

РОЗДІЛ 9

АНАЛІЗ ПОДІЙ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ ТА РОЗРОБЛЕННЯ СЦЕНАРІЇВ МОНІТОРИНГУ БЕЗПЕКОВОГО СТАНУ

Терещенко Тетяна Павлівна, старший науковий співробітник, Військового інституту телекомунікацій та інформатизації імені Героїв Крут, Київ

Терещенко Катерина Володимирівна, студентка, Державного університету “Київський авіаційний інститут”, Київ

Черниш Юлія Олександрівна, старший науковий співробітник, Військового інституту телекомунікацій та інформатизації імені Героїв Крут, Київ

Вступ. Стрімкий розвиток інформаційних технологій, поширення розподілених систем і хмарних сервісів супроводжується зростанням кількості кіберзагроз. Сучасні атаки характеризуються прихованістю, багаторівневістю та здатністю обходити базові механізми захисту. За таких умов особливого значення набуває моніторинг подій безпеки, що забезпечує своєчасне виявлення інцидентів та реагування на них.

У цьому контексті журнали подій виступають не лише технічним засобом фіксації активності, а й важливим джерелом аналітичної інформації, що дає змогу відновити логіку дій користувачів, виявити відхилення від нормальної поведінки та своєчасно ідентифікувати ознаки потенційної компрометації системи [1].

Основна частина. Практична значущість запропонованого підходу полягає у можливості використання розроблених правил моніторингу як основи для налаштування SIEM-систем, систем виявлення вторгнень та

внутрішніх механізмів контролю безпеки в корпоративних інформаційно-комунікаційних системах.

Події безпеки формуються різними компонентами інформаційної системи та відображають дії користувачів, процесів, мережевих пристроїв і засобів захисту. Їх аналіз дозволяє виявляти аномальну активність, порушення політик безпеки та ознаки атак. Ефективність моніторингу значною мірою залежить від коректного формування правил аналізу, порогових значень та механізмів кореляції подій.

Подія безпеки визначається як будь-яка зафіксована зміна стану інформаційної системи, що має значення для забезпечення її захищеності. Події формуються операційними системами, мережевими пристроями, серверами, засобами захисту інформації та іншими компонентами системи.

Необхідно розмежовувати поняття події та інциденту. Подія є окремим фактом функціонування системи, тоді як інцидент являє собою сукупність взаємопов'язаних подій, що призводять або можуть призвести до порушення інформаційної безпеки [1; 8].

Порівняльна характеристика понять події та інциденту наведена в таблиці 1.

Таблиця 1.

Порівняльна характеристика понять “подія безпеки” та “інцидент безпеки”

Термін	Визначення	Приклад	Значення для моніторингу
Подія (event)	Будь-яка зафіксована дія або зміна стану інформаційної системи, що реєструється у журналі подій	Введення пароля, запуск процесу, доступ до файлу	Є базовою одиницею аналізу; сама по собі не завжди є небезпечною
Інцидент (incident)	Подія або сукупність взаємопов'язаних подій, що призводять або можуть призвести до порушення інформаційної безпеки	Серія невдалих входів + успішний вхід → злам акаунта	Виявляється через аналіз і кореляцію подій; є об'єктом реагування

Таким чином, подія безпеки набуває практичного значення лише в контексті її зв'язку з іншими діями в системі. Одиначний запис у журналі може бути наслідком звичайної роботи користувача, однак у поєднанні з іншими подіями він здатний вказувати на розвиток інциденту або спробу прихованого впливу на інформаційну систему.

Основними джерелами подій безпеки є операційні системи, міжмережеві екрани, сервери, бази даних, антивірусні засоби та мережеві пристрої.

Різноманітність джерел подій зумовлює необхідність їх систематизації, оскільки кожен компонент інформаційно-комунікаційної системи відображає окремий аспект її функціонування та безпекового стану.

Основні джерела подій безпеки наведено в таблиці 2.

Таблиця 2.

Основні джерела подій безпеки в інформаційних системах та їх характеристика

Джерело	Типові події	Приклади подій	Значення для безпеки
Операційна система (Windows)	Вхід/вихід, зміна прав, запуск процесів	Event ID 4624, 4625, 4672	Основне джерело інформації про дії користувачів
Linux (syslog, auditd)	Аутентифікація, зміни конфігурацій	SSH login, sudo, зміна /etc/passwd	Дає змогу відстежувати адміністративні дії
Мережеві пристрої (Router, Switch)	Підключення, зміни маршрутів, ACL	VPN login, зміна правил доступу	Виявлення мережевих атак і несанкціонованих підключень
Міжмережеві екрани (Firewall)	Дозволені/заборонені з'єднання	Blocked IP, port scan	Перша лінія захисту від зовнішніх атак
Веб-сервери (Apache, Nginx)	HTTP-запити, помилки доступу	401, 403, SQL injection	Виявлення атак на веб-додатки
Бази даних	Запити, доступ до таблиць	SELECT, DROP, failed login	Контроль доступу до критичних даних
Антивірусні системи	Виявлення шкідливого ПЗ	Trojan detected, scan result	Виявлення зараження системи
DLP-системи	Передача даних, копіювання	Copy to USB, email with sensitive data	Захист від витіку інформації

Отже, використання різних джерел дозволяє не лише виявляти окремі загрози, але й встановлювати взаємозв'язки між ними, що є критично важливим для ідентифікації складних атак [5; 8].

Для аналізу подій безпеки використовуються пороговий, сигнатурний, кореляційний та аномалійний підходи.

Основні підходи до аналізу подій безпеки наведено в таблиці 3.

