

УДОСКОНАЛЕННЯ СИСТЕМ УПРАВЛІННЯ ПІДПРИЄМСТВОМ ДЛЯ ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ ДАНИХ В УМОВАХ ЗАСТОСУВАННЯ ІНСТРУМЕНТІВ ШТУЧНОГО ІНТЕЛЕКТУ

©2026 ДОБОСЕВИЧ Я. В., ШПАК Н. О.

УДК 005.95/.96:004.056:004.8
JEL: C88; D83; L86; M10; M15; O32; O33

Добосевич Я. В., Шпак Н. О. Удосконалення систем управління підприємством для забезпечення конфіденційності даних в умовах застосування інструментів штучного інтелекту

Метою статті є розробка та емпіричне тестування організаційно-управлінської моделі, що забезпечує баланс між безпекою чутливих даних та їх доступністю для систем машинного навчання (ML) на інноваційному підприємстві. Дослідження закриває прогалину, спричинену тим, що наявні наукові підходи розглядають безпеку даних у ML переважно з технічного та юридичного боку, тоді як організаційно-управлінська інтеграція цих процесів залишається малодослідженою: на перетині інтересів інженерів, які прагнуть максимального доступу до даних, і служби безпеки, яка цей доступ обмежує, виникає системний конфлікт, що уповільнює розробку та підвищує ризик витоку. Методологію дослідження становлять: метод аналітичної ієрархії (MAI) для калібрування вагових коефіцієнтів інтегральної моделі ефективності управління даними на основі цільової експертної вибірки із 7 фахівців-практиків (технічні директори, керівники ML-команд, директори з інформаційної безпеки); імітаційне моделювання діяльності IT-департаменту з 5 крос-функціональних команд упродовж двох піврічних періодів за контрольним та експериментальним сценаріями; економічне оцінювання доцільності впровадження. За результатами запропоновано виокремити спеціалізовану управлінську роль «AI Data Custodian» і супровідний процесний протокол «Data-Sec-AIOps». Імітаційне моделювання підтвердило гіпотезу: впровадження ролі скоротило час доступу до підготовлених даних (Time-to-Data) на 71% (з 14,5 до 4,2 дня), знизило кількість інцидентів безпеки на 83% (з 12 до 2), зменшило частку неструктурованих даних із 22% до 5% та підвищило середню точність ML-моделей (F1) із 0,74 до 0,86. Інвестиції окупуються протягом 4–5 місяців, а орієнтовна річна економія для підприємства з 5 ML-командами становить 300 000–440 000 дол. США. Наукова новизна полягає у зміщенні фокусу з технічного блокування доступу на превентивний менеджмент даних через управління впливом (management by influence): Custodian не забороняє доступ, а створює безпечні середовища (secure enclaves), керує анонімізацією та синтетичними даними і виступає єдиним центром відповідальності за життєвий цикл даних для ML, маючи операційну, на відміну від CDO та DPO, природу. Практична цінність дослідження – дорожня карта впровадження ролі з п'яти фаз (діагностика – дизайн – технологічне забезпечення – пілот – масштабування) та система з п'яти KPI для вимірювання її ефективності; запропонований підхід може слугувати методологічною основою для побудови систем data governance на українських інноваційних підприємствах, що інтегруються в європейський регуляторний простір згідно з вимогами GDPR і AI Act.

Ключові слова: конфіденційність даних; машинне навчання; система управління підприємством; AI Data Custodian; організаційно-управлінська модель; кібербезпека; data governance; штучний інтелект.

Рис.: 1. Табл.: 2. Формул.: 2. Бібл.: 40.

Добосевич Ярослав Володимирович – аспірант кафедри менеджменту та міжнародного підприємництва, Національний університет «Львівська політехніка» (вул. Степана Бандери, 12, Львів, 79013, Україна)

E-mail: yaroslav.dobosevych.asp.2025@lpnu.ua

ORCID: <https://orcid.org/0009-0007-7423-9267>

Шпак Нестор Омелянович – доктор економічних наук, професор, професор кафедри менеджменту та міжнародного підприємництва, Національний університет «Львівська політехніка» (вул. Степана Бандери, 12, Львів, 79013, Україна)

E-mail: nestor.o.shpak@lpnu.ua

ORCID: <https://orcid.org/0000-0003-0620-2458>

UDC 005.95/.96:004.056:004.8
JEL: C88; D83; L86; M10; M15; O32; O33

Dobosevych Ya. V., Shpak N. O. Improving Enterprise Management Systems to Ensure Data Confidentiality in the Context of Artificial Intelligence Tools Application

