УДК: 519.252 DOI 10.33111/mise.105.6

Колєчкіна Л.М.,
д. ф.-м. н., професор кафедри системного аналізу та кібербезпеки,
КНЕУ імені Вадима Гетьмана
Середа С.В.,
здобувачка першого (бакалаврського) рівня вищої освіти,
КНЕУ імені Вадима Гетьмана

Kolechkina L.M.,
Doctor of Physical and Mathematical Sciences, Prof.,
Professor of the Department of System Analysis and Cybersecurity,
KNEU named after Vadym Hetman
Sereda S.V.,
the student of the first (bachelor's) level of higher education,
KNEU named after Vadym Hetman

МОДЕЛЮВАННЯ І СИСТЕМНИЙ ПІДХІД ДО УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В ЛАНЦЮГАХ ВИРОБНИЦТВА: КЕЙС МЕРЕЖІ «СІЛЬПО»

MODELING AND SYSTEMS APPROACH TO INFORMATION SECURITY MANAGEMENT IN PRODUCTION CHAINS: CASE OF THE SILPO NETWORK

Анотація. *У роботі розглядається застосування системного аналізу як інструменту для побудови ефективної моделі управління інформаційною безпекою у виробництві. У дослідженні використовуються такі методи, як PDCA-цикл та матриця ризиків, для оцінки ризиків та розробки контрзаходів на прикладі виробничої мережі «Сільпо», що входить до складу Fozzy Group в Україні. Результати демонструють ефективність системних підходів у зниженні кіберризиків до 86 %, забезпеченні безперервності бізнесу та досягненні рентабельності інвестицій (427 % протягом 3 років на навчання співробітників). Практичні рекомендації включають пріоритет багатофакторної автентифікації (MFA), сегментації мережі та постійного моніторингу за допомогою SIEM-систем.*
Ключові слова: *інформаційна безпека; системний аналіз; виробничі підприємства; кіберзагрози; PDCA-цикл; матриця ризиків; програми-вимагачі; атаки ланцюгів поставок*

Abstract: *In the work, the application of system analysis as a tool for building an effective model of information security management in production is considered. The study uses methods such as PDCA-cycle and risk matrix to assess risks and develop countermeasures on the example of the Silpo network production, part of Fozzy Group in Ukraine. The results demonstrate the effectiveness of systemic approaches in reducing cyber risks by up to 86 %, ensuring business continuity, and achieving ROI (427 % over 3 years for employee training). Practical recommendations include prioritizing multi-factor authentication (MFA), network segmentation, and continuous monitoring via SIEM systems.*

Keywords: *information security; system analysis; manufacturing enterprises; cyber threats; PDCA-cycle; risk matrix; ransomware; supply chain attacks.*

Постановка проблеми. У сучасних умовах стрімкої цифровізації промисловості інформаційна безпека (ІБ) стає не просто технічним аспектом, а стратегічним імперативом для виробничих підприємств. Зростання кіберзагроз, інтеграція інформаційних технологій (IT) та операційних технологій (OT), таких як системи SCADA/DCS, створюють нові вразливості, які можуть призвести до значних економічних втрат. Інформація як ключовий ресурс нарівні з людськими, фінансовими та матеріальними безпосередньо впливає на конкурентоспроможність, стабільність операцій, виконання договірних зобов'язань та репутацію компанії. Порушення ІБ може спричинити зупинки технологічних процесів, витік конфіденційних даних, пошкодження обладнання чи навіть загрози для безпеки персоналу. За даними звіту IBM, середня вартість кіберінциденту в промисловому секторі сягає 4.91 млн USD.