Таблиця 3.

Основні підходи до аналізу подій безпеки, їх переваги та недоліки

Підхід	Опис	Приклад застосування	Переваги	Недоліки	Доцільність використання
Пороговий (threshold-based)	Виявлення аномалій на основі перевищення заданого порогу	>5 невдалих входів за хвилину	Простота реалізації, швидкість	Хибні спрацювання (false positives)	Базовий моніторинг
Сигнатурний (signature-based)	Пошук відомих шаблонів атак	SQL injection pattern	Висока точність	Не виявляє нові атаки	IDS/IPS системи
Кореляційний (correlation-based)	Аналіз зв'язків між подіями	4625 → 4624	Виявляє складні атаки	Складність налаштування	SIEM
Аномалійний (anomaly-based)	Виявлення відхилень від нормальної поведінки	Логін в незвичний час	Виявляє нові атаки	Багато хибних спрацювань	Поведінковий аналіз
ML (Machine Learning) [8]	Використання моделей для класифікації подій	Виявлення нетипових патернів	Адаптивність	Потребує даних	Просунуті SIEM

У практичних умовах жоден із підходів не є універсальним. Порогові правила забезпечують швидке виявлення очевидних відхилень, сигнатурні методи ефективні проти відомих атак, а кореляційний аналіз дозволяє простежити логіку розвитку інциденту. Саме поєднання цих підходів формує

основу сучасного моніторингу безпекового стану інформаційно-комунікаційних систем [1; 3; 8].

У подальшому аналізі акцент зроблено на пороговому та кореляційному підходах як найбільш придатних для побудови базового сценарію моніторингу.

Для дослідження розглядається умовна корпоративна інформаційно-комунікаційна система з розподіленою архітектурою, що включає центральний сегмент (Central), філію (Branch) та сегмент віддаленого доступу (Home Office).

Система містить сервери, робочі станції, мережеве обладнання та засоби віддаленого доступу. Взаємодія між сегментами здійснюється через VPN-з'єднання.

Кожен сегмент інформаційної системи містить компоненти, які генерують події безпеки різного типу. Для систематизації таких компонентів та подій доцільно представити їх у табличному вигляді.

Таблиця 4.

Основні компоненти інформаційно-комунікаційної системи та події безпеки, що ними генеруються

Сегмент	Компонент	Функціональне призначення	Типи подій	Приклади
Central	Сервери	Обробка даних, адміністрування	Вхід/вихід, зміна прав	4624, 4625, 4672
	Комутатори, маршрутизатори	Передача трафіку	Зміни конфігурації	ACL changes
Branch	Робочі станції	Дії користувачів	Логін, запуск програм	logon, process start
	Сервер філії	Зберігання даних	Доступ до ресурсів	file access
	Wi-Fi / Access Point	Підключення пристроїв	Аутентифікація	new device
Home Office	ПК, ноутбуки	Віддалений доступ	VPN, логін	remote login
Internet	Зовнішнє середовище	Мережевий вплив	Сканування, атаки	port scan

Найбільш критичними є події, пов'язані зі зміною прав доступу, використанням привілеїв адміністратора, вимкненням засобів захисту та віддаленим доступом.

Для аналізу використано журнал Windows Security Event Log [2]. Повний перелік подій безпеки наведено в таблиці 5.

Таблиця 5.

Перелік подій безпеки на основі Windows Security Event Log

Код	Назва (укр.)	Категорія	Детальний опис
4624	Успішний вхід	Logon/Logoff	Користувач успішно пройшов автентифікацію
4625	Невдалий вхід	Logon/Logoff	Спроба входу з невірними обліковими даними
4672	Спеціальні права	Privilege Use	Надання прав адміністратора
4720	Створення облікового запису	Account Management	Створено новий обліковий запис
4723	Зміна пароля	Account Management	Користувач змінив власний пароль
4724	Скидання пароля	Account Management	Адміністратор скинув пароль іншому користувачеві
4725	Видалення облікового запису	Account Management	Обліковий запис видалено
4740	Блокування облікового запису	Account Lockout	Обліковий запис заблоковано
4656	Доступ до об'єкта	Object Access	Спроба доступу до файлу або папки
4663	Доступ до файлу	Object Access	Доступ до файлу виконано
4670	Зміна прав доступу	Object Access	Змінено дозволи на об'єкті
4698	Створення завдання	Scheduled Task	Створено нове завдання в планувальнику
5007	Вимкнення антивірусу	Antivirus	Захист у реальному часі вимкнено
5032	Виявлення шкідливого ПЗ	Antivirus	Антивірус виявив загрозу
5447	Зміна політики аудиту	Policy Change	Змінено налаштування аудиту

Особливу роль у процесі моніторингу відіграють події автентифікації, управління обліковими записами, зміни прав доступу та роботи засобів захисту. Саме ці категорії найчастіше відображають дії, пов'язані з початковим доступом, закріпленням у системі, ескалацією привілеїв або приховуванням слідів атаки [5]. Події класифіковано за рівнем небезпеки в таблиці 6.

Таблиця 6.

Класифікація подій за рівнем небезпеки.

Рівень	Характеристика
Звичайні	Типова активність користувачів
Підозрілі	Нетипові або аномальні дії
Критичні	Події, що можуть свідчити про компрометацію системи

Особливу небезпеку становлять серії невдалих входів, зміна прав доступу, вимкнення антивірусного захисту та підозрілі адміністративні дії.

Сценарій моніторингу базується на пороговому та кореляційному підходах до аналізу подій.