The aim of the article is to develop and empirically test an organizational and managerial model that ensures a balance between the security of sensitive data and its availability for machine learning (ML) systems at an innovative enterprise. The study addresses a gap arising from the fact that existing scientific approaches consider data security in ML mainly from the technical and legal perspectives, while the organizational and managerial integration of these processes remains underexplored: a systemic conflict emerges at the intersection of the interests of engineers, who seek maximum access to data, and the security function, which restricts such access, slowing down development and increasing the risk of leaks. The research methodology comprises: the Analytic Hierarchy Process (AHP) for calibrating the weighting coefficients of an integral model of data management efficiency, based on a purposive expert sample of 7 practitioners (chief technology officers, ML team leads, chief information security officers); a simulation of an IT department of 5 cross-functional teams over two six-month periods under control and experimental scenarios; and an economic feasibility assessment. As a result, the study proposes introducing a dedicated managerial role, the AI Data Custodian, and an accompanying process protocol, Data-Sec-AIOps. The simulation confirmed the hypothesis: introducing the role reduced the time to access prepared data (Time-to-Data) by 71% (from 14.5 to 4.2 days), decreased the number of security incidents by 83% (from 12 to 2), reduced the share of unstructured data from 22% to 5%, and increased the average accuracy of ML models (F1) from 0.74 to 0.86. The investment pays off within 4–5 months, and the estimated annual savings for an enterprise with 5 ML teams amount to USD 300,000–440,000. The scientific novelty lies in shifting the focus from technical access blocking to preventive data management through management by influence: the Custodian does not prohibit access but creates secure

enclaves, manages anonymization and synthetic data, and acts as the single point of accountability for the ML data lifecycle, having an operational rather than strategic nature, unlike the CDO and DPO. The practical value of the study is a five-phase implementation roadmap (diagnostics – design – technological enablement – pilot – scaling) and a system of five KPIs for measuring the role's efficiency; the proposed approach can serve as a methodological basis for building data governance systems at Ukrainian innovative enterprises integrating into the European regulatory space in line with GDPR and the AI Act requirements.

Keywords: data confidentiality; machine learning; enterprise management system; AI Data Custodian; organizational and managerial model; cybersecurity; data governance; artificial intelligence.

Fig.: 1. Tabl.: 2. Formulae: 2. Bibl.: 40.

Dobosevych Yaroslav V. – Postgraduate Student of the Department of Management and International Entrepreneurship, National University «Lviv Polytechnic» (12 Stepana Bandery Str., Lviv, 79013, Ukraine)

E-mail: yaroslav.dobosevych.asp.2025@lpnu.ua

ORCID: <https://orcid.org/0009-0007-7423-9267>

Shpak Nestor O. – D. Sc. (Economics), Professor, Professor of the Department of Management and International Entrepreneurship, National University «Lviv Polytechnic» (12 Stepana Bandery Str., Lviv, 79013, Ukraine)

E-mail: nestor.o.shpak@lpnu.ua

ORCID: <https://orcid.org/0000-0003-0620-2458>

Системи штучного інтелекту (ШІ) в застосуванні в сучасних, інноваційних підприємствах виступають драйверами автоматизації, предиктивної аналітики та оптимізації бізнес-процесів. Проте ключовим «паливом» для будь-якої моделі машинного навчання є дані. Для ефективного аналізу, синтезу та генерування відповідей сучасні моделі потребують колосальних масивів інформації, обсяги яких подвоюються кожні 2–3 роки. Згідно з аналітикою International Data Corporation, у 2025 р. світовий обсяг створених і реплікованих даних перевищить 180 зетабайт, причому понад 80% із них становитимуть неструктуровані дані з потенційно конфіденційним змістом [1].

Економічні наслідки витоку інформації для підприємств давно вийшли за межі простих витрат на відновлення ІТ-інфраструктури. За звітом IBM Security «Cost of a Data Breach Report 2024», середня вартість, яка лягає на компанію після інциденту порушення безпеки даних у світі, досягла 4,88 млн доларів США – це історичний максимум і зростання на 10% порівняно з попереднім роком [2]. Інциденти, які стосуються ML-систем і навчальних датасетів, обходяться компаніям ще дорожче: середня вартість витоку через так звану «shadow AI» – некеровані експерименти інженерів із виробничими даними – становить 4,63 млн доларів. Кожен байт конфіденційних даних сьогодні має чіткий грошовий еквівалент, а його втрата запускає ланцюгову реакцію: від юридичних штрафів за порушення регуляторних протоколів (наприклад, GDPR, де штрафи сягають 4% річного обороту [3]) до прямих втрат інтелектуальної власності, що забезпечувала конкурентну перевагу.