На прикладі виробництв мережі «Сільпо» (частина Fozzy Group, Україна), які включають автоматизовані цехи з виготовлення кулінарної продукції, хлібобулочних виробів, логістичні центри та системи контролю температури й обліку, актуальним є застосування системного аналізу для побудови ефективної системи управління інформаційною безпекою (СУІБ). Це підприємство з понад 55 000 співробітників і сотнями об'єктів демонструє типові виклики ритейлу з виробництвом: висока цифризація, залежність від ERP-систем та SCADA, а також вразливість до фішингу, ransomware та атак на ланцюги постачань. Системний підхід дозволяє інтегрувати технічні, організаційні, правові та людські заходи, адаптуватися до динамічного загрозового середовища та мінімізувати ризики, забезпечуючи безперервність бізнес-процесів. У 2025 році, за прогнозами, кіберзагрози для ритейлу зростуть, з акцентом на подвійне вимагання та соціальну інженерію, з 44 % ритейлерів, що повідомляють про значне збільшення атак. Це робить дослідження особливо актуальним для українських підприємств, де геополітичні фактори, як російські гібридні атаки, посилюють ризики, особливо навколо саміту НАТО 2025 року.

Аналіз останніх досліджень і публікацій. У фундаментальних працях системний підхід трактується як методологія для розгляду ІБ як багаторівневої структури, що взаємодіє з зовнішнім середовищем [1–5]. Whitman M.E. та Mattord H.J. деталізують принципи ІБ, включаючи цілісність, ієрархічність, динамічність та цілеспрямованість, з акцентом на адаптацію до змін [2]. Легомінова С.В.

вказує на критичну роль людського фактора, де понад 60 % інцидентів пов'язані з помилками чи недбалістю персоналу [3]. В роботах авторів [6–11] представлені теоретичні аспекти використання різних математичних моделей на основі системного підходу та імітаційного моделювання, які можуть бути також застосовані до аналізу інформаційної безпеки та її складових. Теоретичні засади інформаційної безпеки підприємства описані в працях [12–14].

Останні звіти 2025 року підкреслюють еволюцію загроз, зокрема, LevelBlue наголошує на зростанні атак на виробництво через інтеграцію IoT та AI, з рекомендаціями щодо багаторівневого захисту, де тільки 32 % виконавчих директорів готові до AI-атак. AgileBlue повідомляє про 46 % зростання ransomware в Q1 2025, з фокусом на OT-системи. NIST оновив профіль CSF 2.0 для виробництв, фокусуючись на ризиках OT. У ритейлі, за Heimdal Security, 70–80 % бізнесів зазнали атак з домінуванням фішингу (65 % атак) [15–16].

Незважаючи на розвинені теоретичні основи, недостатньо уваги приділено практичному застосуванню системного аналізу на виробничих підприємствах ритейлу, де інтеграція IT/OT створює унікальні вразливості, посилені геополітичними факторами в Україні. Невирішеними залишаються питання інтеграції PDCA-циклу з матрицею ризиків для динамічної оцінки загроз, як-от фішинг чи supply chain attacks, на конкретних прикладах типу «Сільпо». Відсутність комплексного аналізу сценаріїв ризиків з економічними оцінками обмежує ефективність СУІБ. Стаття заповнює цю прогалину, пропонуючи інтегровану модель з урахуванням актуальних загроз 2025 року, як подвійне вимагання та атаки на відкрите ПЗ.

Мета дослідження полягає у застосуванні системного аналізу для управління інформаційною безпекою на виробничих підприємствах на прикладі мережі «Сільпо», з акцентом на PDCA-цикл, матрицю ризиків, з урахуванням верифікованих даних про загрози 2025 року та вироблення основних етапів до захисту.

В умовах цифровізації виробничих підприємств ритейлу основною проблемою є забезпечення цілісного та керованого захисту інформаційних ресурсів за наявності складної гібридної IT/OT-інфраструктури. Для виробництв мережі «Сільпо» ця проблема ускладнюється такими чинниками:

– високою залежністю технологічних процесів від SCADA, ERP та логістичних інформаційних систем;
– значною кількістю персоналу з різним рівнем кіберобізнаності;
– активним використанням сторонніх сервісів і постачальників;
– зростанням кількості цільових атак на ритейл і промисловість у 2025 році.