Побудова сценарію моніторингу передбачає перехід від пасивного накопичення журналів до активного виявлення закономірностей у поведінці системи. Для цього окремі події розглядаються не ізольовано, а як частини ширшого процесу, що може свідчити про формування інциденту безпеки. Розроблені правила моніторингу наведено в таблиці 7.

Розроблений сценарій моніторингу поєднує пороговий та кореляційний підходи до аналізу подій безпеки. Порогові правила дозволяють оперативно виявляти аномальні ситуації, такі як масові спроби входу або різке зростання активності, тоді як кореляційні правила

забезпечують виявлення складніших інцидентів, що формуються в результаті послідовності подій [1; 5; 8].

Таблиця 7.

Правила сценарію моніторингу подій безпеки

№	Назва правила	Джерело (сегмент)	Умова спрацювання	Інтервал	Пріоритет	Дія
1	Brute force (один користувач)	Domain Controller (Central)	Кількість подій 4625 > 5	1 хвилина	Високий	Alert, блокування IP/акаунта
2	Незвичний час входу	Domain Controller (Central/Branch)	Подія 4624 між 01:00-05:00	Моментально	Середній	Alert, перевірка
3	Вхід після серії невдалих	Domain Controller (Central)	4624 після ≥ 3 подій 4625	Ковзне вікно 5 хв	Високий	Alert, аналіз активності
4	Створення облікового запису	Domain Controller (Central)	Подія 4720	Моментально	Середній	Alert, аудит
5	Скидання пароля	Domain Controller (Central)	Подія 4724	Моментально	Критичний	Alert, розслідування
6	Зміна прав доступу	File Server (Central)	Подія 4670	Моментально	Критичний	Alert, перевірка
7	Вимкнення антивірусу	Client (Home/Branch)	Подія 5007	Моментально	Критичний	Alert, ізоляція хоста
8	Виявлення шкідливого ПЗ	Client (Home/Branch)	Подія 5032	Моментально	Високий	Alert, запуск сканування
9	Раптове зростання активності	Усі сегменти	Зростання кількості подій >300%	10 хв	Середній	Alert, аналіз
10	Підозрілий доступ до файлів	File Server (Branch)	Масовий доступ (4663)	5 хв	Високий	Alert, перевірка
11	Підключення з нового пристрою	Home Office	Новий IP / пристрій	Моментально	Середній	Alert
12	Створення підозрілого завдання	Server (Central)	Подія 4698	Моментально	Середній	Перевірка, видалення

Особливу роль відіграє врахування джерела подій та сегмента системи. Зокрема, події, що виникають у сегменті віддаленого доступу (Home Office), мають підвищений рівень ризику, тоді як події в центральному сегменті (Central) можуть свідчити про компрометацію критичних ресурсів.

Таким чином, запропонований сценарій моніторингу дозволяє ефективно виявляти як прості, так і складні інциденти безпеки, і може бути використаний як основа для впровадження в реальних системах класу SIEM [3; 8; 9].

Для моделювання процесу аналізу подій використано мову програмування Python та бібліотеки pandas, numpy і matplotlib [6].

У процесі моделювання сформовано набір нормальних і аномальних подій, що імітують:

- атаку brute force;
- успішний вхід після серії невдалих спроб;
- вимкнення антивірусного захисту;
- скидання пароля адміністратора.

Для виявлення аномалій застосовано пороговий аналіз.

Лістинг 1. Виявлення аномалій за пороговими значеннями

```
thresholds = {
    4625: 5, # невдалий вхід: >5 за годину
    4724: 1, # скидання пароля
    5007: 1, # вимкнення антивірусу
    4670: 3, # зміна прав
    4720: 3 # створення акаунта
}

for code, threshold in thresholds.items():
    count = freq_by_code.get(code, 0)
    if count > threshold:
        print(f"      ▲ {events_info[code][0]} (код {code}) - {count}
разів
(поріг: {threshold})")
```

Кореляційний аналіз дозволив виявити сценарії, за яких успішна автентифікація відбувається після серії невдалих спроб входу.

Для оцінювання динаміки подій використано часову агрегацію та візуалізацію активності за 5-хвилинними інтервалами.

Отримані результати засвідчили доцільність використання порогових і кореляційних правил як базового інструменту виявлення аномальної активності в інформаційно-комунікаційних системах.

Водночас пороговий підхід має певні обмеження, зокрема ризик хибних спрацювань та залежність від коректно визначених порогових значень. Тому в реальних умовах його доцільно поєднувати з кореляційним аналізом, поведінковими моделями та засобами машинного навчання [1; 8].

Отже, аналіз подій безпеки є не лише технічною процедурою обробки журналів, а й аналітичним процесом, спрямованим на розуміння поведінки системи, оцінювання ризиків і своєчасне прийняття рішень щодо реагування. Найбільшу практичну цінність має не ізольований розгляд окремих подій, а їх поєднання у логічні послідовності, які відображають можливий розвиток інциденту безпеки.

У результаті проведеного дослідження проаналізовано основні типи подій інформаційної безпеки та визначено їх значення для моніторингу інформаційно-комунікаційних систем.

Розроблено сценарій моніторингу, що базується на використанні порогових та кореляційних правил аналізу подій. Запропонований підхід дозволяє виявляти спроби несанкціонованого доступу, атаки brute force, ескалацію привілеїв та інші типи аномальної активності.