Матеріальна цінність інформації підприємства проявляється в момент її відсутності, коли зупинка бізнес-процесів через недоступність баз даних або компрометацію комерційної таємниці

призводить до стрімкого падіння ринкової вартості компанії. У цифровій економіці дані – це не просто супутній актив, а фундаментальний капітал, вилучення якого з обороту здатне довести навіть стійке підприємство до банкрутства [4].

Найбільш руйнівним наслідком інцидентів із безпекою є деградація «гудвілу» (*goodwill*) – нематеріального активу, що втілює ділову репутацію та лояльність клієнтів. Коли конфіденційна інформація стає публічною або потрапляє до рук зловмисників, компанія втрачає кредит довіри, що будувався роками. Цей актив надзвичайно крихкий: на відміну від пошкодженого обладнання, репутацію неможливо просто замінити за страховим полісом. Втрата *goodwill* конвертується в цілком реальні цифри: відтік клієнтів, зниження інвестиційної привабливості, необхідність колосальних витрат на кризовий PR. Показовим є кейс компанії Samsung (квітень 2023 р.), коли інженери випадково передали службовий вихідний код у публічний інтерфейс ChatGPT. Після цього інциденту компанія повністю заборонила використання генеративного ШІ для робочих завдань, а її акції зазнали короткострокової корекції [5].

Таким чином, безпека даних стає не просто технічним завданням, а стратегічною функцією збереження ринкової капіталізації та життєздатності бренду. Ці дані часто є чутливими, становлять комерційну таємницю, містять персональну інформацію клієнтів та є предметом інтелектуальної власності компанії. Їхня ринкова вартість стрімко зростає, а отже, ризики та наслідки їх втрати, витоку чи несанкціонованої модифікації критично недооцінені в сучасному корпоративному управлінні. Інноваційні підприємства стикаються з парадоксом: для отримання конкурентної переваги через ШІ необхідно відкри-

вати доступ до даних, але для збереження стійкості – ці дані потрібно жорстко захищати.

Для України ця проблема має додаткове геополітичне забарвлення: відповідно до звітів Державної служби спеціального зв'язку та захисту інформації, у 2022–2024 рр. кількість кібератак на українські підприємства, зокрема із застосуванням ML-методів профілювання жертв, зросла у 2,8 разу. Це підвищує актуальність побудови організаційно-управлінських механізмів захисту даних саме на рівні систем менеджменту, а не лише технічними засобами.

ОГЛЯД ЛІТЕРАТУРИ ТА ВИДІЛЕННЯ НЕВИРІШЕНИХ ЧАСТИН ПРОБЛЕМИ

Питання безпеки даних підприємств у контексті використання машинного навчання розглядається в науковій літературі переважно з чотирьох ракурсів: економіко-управлінського, технічного, юридично-комплаєнсного та етично-філософського. Кожен із напрямів має значні напрацювання, проте, як буде показано далі, жоден не покриває організаційно-управлінський аспект інтеграції безпеки в життєвий цикл ML-моделі.

Економіко-управлінський підхід акцентує увагу на вартісних і організаційних вимірах безпеки даних у ML-проектах. Т. Davenport і Р. Ronanki (2018) розглянули практичні моделі впровадження ШІ на підприємствах, зокрема проблему оцінювання ROI та організаційної готовності до трансформації [26]. V. Mayer-Schönberger і К. Cukier (2013) одними з перших описали трансформацію даних на стратегічний капітал компанії, що принципово змінює логіку управлінських рішень щодо їх захисту [4]. Дослідники McKinsey Global Institute (Bughin et al., 2018) кількісно оцінили економічний потенціал ШІ та супутні операційні ризики, підкресливши, що витоки даних у ML-системах несуть не лише репутаційні, а й прямі фінансові наслідки для бізнесу. Етичний і стратегічний вимір представлений у працях L. Floridi та J. Cowsls (2019), які запропонували уніфіковану рамку п'яти етичних принципів ШІ [24], M. Brundage et al. (2018) у дослідженні «The Malicious Use of Artificial Intelligence» [25], С. O'Neil (2016), яка показала ризики алгоритмічної дискримінації [27], та S. Zuboff (2019) з концепцією «капіталізму спостереження» [28].