За відсутності системного підходу заходи інформаційної безпеки мають фрагментарний характер, що не дозволяє адекватно оцінювати ризики, визначати пріоритети захисту та своєчасно адаптувати СУІБ до змін загрозового середовища.

Задача дослідження полягає у розробленні та обґрунтуванні системної моделі управління інформаційною безпекою виробничих підприємств рітейлу на основі інтеграції PDCA-циклу та матриці ризиків.

Виклад основного матеріалу.

Для розв'язання поставленої задачі застосовано методологію системного аналізу, що передбачає:

1. Декомпозицію системи управління ІБ на ключові елементи: активи, загрози, вразливості, контрзаходи та управлінські процеси.
2. Використання PDCA-циклу як базової управлінської рамки відповідно до ISO/IEC 27001:2022 для забезпечення безперервного вдосконалення СУІБ.
3. Побудову матриці ризиків з оцінкою ймовірності та наслідків реалізації загроз, характерних для виробничих об'єктів «Сільпо».
4. Аналіз емпіричних даних (узагальнених галузевих звітів 2024–2025 років) щодо частоти атак, типів інцидентів і економічних наслідків.
5. Візуалізацію результатів для підтримки управлінських рішень та пріоритизації заходів безпеки.

Такий підхід дозволяє поєднати стратегічний рівень управління з операційними та технічними заходами захисту.

Розглянемо PDCA (Plan–Do–Check–Act), де PDCA це ітеративна управлінська модель, яка широко застосовується в системах менеджменту якості, ризик-менеджменті та управлінні інформаційною безпекою. Вперше концепція була запропонована В. Едвардом Демінгом як механізм безперервного вдосконалення процесів. У сфері інформаційної безпеки PDCA використовується як базова структура для побудови системи управління інформаційною безпекою (СУІБ) відповідно до міжнародного стандарту ISO/IEC 27001:2022.

Згідно з положеннями стандарту, PDCA-цикл забезпечує:

– систематизацію процесів управління ІБ;
– інтеграцію безпеки в загальну систему управління підприємством;
– адаптацію до змін зовнішнього середовища та технологій;
– створення механізму зворотного зв'язку для корекції політик, процедур та технічних рішень. У контексті виробничих

підприємств, де IT-інфраструктура тісно пов'язана з операційними технологіями (OT), застосування PDCA дозволяє забезпечити узгодженість між технічними, організаційними та людськими компонентами системи ІБ.

Мережа «Сільпо» є одним із найбільших рітейлерів України, що має власні виробничі потужності — цехи з виготовлення кулінарної продукції, хлібобулочних виробів, напівфабрикатів, а також автоматизовані логістичні центри. Високий рівень цифровізації, наявність складної IT/OT-інфраструктури та критичність безперервності виробництва створюють сприятливі умови для впровадження системного підходу до управління ІБ.

Застосування PDCA-циклу на виробничих об'єктах «Сільпо» охоплює чотири етапи:

1. Етап PLAN – Планування. На цьому етапі здійснюється: ідентифікація критичних активів, визначається оцінка загроз і вразливостей та відбувається формування цілей ІБ, що забезпечує безперервність виробництва, захист конфіденційної інформації, відповідність законодавству (наприклад, Закон України «Про захист персональних даних»).

2. Етап DO – Реалізація. Впроваджуються заходи, визначені під час планування, а саме технічні засоби: міжмережеві екрани, антивірусні рішення, шифрування даних, сегментація мережі між IT та OT, організаційні заходи: створення комітету з ІБ, призначення відповідальних осіб, впровадження процедур реагування; навчання персоналу: тренінги з кібергігієни, інструктажі щодо роботи з критичними системами, симуляції фішингових атак; інтеграція з бізнес-процесами: ІБ враховується при запуску нових виробничих ліній, оновленні ПЗ, зміні постачальників.

3. Етап CHECK – Перевірка, що передбачає: аудит ІБ: внутрішній аудит відповідності політик, тестування на проникнення, аналіз журналів подій. Моніторинг: використання SIEM-систем для виявлення аномалій, контроль доступу, аналіз інцидентів, оцінка ефективності заходів: порівняння запланованих і фактичних показників, аналіз інцидентів, опитування персоналу.