Моделювання процесу аналізу подій у середовищі Python підтвердило ефективність запропонованого підходу та можливість його використання як основи для побудови систем моніторингу класу SIEM.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

To chapter 1

1. Kravchenko, S. (2025). Economic efficiency and adaptability of the development of entrepreneurial entities engaged in grape production in times of war. *International Scientific Journal "Internauka". Series: "Economic Sciences"*, 11(103). doi: <https://doi.org/10.25313/2520-2294-2025-11-11598>.

2. Kravchenko, S. (2025). Analysis of the organizational and economic development of entrepreneurial structures in the agricultural sector of the economy under martial law. *Moderní aspekty vědy : LX. Díl mezinárodní kolektivní monografie / Mezinárodní Ekonomický Institut s.r.o. Česká republika: Mezinárodní Ekonomický Institut s.r.o., P. 86-97*. doi: <https://doi.org/10.52058/60-2025>.

3. Kravchenko, S. (2025). Economic efficiency of the development of micro-enterprises engaged in grape production and their adaptation to war conditions. *International Scientific Journal "Internauka". Series: "Economic Sciences"*, 11(104). doi: <https://doi.org/10.25313/2520-2294-2025-12-11681>.

4. Kravchenko, S. (2025). Effectiveness of the development of entrepreneurial structures for the production of plant products and their organisational-economic adaptation to the conditions of war in Ukraine. *Economics, sociology, business, administration and services: modern technologies and theories : collective monograph. Section – Economy / Breus S., Siruk O. etc. International Science Group. USA, Boston: Primedia eLaunch, P. 55-66*. doi: <https://doi.org/10.46299/ISG.2025.MONO.ECON.3.1.3>.

5. Kravchenko, S. (2026). Economic adaptation of small agribusiness enterprises to operate in war conditions and stimulating their european integration development. *Modern challenges and opportunities of the economy: analysis of new trends in management, implementation of technologies and ideas in tourism : collective monograph. Section – Economy / Bahalika T. etc. International Science*

Group. Boston : Primedia eLaunch, 608 p. P. 73-83. doi: <https://doi.org/10.46299/ISG.2026.MONO.ECON.1.2.3>.

6. Latifundist.com. Official web-site. (n.d.). Retrieved from : <https://latifundist.com/analytics/39-derzhavna-ta-mizhnarodna-pidtrimka-agrosektoru-u-2026-rotsi-granti-krediti-dotatsiyi>.

7. Matiienko, V. (2024). Formation of the management mechanism for the development of agricultural enterprises in rural areas. *Journal of Strategic Economic Research*, 25(3), 93-107. doi: <https://doi.org/10.30857/2786-5398.2024.3.10>.

8. Adamchuk, V., Perepelytsia, N., Hrytsyshyn, M. (2026). Intelligent agriculture – a determinant of innovative development of technical support for agro-industrial production. *Bulletin of Agricultural Science*, 104(2). doi: <https://doi.org/10.31073/agrovisnyk202602-05>.

9. Aksenko, P.A. (2024). Organizational and economic mechanism of development of agricultural formations: theoretical content and interaction algorithm. *Journal of Management, Economics and Technologies*, 2, 63-74. doi: <https://doi.org/10.69803/3083-6034-2024-2-63>.

10. Aksenko, P.A. (2025). Innovative transformation of the organizational and economic mechanism of the development of agricultural formations: strategic vectors of modernization. *Journal of Management, Economics and Technologies*, 4, 87-102. doi: <https://doi.org/10.69803/3083-6034-2025-4-87>.

11. Vasiliev, A.S. (2025). Adaptive business strategies as a tool for increasing the competitiveness of enterprises in conditions of uncertainty. *Business Inform*, 12, 57-57. doi: <https://doi.org/10.32983/2222-4459-2025-12-57-57>.

12. State Statistics Service of Ukraine. (n.d.). Retrieved from <http://www.ukrstat.gov.ua>.

13. Dyukarev, A.O., Chernega, I.I. (2025). Methodological principles of business management in agribusiness in the context of digital transformation and

sustainable development. *Journal of Management, Economics and Technologies*, 2, 307-321. doi: <https://doi.org/10.69803/3083-6034-2025-2-307>.

14. Zolotnytska, Y.V. (2025). Methodological approaches to managing the development of family farming: an interdisciplinary dimension. *Agrosvit*, 19, 86-94. doi: <https://doi.org/10.32702/2306-6792.2025.19.86>.

15. Ilchuk, M.M., Svinous, I.V., Tomashevskaya, O.A. (2024). Organizational and economic support for the competitiveness of agribusiness enterprises. *Agrosvit*, 22, 31-37. doi: <https://doi.org/10.32702/2306-6792.2024.22.31>.

16. Kalachevska, L. (2025). The impact of digitalization on the efficiency of the production process in the agricultural sector. *Bulletin of Sumy National Agrarian University*, 4(104), 49-56. doi: <https://doi.org/10.32782/bsnau.2025.4.8>.

17. Kyrylko, N.M. (2025). Modeling the organizational process of enterprise recovery in post-conflict conditions. *Journal of Management, Economics and Technologies*, 2, 33-46. doi: <https://doi.org/10.69803/3083-6034-2025-2-33>.

18. Koval, V.V., Savenko, I.I., Gontaruk, Ya.V., Metil, T.K., Drozdova, V.A., Asaulenko, N.V. (2025). Financial and credit support for grain production in agricultural enterprises: strategic approaches to minimizing risks and ensuring food security. *Business Inform*, 9, 297-309. doi: <https://doi.org/10.32983/2222-4459-2025-9-297-309>.

19. Livinsky, A., Melnychuk, O., Petrenko, O. (2024). Development of farming as a form of agrarian entrepreneurship in the context of institutional transformations. *Sustainable economic development*, 1(48), 378-383. doi: <https://doi.org/10.32782/2308-1988/2024-48-52>.