Технічний підхід розвивається у працях провідних дослідників із галузі прикладної криптографії та машинного навчання. Основу сучасного розуміння федеративного навчання заклала робота Н. В. McMahan та співавторів (2017), які запропонували алгоритм комунікаційно-ефективного навчання глибоких нейромереж на децентралізованих пристроях без передачі сирих даних на центральний сервер [6]. Подальші роботи К. Bonawitz et al. (2017)

розширили цю парадигму через протоколи безпечної агрегації (Secure Aggregation), які приховують внески окремих учасників навіть від координатора [7]. Паралельно розвинулась галузь диференційної приватності (Differential Privacy), теоретичні засади якої систематизовано С. Dwork та А. Roth (2014) [8], а практичне застосування для глибокого навчання продемонстровано в роботі М. Abadi et al. (2016) «Deep Learning with Differential Privacy» [9].

Окрему підгрупу становлять дослідження загроз, специфічних саме для ML-систем. R. Shokri et al. (2017) вперше системно описали *membership inference attacks* – атаки, що дозволяють визначити, чи входив конкретний запис у навчальну вибірку моделі [10]. N. Papernot, Р. McDaniel та співавтори створили таксономію загроз безпеки та приватності в ML (SoK, 2018), яка стала стандартом для академічних публікацій у цій сфері [11]. І. Goodfellow et al. (2015) виявили феномен *adversarial examples* – спеціально сконструйованих вхідних даних, які змушують модель робити неправильні прогнози з високою впевненістю [12]. В. Biggio та F. Roli (2018) проаналізували десятиріччя розвитку *adversarial machine learning* як самостійної дисципліни [13]. N. Carlini, F. Tramèr, E. Wallace et al. (2021) продемонстрували можливість екстракції фрагментів навчальних даних із великих мовних моделей, що відкрило нову категорію ризиків для генеративного ШІ [14]. Архітектурні рекомендації узагальнено в стандарті NIST SP 800-207 «Zero Trust Architecture» [15].

Юридичний і комплаєнс-підхід зосереджений на імплементації регуляторних вимог, що формують правове поле обробки даних у ML. Базовим документом для європейського ринку залишається Регламент (ЄС) 2016/679 «Загальний регламент про захист даних» (GDPR) [3], аналіз застосування якого в контексті ML наведено в роботі С. J. Hoofnagle, В. van der Sloot та F. Z. Borgesius (2019) [16]. Прийнятий у 2024 році Регламент (ЄС) 2024/1689 «Акт про штучний інтелект» (AI Act) уперше встановив ризик-орієнтований підхід до регулювання ШІ та запровадив окремі вимоги до high-risk систем [17]. Критичний аналіз положень AI Act здійснено в дослідженнях М. Veale та F. Z. Borgesius (2021) [18]. На рівні корпоративних стандартів ключову роль відіграють ISO/IEC 27001:2022 (системи менеджменту інформаційної безпеки) [19] та ISO/IEC 27701:2019 (управління приватністю) [20], а специфічно для ШІ – рамкова модель NIST AI Risk Management Framework (AI RMF 1.0, 2023) [21]. Український контекст представлений у Законі України «Про захист персональних даних» (№ 2297-VI) [22] та в Законі України «Про основні засади забезпечення кібербезпеки України» (№ 2163-VIII) [23].

Таким чином, аналіз наукової літератури засвідчує, що проблема безпеки даних у ML охоплена з різних сторін:

- ✦ *технічна школа* пропонує криптографічні та архітектурні інструменти захисту;
- ✦ *юридична* – формує регуляторну відповідальність;
- ✦ *економічна* – оцінює вартість ризиків і стратегічну цінність даних;
- ✦ *етична* – окреслює суспільні межі допустимого.

Водночас усі ці напрями залишаються здебільшого ізольованими: безпека розглядається або як функція IT-відділу, або як об'єкт нормативного контролю, тоді як процес підготовки даних для III перебуває у віданні інженерів (Data Scientists).

Узагальнення літературних джерел, практики діяльності сучасних підприємств і власні напрацювання дозволили виявити прогалину саме на перетині цих підходів: *у сучасних структурах управління інноваційними підприємствами бракує сполучної ланки, яка б керувала захистом даних крос-функціонально – маючи повноваження водночас у площині ML-розробки, кібербезпеки та управлінського прийняття рішень.*

Виникає системний конфлікт інтересів: інженери прагнуть максимального доступу до даних для якісного навчання моделей, тоді як служба безпеки прагне цей доступ мінімізувати, а менеджмент

не має інструментарію для його розв'язання на рівні організаційної структури. Саме на закриття цієї прогалини спрямоване подальше дослідження.

