. С., Нор В. В. Концепт формування аналітичного інструментарію діагностики економічної безпеки підприємства. *Часопис економічних реформ*. 2024. № 4 (56). С. 17–23. DOI: <https://doi.org/10.32620/cher.2024.4.02>

10. Калінеску Т. В., Ревенко Д. С., Мостіпан І. Л. Концептуальні положення створення моніторингу систем економічної безпеки підприємництва. *Часопис економічних реформ*. 2021. № 4(44), С. 12–18. DOI: <https://doi.org/10.32620/cher.2021.4.02>

11. Калінеску Т. В., Ревенко Д. С., Підмогильний С. С. Парадигма формування механізму зміцнення економічної безпеки підприємницької діяльності. *Часопис економічних реформ*. 2021. № 3(43), С. 35–41. DOI: <https://doi.org/10.32620/cher.2021.3.04>

12. Ревенко Д. С. Методологія моделювання діагностики та управління стійкістю соціально-економічних систем : монографія. Харків : Нац. аерокосм. ун-т ім. М. Є. Жуковського «Харків. авіац. ін-т», 2019. 320 с.

REFERENCES:

1. Halitsyn V. K., Suslov O. P., Samchenko N. K. (2013) Kontseptualni zasady monitorynhu [Conceptual framework for monitoring]. *Biznes Inform*, vol. 9, pp. 330–335.

2. Kyrylenko O. V., Stohnii B. S., Denysiuk S. P., Sopel M. F. (2024) Smart-monitorynh elektroenerhetychnykh system [Smart monitoring of power systems]. *Tekhnichna elektrodynamika*, vol. 5, pp. 48–62. DOI: <https://doi.org/10.15407/techned2024.05.048>.

3. Holub C. V., Kynytska S. Yu. (2020) Poliahentni funktsionaly v informatsiynykh tekhnolohiiakh intelektualnoho monitorynhu [Multi-agent functionalities in information technologies of intelligent monitoring]. *Matematychni mashyny i systemy*, vol. 4, pp. 11–19.

4. Holub S. V., Ostapiuk V. V. (2025) Mashynne navchannia bahatosharovykh modelei monitorynhovoho prohramnoho ahenta [Machine learning of multilayer monitoring software agent models]. *Matematychni mashyny i systemy*, vol. 2, pp. 76–95. DOI: <https://doi.org/10.34121/1028-9763-2025-2-76-95>.

5. Ostapiuk V. V., Holub S. V. (2025) Kontseptualni pidkhody do adaptivnoho syntezu modelei dlia zadach intelektualnoho monitorynhu [Conceptual approaches to adaptive model synthesis for intelligent monitoring tasks]. *Informatsiini tekhnolohii ta kompiuterne modeliuvannia: materialy Mizhnarodnoi naukovo-praktychnoi konferentsii. m. Ivano-Frankivsk, 20–23 travnia 2025*, pp. 142–143.

6. Kaharlytskyi Ye., Parshyn M. (2025) Intelektualni systemy monitorynhu ta analizu syhnaliv i zobrazhen na osnovi metodiv shtuchnoho intelektu [Intelligent systems for monitoring and analyzing signals and images based on artificial intelligence methods]. *Doslidzhennia ta innovatsii*, vol. 1 (5 (8)), pp. 89–94.

7. Laktionov I. S., Hnatushenko V. V., Kashtan V. Yu., Diachenko H. H. (2025) *Intelektualni informatsiini ta kompiuterne tekhnolohii zboru ta analizu danykh ahromonitorynhu : monohrafiia* [Intelligent information and computer technologies for collecting and analyzing agricultural monitoring data: monograph]. Dnipro: NTU «DP», 235 p. (in Ukrainian)

8. Oreshkivska V., Siryk A. (2022) Teoretychni aspekty formuvannia skladovykh intelektualnoi informatsiino-analitychnoi systemy z ekoloho-ekonomichnoho monitorynhu na pidpriemstvakh kharchovoi promyslovosti v konteksti staloho rozvytku [Theoretical aspects of the formation of components of an intelligent information and analytical system for environmental and economic monitoring at food industry enterprises in the context of sustainable development]. *Vybrani materialy IV Mizhnarodnoi konferentsii z yevropeiskykh aspektiv staloho rozvytku (20–21 zhovtnia 2022 r., m. Kyiv)*. Kyiv: NUKhT, 187 p.

9. Kalinesku T. V., Revenko D. S., Nor V. V. (2024) Kontsept formuvannia analitychnoho instrumentariiu diahnostyky ekonomichnoi bezpeky pidpriemstva [The concept of forming analytical tools for diagnosing the economic security of an enterprise]. *Chasopys ekonomichnykh reform*, vol. 4 (56), pp. 17–23. DOI: <https://doi.org/10.32620/cher.2024.4.02>.

10. Kalinesku T. V., Revenko D. S., Mostipan I. L. (2021) Kontseptualni polozhennia stvorennia monitorynhu system ekonomichnoi bezpeky pidpriemnytstva [Conceptual provisions for the creation of monitoring systems for the economic security of entrepreneurship]. *Chasopys ekonomichnykh reform*, vol. 4(44), pp. 12–18. DOI: <https://doi.org/10.32620/cher.2021.4.02>.

11. Kalinesku T. V., Revenko D. S., Pidmohylnyi S. S. (2021) Paradyhma formuvannia mekhanizmu zmitsnennia ekonomichnoi bezpeky pidpriemnytskoi diialnosti [Paradigm for forming a mechanism for strengthening the

economic security of entrepreneurial activity]. *Chasopys ekonomichnykh reform*, vol. 3(43), pp. 35–41. DOI: <https://doi.org/10.32620/cher.2021.3.04>.

12. Revenko D. S. (2019) *Metodolohiia modeliuвання diahnostrykyta upravlinnia stiiikistiu sotsialno-ekonomichnykh system : monohrafiia* [Methodology for modeling diagnostics and managing the stability of socio-economic systems: monograph]. Kharkiv : Nats. aerokosm. un-t im. M. Ye. Zhukovskoho «Kharkiv. aviats. in-t», 320 p. (in Ukrainian)

Дата надходження статті: 16.04.2026

Дата прийняття статті: 15.05.2026

Дата публікації статті: 27.05.2026