20. Lypovy, D.V. (2025). Social responsibility management of agrarian business enterprises based on the methodology of continuous process improvement. *Business Inform*, 7, 285-292. doi: <https://doi.org/10.32983/2222-4459-2025-7-285-292>.

21. Mahsma, M.B., Banshchikov, P.G. (2025). Managing the competitiveness of business organizations in the agricultural sector. *Business Inform*, 9, 239-246. doi: <https://doi.org/10.32983/2222-4459-2025-9-239-246>.

22. Nitsenko, V.S., Ponomareva, M.S. (2025). Modeling of production and economic activities of an agricultural enterprise: a managerial aspect. *Journal of Management, Economics and Technologies*, 3, 3-17. doi: <https://doi.org/10.69803/3083-6034-2025-3-3>.

23. Oliynyk, T.I., Oliynyk, E.O., Shcherbakov, Y.M. (2025). The concept of effective management of the competitiveness of an agricultural enterprise. *Agrosvit*, 18, 100-106. doi: <https://doi.org/10.32702/2306-6792.2025.18.100>.

24. Orlov, V.V. (2025). Methodological basis and specifics of assessing factors for the development of the potential of agricultural enterprises. *Journal of Management, Economics and Technologies*, 4, 239-250. doi: <https://doi.org/10.69803/3083-6034-2025-4-239>.

25. Pavlova, G.E., Lopatovsky, V.G. (2026). Institutional support of economic sustainability of farms under the influence of military challenges. *Agrosvit*, 2, 21-28. doi: <https://doi.org/10.32702/2306-6792.2026.2.21>.

26. Ponomareva, M.S. (2025). Models of effective agribusiness management: organizational mechanisms and economic indicators. *Journal of Management, Economics and Technology*, 1, 154-169. doi: <https://doi.org/10.69803/3083-6034-2025-1-154>.

27. Prokopyshyn, O.S., Dranus, L.S., Dranus, V.V. (2026). Business process management in agricultural enterprises and their financial support. *Effective economy*, 2. doi: <https://doi.org/10.32702/2307-2105.2026.2.115>.

28. Svinous, I.V., Grinchuk, Yu.S., Paska, I.M., Nyanko, V.M., Zhelavska, N.V. (2026). Risk management as an element of the institutional architecture of management of production and economic activities of agricultural enterprises. *Agrosvit*, 2, 35-61. doi: <https://doi.org/10.32702/2306-6792.2026.2.55>.

29. Solyanyk, L.G. (2026). Optimization of the financing structure of agricultural enterprises in the conditions of modern transformations. *Effective Economy*, 2. doi: <https://doi.org/10.32702/2307-2105.2026.2.64>.

30. Sudomyr, S.M., Zhybak, M.M., Kulyak, M.R. (2025). Integrated mechanisms for developing the potential of small businesses: logistic and cooperative dimensions. *Journal of Management, Economics and Technologies*, 3, 118-129. doi: <https://doi.org/10.69803/3083-6034-2025-3-118>.

31. Tulchynska, S., Kryvda, O. (2024). Capitalization of agro-industrial companies in conditions of macroeconomic instability. *Economy and Society*, 59. doi: <https://doi.org/10.32782/2524-0072/2024-59-71>.

32. Khalatur, S.M. (2025). Financial management of the competitiveness of agricultural enterprises in the context of ESG transformations. *Effective economy*, 12. doi: <https://doi.org/10.32702/2307-2105.2025.12.3>.

33. Khalatur, S.M., Grabchuk, O.M., Pavlenko, O.P., Manzheliy, K.M. (2025). Financial management in small agribusiness: adaptive strategies for financial support. *Agrosvit*, 17, 43-47. doi: <https://doi.org/10.32702/2306-6792.2025.17.43>.

34. Shchadura-Nikiporets, N.T., Derii, Zh.V., Minina, O.V. (2026). Financial condition of agro-industrial enterprises in conditions of economic instability. *Agrosvit*, 4, 68-76. doi: <https://doi.org/10.32702/2306-6792.2026.4.68>.

До розділу 2

1. Awan U., Kanwal N., Alawi S., Huiskonen J., Dahanayake A. *Artificial Intelligence for Supply Chain Success in the Era of Data Analytics* // In: The Fourth Industrial Revolution: Implementation of Artificial Intelligence for Growing Business Success. Cham : Springer, 2021. P. 3–21. DOI: https://doi.org/10.1007/978-3-030-62796-6_1

2. Blackburn O., Ritala P., Keränen J. *Digital Platforms for the Circular Economy: Exploring Meta-Organizational Orchestration Mechanisms* // Organi-

zation & Environment. 2023. Vol. 36. No. 2. P. 253–281. DOI: <https://doi.org/10.1177/10860266221130717>

3. Cioffi R., Travaglioni M., Piscitelli G., Petrillo A., Parmentola A. *Smart Manufacturing Systems and Applied Industrial Technologies for a Sustainable Industry: A Systematic Literature Review // Applied Sciences*. 2020. Vol. 10. No. 8. Article 2897. DOI: <https://doi.org/10.3390/app10082897>

4. Ghisellini P., Cialani C., Ulgiati S. *A Review on Circular Economy: The Expected Transition to a Balanced Interplay of Environmental and Economic Systems // Journal of Cleaner Production*. 2016. Vol. 114. P. 11–32. DOI: <https://doi.org/10.1016/j.jclepro.2015.09.007>