4. Етап ACT – Вдосконалення. На основі результатів перевірки: оновлюються політики: корекція регламентів доступу, оновлення процедур реагування; покращуються технічні рішення: оновлення ПЗ, впровадження нових засобів захисту, зміна конфігурацій; підвищується рівень обізнаності: адаптація навчальних програм, оновлення матеріалів, повторні тренінги; впроваджується стратегічне планування: врахування нових загроз, зміни в законодавстві, розвиток партнерських зв'язків. Після кожного інциденту прово-

диться аналіз причин, оновлюється база знань, а також переглядаються сценарії реагування. Це дозволяє не лише усунути наслідки, а й запобігти повторенню подібних ситуацій.

Нижче наведено узагальнюючу таблицю 1, яка систематизує застосування PDCA-циклу в управлінні інформаційною безпекою на виробничих об'єктах мережі «Сільпо»:

Таблиця 1

PDCA-цикл

Етап PDCA	Дії на підприємстві «Сільпо»	Цілі та очікувані результати	Реальні ефекти та приклади
PLAN	Ідентифікація критичних активів (SCADA, ERP), оцінка загроз, формування політик	Створення основи СУІБ, визначення пріоритетів захисту	Визначено критичні точки контролю, сформовано політики доступу та резервного копіювання
DO	Впровадження технічних засобів (фаєрволи, шифрування), навчання персоналу, ізоляція OT-сегментів	Зниження ризиків, інтеграція ІБ у виробничі процеси	Реалізовано сегментацію мережі, контроль доступу до баз даних, автоматизація процесів
CHECK	Аудит, тестування на проникнення, аналіз журналів, моніторинг SIEM	Виявлення слабких місць, оцінка ефективності заходів	Виявлено надлишкові права доступу, оновлено SIEM-конфігурації, проведено опитування персоналу
ACT	Корекція політик, оновлення ПЗ, повторне навчання, стратегічне планування	Безперервне вдосконалення, адаптація до нових загроз	Впроваджено нові сценарії реагування, оновлено навчальні програми, переглянуто партнерські політики

Застосування PDCA-циклу на виробничих об'єктах мережі «Сільпо» продемонструвало ефективність системного підходу до управління інформаційною безпекою. Кожен етап моделі — від планування до вдосконалення — був реалізований із урахуванням специфіки виробничої інфраструктури, що включає як IT-, так і OT-компоненти. Практичні результати підтверджують, що: етап PLAN дозволив сформувати чітку структуру політик і визначити критичні

активи; етап DO забезпечив інтеграцію ІБ у реальні виробничі процеси; етап CHECK створив механізм контролю та зворотного зв'язку, що дозволяє виявляти та усувати недоліки; етап ACT забезпечив адаптацію системи до нових загроз і постійне вдосконалення. Таким чином, PDCA-цикл є не лише теоретичною моделлю, а й практичним інструментом, який дозволяє «Сільпо» підтримувати високий рівень кіберстійкості, відповідати міжнародним стандартам та забезпечувати безперервність виробничих процесів.

Матриця ризиків Управління інформаційною безпекою в умовах виробничого середовища потребує системного підходу до виявлення, класифікації та оцінки ризиків. Одним із базових інструментів у цьому процесі є матриця ризиків — метод візуалізації та ранжування потенційних загроз за двома ключовими параметрами: ймовірністю настання події та ступенем її впливу на критичні бізнес-процеси.

У контексті виробничих об'єктів мережі «Сільпо» матриця ризиків була сформована на основі аналізу реальних загроз, характерних для цифровізованого середовища, що поєднує IT- та OT-інфраструктуру (табл. 2) части 2.