5. Hoosain M. S., Paul B. S., Ramakrishna S. *The Impact of 4IR Digital Technologies and Circular Thinking on the United Nations Sustainable Development Goals // Sustainability*. 2020. Vol. 12. No. 23. Article 10143. DOI: <https://doi.org/10.3390/su122310143>

6. Noman A. A., Akter U. H., Pranto T. H., Haque A. B. *Machine Learning and Artificial Intelligence in Circular Economy: A Bibliometric Analysis and Systematic Literature Review // Annals of Emerging Technologies in Computing*. 2022. Vol. 6. No. 2. P. 13–40. DOI: <https://doi.org/10.33166/AETiC.2022.02.002>

7. Petrik D., Hiller S., Morar D. *Digital Platforms for Circular Economy: Empirical Development of a Taxonomy and Archetypes // Electronic Markets*. 2025. Vol. 35. Article 60. DOI: 10.1007/s12525-025-00792-w.

8. Ramakrishna S., Ngowi A., De Jager H., Awuzie B. *Emerging Industrial Revolution: Symbiosis of Industry 4.0 and Circular Economy: The Role of Universities // Science, Technology and Society*. 2020. Vol. 25. No. 3. P. 505–525. DOI: <https://doi.org/10.1177/0971721820912918>

9. Wilts H., Riesco Garcia B., Guerra Garlito R., Saralegui Gómez L., González Prieto E. *Artificial Intelligence in the Sorting of Municipal Waste as an Enabler of the Circular Economy // Resources*. 2021. Vol. 10. No. 4. Article 28. DOI: <https://doi.org/10.3390/resources10040028>

10. Wu H., Li S., Hou W., Zhang X. *Leveraging Digital Platforms for Circular Economy: A Value Creation View // Sustainability*. 2024. Vol. 16. Article 11180. DOI: <https://doi.org/10.3390/su162411180>

To chapter 3

1. CIPD. (2025). Talent Management: Factsheet. Chartered Institute of Personnel and Development. URL: <https://www.cipd.org/en/knowledge/factsheets/talent-factsheet/>

2. Deloitte. (2024). 2024 Global Human Capital Trends. Deloitte Insights. URL: <https://www.deloitte.com/ua/en/about/press-room/human-capital-trends.html>

3. Drahan, O. I., & Pylypenko, M. L. (2021). Development of talent management in the enterprise personnel management system. *Economy and Society*, 33. DOI: <https://doi.org/10.32782/2524-0072/2021-33-52> [in Ukrainian].

4. Dyakiv, O., Shushpanov, D., Prokhorovska, S., & Khlypovka, O. (2024). Innovative approaches to talent management under conditions of digital transformation. *Visnyk Ekonomiky*, 3, 73-95. DOI: 10.35774/visnyk2024.03.073 [in Ukrainian].

5. Yukhnovska, Yu. O., Didenko, A. V., & Ryzhenko, O. M. (2024). Human capital potential in the enterprise management system. *Scientific Bulletin of the International Humanitarian University. Series: Economics and Management*, 58. DOI: <https://doi.org/10.32782/2413-2675/2024-58-6> [in Ukrainian].

6. Kravariti, F., & Johnston, K. (2020). Talent Management: A Critical Literature Review and Research Agenda for Public Sector Human Resource Management. *Public Management Review*, 22(1), 75-95. DOI: 10.1080/14719037.2019.1638439.

7. OECD. (2025). Empowering the Workforce in the Context of a Skills-First Approach. Paris: OECD Publishing. URL:

https://www.oecd.org/en/publications/empowering-the-workforce-in-the-context-of-a-skills-first-approach_345b6528-en.html

8. Zavorodnii, A. (2025). The essence and evolution of human capital management in the context of digital transformation. *Economy and Society*, 74. DOI: <https://doi.org/10.32782/2524-0072/2025-74-23> [in Ukrainian].

9. Plaksiuk, O., Horvatova, O., & Yakushev, O. V. (2023). Human capital as a factor in improving company efficiency and competitiveness. *Academic Review*, 1. DOI: [10.32342/2074-5354-2023-1-58-12](https://doi.org/10.32342/2074-5354-2023-1-58-12) [in Ukrainian].

10. Kholodnytska, A., & Shkalaberda, V. (2023). Development and implementation of a talent-management system as a strategic innovative tool of personnel management. *Problems and Prospects of Economics and Management*, 2(34), 88-100. DOI: [https://doi.org/10.25140/2411-5215-2023-2\(34\)-88-100](https://doi.org/10.25140/2411-5215-2023-2(34)-88-100) [in Ukrainian].

До розділу 4

1. Чорнобай В. Лексико-семантичний аспект комунікації у соціальних мережах // Наукові праці МАУП. Філологія. 2023. № 5. С. 44–49.

2. Антонюк Г., Гоца В. Інтернет мовлення та соціальні медіа: аналіз використання мовних засобів у коментарях користувачів на форумах та у соціальних мережах // Наукові записки Острозької академії. 2023. № 15. С. 111–116.

3. Літвінова-Михальюк Т. Трансформація засобів комунікації: як інтернет і соціальні мережі впливають на політичну комунікацію і змінюють відчуття реальності // Обрії друкарства. 2022. № 1(11). С. 99–109.

4. Соколов Б. Цифровий дискурс у соціальних мережах: методологічні виклики дискурс-аналізу // Слобожанський науковий вісник. Серія: Філологія. 2025. № 10. С. 55–61.

5. Crystal D. *Language and the Internet*. Cambridge: Cambridge University Press, 2011. 272 p.

6. Goel R., Soni S., Goyal N. et al. The Social Dynamics of Language Change in Online Networks // arXiv. 2016. P. 1–12.
7. Shao C., Ciampaglia G., Varol O. et al. The spread of low-credibility content by social bots // arXiv. 2017. P. 1–10.
8. Швелідзе Л. Соціальна мережа Twitter: основні дискурсивні ознаки в українськомовному та англійськомовному комунікативному середовищі // Вісник ОНУ. Філологія. 2021. № 2(24). С. 70–78.

До розділу 5

1. Макух, Т., Коробович, Л., & Рубан, В. (2023). СТІЙКІСТЬ ЯК МЕХАНІЗМ ЗАБЕЗПЕЧЕННЯ СТАЛОГО РОЗВИТКУ ПІДПРИЄМСТВА. *Таврійський науковий вісник. Серія: Економіка*, (18), 122-127. <https://doi.org/10.32782/2708-0366/2023.18.13>
2. Що таке сталий розвиток підприємства? URL: <https://tms.ua/blog/shcho-take-stalyj-rozvytok-pidpryiemstva/> (Дата звернення 03.05.2026 р.).
3. Сталий розвиток як основа економічного зростання підприємства URL: <https://confmanagement-proc.kpi.ua/article/view/230477> (Дата звернення 03.05.2026 р.).
4. Виправляємо плутанину між термінами «стійкість» і «сталість»: економічні приклади URL: <https://ukraine-oss.com/vypravlyayemo-plutanynu-mizh-terminamy-stijkist-i-stalist-ekonomichni-pryklady/> (Дата звернення 03.05.2026 р.).
5. Хахалев Д., Гагарінов О. Економічна стійкість підприємства як основа сталого розвитку в умовах глобальних змін. *Modeling the development of the economic systems*. 2024. № 3. С. 145-151. DOI: <https://doi.org/10.31891/mdes/2024-13-19>

6. Кудріна О., Ковтун О.. Стійкість як основа економічного розвитку підприємств. *Зб. наук. пр. Державного податкового університету*. 2024. № 2. С. 61-64. DOI: <https://doi.org/10.32782/2617-5940.2.2024.11>

7. Ковтун О. А. *Методологія управління стійким розвитком підприємств в сучасних умовах: монографія; за наук. ред. О.Ю. Кудріної*. Суми : ФОП Цьома С.П., 2024. 310 с.

До розділу 6

1. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР. URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text>

2. Конвенція про права осіб з інвалідністю : Конвенція ООН від 13.12.2006. URL: https://zakon.rada.gov.ua/laws/show/995_g71#Text

3. Про основи соціальної захищеності осіб з інвалідністю в Україні : Закон України від 21.03.1991 № 875-XII. URL: <https://zakon.rada.gov.ua/laws/show/875-12#Text>

4. Про реабілітацію осіб з інвалідністю в Україні : Закон України від 06.10.2005 № 2961-IV. URL: <https://zakon.rada.gov.ua/laws/show/2961-15#Text>

5. Про засади запобігання та протидії дискримінації в Україні : Закон України від 06.09.2012 № 5207-VI. URL: <https://zakon.rada.gov.ua/laws/show/5207-17#Text>

6. Convention for the Protection of Human Rights and Fundamental Freedoms. Rome, 1950. URL: https://www.echr.coe.int/documents/convention_eng.pdf

7. Americans with Disabilities Act of 1990. URL: <https://www.ada.gov/law-and-regs/ada/>

8. ADA Requirements: Service Animals. URL: <https://www.ada.gov/resources/service-animals-2010-requirements/>

9. European Accessibility Act: Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019. URL: <https://eur-lex.europa.eu/eli/dir/2019/882/oj>
10. Quinn G., Degener T. Human Rights and Disability: The Current Use and Future Potential of United Nations Human Rights Instruments in the Context of Disability. New York ; Geneva : United Nations, 2002. 289 p.
11. Lawson A. Disability and Equality Law in Britain: The Role of Reasonable Adjustment. Oxford : Hart Publishing, 2008. 304 p.
12. Shakespeare T. Disability Rights and Wrongs Revisited. London : Routledge, 2014. 252 p.
13. Gooding P. A New Era for Mental Health Law and Policy: Supported Decision-Making and the UN Convention on the Rights of Persons with Disabilities. Cambridge : Cambridge University Press, 2017. 280 p.
14. United Nations. Accessibility and Development: Mainstreaming disability in the post-2015 development agenda. New York : United Nations, 2013. URL: https://www.un.org/disabilities/documents/accessibility_and_development.pdf
15. Wackenheim v. France, Communication No. 854/1999, U.N. Doc. CCPR/C/75/D/854/1999 (2002).
16. Harpur P. Discrimination, Copyright and Equality: Opening the E-Book for the Print Disabled. Cambridge : Cambridge University Press, 2017. 424 p.
17. Stein M. A., Lord J. E. Future Prospects for the United Nations Convention on the Rights of Persons with Disabilities. In: The UN Convention on the Rights of Persons with Disabilities. Oxford : Oxford University Press, 2018. P. 17–35.