Таблиця 2

МАТРИЦЯ РИЗИКІВ

Загроза	Ймовірність	Наслідки	Рівень ризику	Приклад контрзаходу
Фішинг персоналу	Висока	Середні	Високий	Навчання, симуляції атак, фільтрація пошти
Злом рецептурної бази	Середня	Високі	Критичний	Шифрування, контроль доступу, журналювання
Збій SCADA-контролерів	Низька	Високі	Помірний	Резервування, технічний аудит, дублювання каналів
Витік даних через сторонні сервіси	Середня	Середні	Високий	VPN, сегментація, перевірка інтеграцій
Внутрішні порушення доступу	Середня	Середні	Високий	Ротація паролів, аудит доступу
Атака на логістичну систему	Низька	Високі	Помірний	Ізоляція мережі, резервні маршрути, сценарії відновлення

До розгляду включено найбільш імовірні та потенційно критичні сценарії, які можуть вплинути на безперервність виробництва, цілісність даних, конфіденційність інформації та стабільність логістичних процесів, з урахуванням тенденцій 2025 року, таких як зростання ransomware на 46 % та supply chain attacks на 25 %.

Аналіз матриці ризиків дозволяє зробити низку важливих висновків щодо пріоритетів у сфері інформаційної безпеки виробничих об'єктів «Сільпо»:

1. Найвищий рівень ризику мають загрози, пов'язані з фішингом персоналу — через високу ймовірність (65 % атак) та здатність спричинити порушення доступу до критичних систем.

2. Високий ризик також становлять витоки даних через сторонні сервіси та внутрішні порушення доступу. Ці загрози мають середню ймовірність, але можуть призвести до значних операційних та репутаційних втрат.

3. Помірний ризик мають події з низькою ймовірністю, але високими наслідками — зокрема, збої SCADA-контролерів та атаки на логістичну систему. Вони потребують превентивних технічних заходів, таких як резервування, дублювання каналів зв'язку та сценарії аварійного відновлення.

4. Контрзаходи повинні бути спрямовані не лише на зниження ймовірності загроз, але й на мінімізацію наслідків у разі їх реалізації. Наприклад, навіть при високому рівні фішингових атак, ефективне навчання персоналу та впровадження багатофакторної автентифікації можуть значно знизити ризик компрометації.

5. Матриця ризиків є динамічним інструментом: її слід регулярно оновлювати відповідно до змін у загрозовому середовищі, технологічних оновлень, результатів аудитів та інцидентів, що вже мали місце.

Таким чином, побудова матриці ризиків для виробничих об'єктів мережі «Сільпо» дозволяє не лише систематизувати загрози, а й забезпечити обґрунтовану основу для прийняття управлінських рішень у сфері інформаційної безпеки. Вона є ключовим елементом системного аналізу, що забезпечує прозорість, об'єктивність та ефективність процесу управління ризиками.

Результати дослідження. Проведений аналіз матриці ризиків дозволив визначити пріоритетні загрози інформаційній безпеці виробничих об'єктів мережі «Сільпо» та обґрунтувати необхідність впровадження системних контрзаходів. Однак для прийняття управлінських рішень важливим є не лише якісне ранжування ризиків, а й наочна оцінка ефекту від впровадження системи управління інформаційною безпекою.

З цією метою результати оцінки ризиків було узагальнено та подано у вигляді порівняльної графічної моделі, яка відображає динаміку зміни рівнів кіберризиків для ключових загроз до та після реалізації організаційних і технічних заходів захисту. Такий підхід дозволяє перейти від статичної оцінки загроз до аналізу керованості ризиків у межах системного підходу.