До розділу 7

1. Khalfallah H. B., Jelassi M., Demongeot J., Ben Saoud N. B. Decision support systems in healthcare: systematic review, meta-analysis and prediction, with example of COVID-19 // *AIMS Bioengineering*. 2023. Vol. 10, No. 1. P. 27–52.
2. Marashi-Hosseini L., Jafarirad S., Hadianfard A. M. A fuzzy based dietary clinical decision support system for patients with multiple chronic conditions (MCCs) // *Scientific Reports*. 2023. Vol. 13. Article 12166.
3. Tun H. M., Rahman H. A., Naing L., Malik O. A. Trust in Artificial Intelligence-Based Clinical Decision Support Systems: Systematic Review // *Journal of Medical Internet Research*. 2025. Vol. 27. Article e69678.
4. Nasarian E., Alizadehsani R., Acharya U. R., Tsui K.-L. Designing Interpretable ML System to Enhance Trust in Healthcare: A Systematic Review to Proposed Responsible Clinician-AI-Collaboration Framework. 2023. arXiv:2311.11055.
5. Hossain E., Rana R., Higgins N. et al. Natural Language Processing in Electronic Health Records in Relation to Healthcare Decision-making: A Systematic Review. 2023. arXiv:2306.12834.
6. Li S., Liu P., Nascimento G. G. et al. Federated and Distributed Learning Applications for Electronic Health Records and Structured Medical Data: A Scoping Review. 2023. arXiv:2304.07310.
7. Квітка Д. М., Паламарчук В. О., Земсков С. В., Січінава Р. М. Введення поняття якості життя в практичну медицину. *Clinical Endocrinology and Endocrine Surgery*. 2021. № 1 (73). С. 70–75.
8. Centers for Disease Control and Prevention. Health-Related Quality of Life (HRQOL): CDC HRQOL-4. URL: <https://www.cdc.gov/hrqol> (дата звернення: 15.05.2026).

До розділу 8

1. Гришко І. В. Психолого педагогічні аспекти професійного самовизначення викладача вищої школи / І. В. Гришко // Вісник педагогічних наук. — 2023. — № 4. — С. 67–75.

2. Гріньова О. М. Професійне самовизначення особистості як психолого педагогічна проблема / О. М. Гріньова // Освіта. Інноватика. Практика. — 2023. — № 5 (11). — С. 52–58.

3. Дідусь О. М. Психолого педагогічний супровід особистісного і професійного самовизначення фахівців у системі вищої освіти / О. М. Дідусь. — К.: НАПН України, 2022. — 144 с.

4. Зінкевич Лісова Н. В. Психолого педагогічні основи професійного самовизначення викладача в епоху цифрових трансформацій / Н. В. Зінкевич Лісова // Вісник Київського університету. Серія «Педагогіка та психологія». — 2024. — № 1. — С. 82–91.

5. Кравчук Л. А. Професійна адаптація та самовизначення викладача в умовах сучасних освітніх реформ / Л. А. Кравчук // Вісник Херсонського державного університету. Серія «Педагогіка». — 2023. — № 3. — С. 105–114.

6. Мельник О. В. Психолого педагогічні детермінанти професійного самовизначення викладачів у закладах вищої освіти / О. В. Мельник // Науковий вісник педагогічного інституту. — 2022. — Вип. 21. — С. 118–126.

7. Освіта України. Професійний стандарт викладача закладу вищої освіти / МОН України. — К.: Освіта.UA, 2021. — 18 с. (рекомендовано використовувати як нормативне джерело).

8. Павличко О. В. Психолого педагогічний аналіз професійного вибору викладача в закладі вищої освіти / О. В. Павличко // Педагогічні науки: теорія, історія, інноваційні технології. — 2024. — Вип. 23. — С. 95–104.

9. Степаненко І. М. Професійне самовизначення викладача як фактор якості освітнього процесу / І. М. Степаненко // Вісник Житомирського

державного університету імені І. Франка. Серія «Педагогіка та психологія». — 2022. — Вип. 1. — С. 132–141.

10. Шевченко Л. В. Психолого педагогічна модель професійного самовизначення викладача в закладі вищої освіти / Л. В. Шевченко // Journal «ScienceRise: Pedagogical Education». — 2023. — № 1(21). — С. 56–64.

До розділу 9

1. National Institute of Standards and Technology. *Guide to Computer Security Log Management* : NIST Special Publication 800-92 / К. Kent, М. Soupra. Gaithersburg : NIST, 2006. 72 p.

2. Microsoft. *Windows Security Event Log Reference*. URL: <https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/security-events> (дата звернення: 20.05.2026).

3. Chuvakin A., Schmidt K., Phillips C. *Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management*. Waltham : Syngress, 2012. 460 p.

4. Verizon. *2024 Data Breach Investigations Report*. URL: <https://www.verizon.com/business/resources/reports/dbir/> (дата звернення: 20.05.2026).

5. MITRE. *MITRE ATT&CK Framework*. URL: <https://attack.mitre.org/> (дата звернення: 20.05.2026).

6. pandas. *Time Series / Date functionality*. URL: https://pandas.pydata.org/docs/user_guide/timeseries.html (дата звернення: 20.05.2026).

7. Behl A., Behl K. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford : Oxford University Press, 2017. 272 p.

8. Scarfone K., Mell P. *Guide to Intrusion Detection and Prevention Systems (IDPS)* : NIST Special Publication 800-94. Gaithersburg : NIST, 2007. 127 p.

9. ISO/IEC 27001:2022. *Information security, cybersecurity and privacy protection – Information security management systems – Requirements*. Geneva : ISO, 2022.

Vydavatel:

Publishing house Education and Science s.r.o. IČO : 271 56 877.
Frýdlanská 15/1314 , Praha 8. MS v Praze , oddíl C,vložka 100614

**Cross-Disciplinary Studies in
Science, Innovation and Social
Development**

Volume XII

Signed for printing on May 26, 2026.
Format 60x90/8. Headset Times New Roman.
Mental printing. arc. 6,03. Edition online.