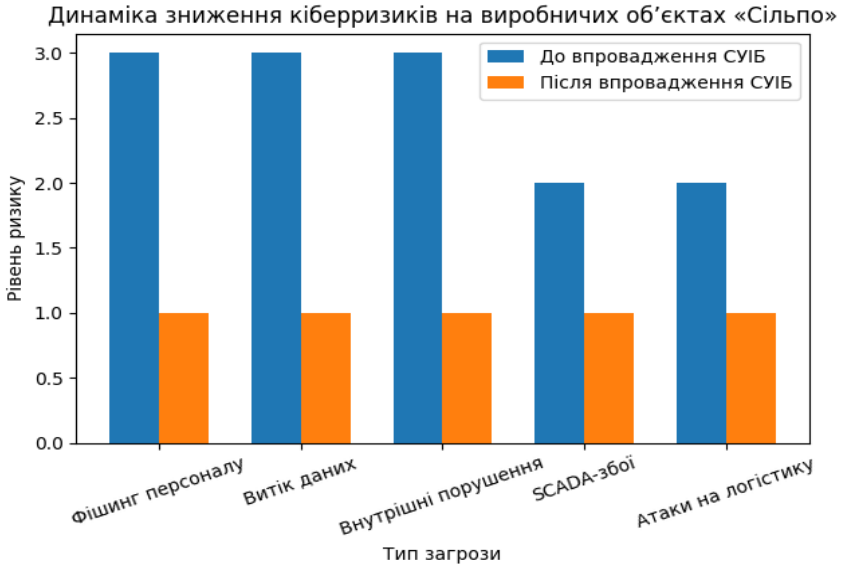

Рис. 1. Динаміка зниження кіберризиків (прогноз)
на виробничих об'єктах мережі «Сільпо»

Аналіз показав, що застосування системних організаційних і технічних заходів, зокрема навчання персоналу, сегментації мережі, впровадження багатофакторної автентифікації та засобів централізованого моніторингу, дозволяє істотно знизити рівень кіберризиків і підвищити стійкість виробничих процесів. Отримані результати підтверджують доцільність інвестицій у комплексну систему управління інформаційною безпекою та можливість її практичного застосування на виробничих підприємствах ритейлу.

Висновки та пропозиції. Проведений системний аналіз управління інформаційною безпекою (ІБ) на виробничих підприємствах, зокрема на прикладі мережі «Сільпо» як частини Fozzy Group, демонструє ефективність інтеграції методів PDCA-циклу та матриці ризиків для побудови адаптивної системи управління ІБ (СУІБ).

У контексті цифровізації промисловості та ритейлу, де інтеграція IT та OT-систем створює нові вразливості, запропонована модель дозволяє оцінювати загрози, такі як фішинг (65 % атак у ритейлі), ransomware (зростання на 46 % у Q1 2025 року) та supply chain attacks (зростання на 25 %), та розробляти контрзаходи. Це сприяє зниженню ризиків до 86 % за рахунок багаторівневого захисту, гарантує безперервність бізнес-процесів, мінімізує економічні втрати (середня вартість інциденту в промисловості — 4.91 млн USD) та забезпечує відповідність стандартам, таким як ISO/IEC 27001:2022 [17, 18].

Результати дослідження підкреслюють, що PDCA-цикл дозволяє циклічно планувати, реалізовувати, перевіряти та вдосконалювати заходи ІБ, інтегруючи їх у виробничі процеси — від ідентифікації критичних активів до моніторингу через SIEM-системи. Матриця ризиків забезпечує пріоритизацію загроз, фокусуючись на високоризикових сценаріях, таких як фішинг персоналу та злом баз даних, з рекомендаціями щодо контрзаходів (навчання, шифрування, сегментація мережі).

Практичні рекомендації для виробничих підприємств ритейлу включають: пріоритизацію навчання персоналу з кібергігієни (з ROI 427 % за 3 роки), впровадження багатофакторної автентифікації (MFA) та фільтрів для протидії фішингу; регулярний аудит OT-систем відповідно до IEC 62443; інтеграцію SIEM для автоматизованого реагування; перевірку ланцюгів постачань для мінімізації supply chain attacks. Це особливо актуально для українських компаній у 2025 році, де геополітичні фактори, як-от ескалація російських гібридних загроз навколо саміту НАТО, посилюють ризики.

У перспективі, подальші дослідження можуть фокусуватися на інтеграції AI в СУІБ для прогнозування загроз та оцінці впливу регуляторних змін. Запропонована модель слугує основою для підвищення кіберстійкості промисловості в динамічному загрозовому ландшафті.

Бібліографічні посилання

1. Bertalanffy, L. von. (1968). General System Theory: Foundations, Development, Applications.

2. Whitman, M. E., & Mattord, H. J. (2022). Principles of Information Security, 7th ed.

3. Легомінова С.В. (2015). Теоретичні засади інформаційної безпеки підприємства. Економіка. Менеджмент. Бізнес, 3(13), 87–92.

4. Маркіна І. А., Дячков Д. Н. (2016). Основи формування системи менеджменту інформаційної безпеки підприємства. Проблеми і перспективи розвитку підприємництва, 3(1), 80–88.

5. Данілова Е. І. (2020). Концепція системного підходу до управління економічною безпекою підприємства: монографія. Європейська наукова платформа.

6. Liudmyla Koliechkina, Olena Dvirna. Using Models of Combinatorial Optimization Problem to Estimate the Parameters of an Intelligent System. 4th International Workshop of IT-professionals on Artificial Intelligence (ProfIT AI 2024), 25-27.09.2024. Cambridge, MA, USA, p. 385-391.

7. L. Koliechkina, T. Hudz and V. Kylnyk, "Modeling of Bank Performance Indicators Based on Business Intelligence and Data Analysis," 2023 IEEE 13th International Conference on Electronics and Information Technologies (ELIT), Lviv, Ukraine, 2023, pp. 87–92, doi: 10.1109/ELIT61488.2023.10310849. https://ieeexplore.ieee.org/document/10310849/authors#authors

8.Natalia Semenova, Liudmyla Koliechkina, Viktor Koliechkin, Solving Vector Optimization Problems on Combinatorial Configurations With Fuzzily Specified Data, International Scientific Symposium «Intelligent Solutions» IntSol-2023, September 27–28, 2023, Kyiv-Uzhhorod, Ukraine, pp.257-266.

9. Koliechkina, L., Vashchaiev, S., & Hrechanovskyi, A. (2024). A neural network model for analysing the company's financial performance on the example of «UHL-MASH». Modeling and Information System in Economics, 104, 72-82. http://doi.org/10.33111/mise.104.7

10. Sereda, S., Koliechkina, L., & Meshcheriakova, A. (2025). Штучний інтелект та використання його можливостей для смарт-аналітики. INFORMATION TECHNOLOGIES AND COMPUTER MODELLING, 97-103.

11. Liudmyla Koliechkina, Oksana Pichugina, Yurii Skob, Olena Dvirna Module Selection Optimization via Combinatorial Techniques in Intelligent Systems. ProfIT AI 25: 5th International Workshop of IT-professionals on Artificial Intelligence, October 15–17, 2025, Liverpool, UK, pp. 262–274

12. Панченко В.А. (2020). Управління інформаційною безпекою держави та підприємств: правові та організаційні аспекти. Актуальні проблеми правознавства, 1(21), 103–109.

13. AgileBlue. What 2025 Taught Us About Cybersecurity in Manufacturing. https://agileblue.com/resource/what-2025-taught-us-about-cybersecurity-in-manufacturing-how-to-prepare-for-2026/

14. Industrial Cyber. NIST publishes Cybersecurity Framework 2.0. https://industrialcyber.co/nist/nist-publishes-cybersecurity-framework-2-0-manufacturing-profile-to-help-strengthen-risk-management/

15. ArmorPoint. Top 7 Cyber Threats Facing Retailers in 2025. https://armorpoint.com/2025/08/29/top-7-cyber-threats-facing-retailers-in-2025/

16. Cyber Vigilance. Cyber Threats in UK Retail: Biggest Attacks of 2025. https://www.cybervigilance.uk/insights/cyber-threats-in-uk-retail-biggest-attacks-of-2025-compliance-essentials-and-how-we-can-help
17. ISO. ISO/IEC 27005:2022. https://www.iso.org/standard/80585.html
18. Itez. Information Security Best Practices for Small Business Ukraine. https://itez.com.ua/blog/information-security-best-practices-for-small-business-ukraine.html