Класифікація специфічних загроз для ML-систем

Перш ніж запропонувати вдосконалення організаційної моделі управління, необхідно класифікувати специфічні для машинного навчання загрози. На відміну від традиційних кібератак, ML-системи мають унікальну поверхню атаки: модель, навчальні дані, інференс-конвеєр та інтерфейс взаємодії з користувачем. На основі синтезу таксономій N. Papernot et al. [11] та NIST AI RMF [21] виокремимо шість ключових категорій ризиків (табл. 1).

Як видно з табл. 1, спектр загроз значно ширший, ніж класичні витoki даних, і покриття цих ризиків потребує одночасних дій у площинах інженерії даних, ML-розробки та кібербезпеки. Жодна окрема функціональна одиниця підприємства немає достатньої експертизи для системного управління всіма категоріями загроз. Це підкріплює тезу про необхідність введення в систему управління додаткової ролі-інтегратора – AI Data Custodian.

ФОРМУЛЮВАННЯ ГІПОТЕЗИ ТА МЕТИ ДОСЛІДЖЕННЯ

Виходячи з виявленої прогалини, *метою* цієї статті є розробка та емпіричне тестування організаційно-управлінської моделі, що забезпечує

Таблиця 1

Класифікація специфічних загроз для ML-систем

Тип загрози	Сутність	Зона відповідальності AI Data Custodian
Забруднення даних (Data Poisoning)	Зловмисне внесення спотворених записів у навчальний датасет з метою деградації моделі або вбудовування «бекдору»	Контроль провенансу даних, версіювання датасетів, аудит каналів збору
Схиблені приклади (Adversarial Examples)	Спеціально сконструйовані вхідні дані, що змушують модель помилятися (I. Goodfellow et al., 2015)	Узгодження політик adversarial-тестування з QA-командою, формування red-team
Висновок про приналежність (Membership Inference)	Атаки, що дозволяють встановити належність конкретного запису до навчальної вибірки (R. Shokri et al., 2017)	Запровадження диференційної приватності, контроль рівня бюджету ε
Інверсія моделі (Model Inversion)	Відновлення характеристик навчальних даних шляхом систематичних запитів до моделі	Rate-limiting інференс-API, моніторинг патернів запитів
Копіювання моделі (Model Extraction)	Копіювання моделі-конкурента через систематичні запити та аналіз відповідей	Watermarking моделей, контракти на доступ до інференсу
Маніпуляції з запитами (Prompt Injection)	Маніпуляція поведінкою LLM через спеціально сконструйовані інструкції в користувацькому вводі (N. Carlini et al., 2021)	Політики санітазації prompts, ізоляція системних інструкцій

Джерело: авторська розробка.

баланс між безпекою чутливих даних та їх доступністю для систем машинного навчання в умовах інноваційного підприємства.

Гіпотеза дослідження. Якщо в організаційну структуру інноваційного підприємства запровадити виділену управлінську роль «AI Data Custodian» («Куратор безпеки та підготовки даних III»), яка діє через механізми непрямого впливу на функціональних лідерів (технічного директора, інженера, менеджера, фахівця забезпечення якості), та одночасно запровадити відповідний процесний протокол «Data-Sec-AIOps», це приведе до синергетичного ефекту. А саме: дані стануть структурованішими, очищенішими та придатнішими для роботи ML-систем при одночасному зниженні кількості інцидентів безпеки (Data Breach) та випадків близько до втрати (Near-miss).

Новизна підходу полягає у зміщенні фокусу з технічного блокування на превентивний менеджмент даних: Custodian не забороняє доступ, а створює безпечні «пісочниці» (*secure enclaves*), керує процесом анонімізації та виступає єдиним центром відповідальності за життєвий цикл даних для ML. На відміну від існуючих ролей директора з даних (Chief Data Officer – CDO) і директора з захисту даних (Data Protection Officer – DPO), Custodian має операційну, а не стратегічну природу та діє в режимі short-cycle коригувань спринтів.

Завдання дослідження:

- 1) обґрунтувати функціонал ролі AI Data Custodian;
- 2) сформулювати математичну модель ефективності управління даними для ML-сервісів;
- 3) провести імітаційне моделювання за двома сценаріями (контрольним та експериментальним);
- 4) оцінити економічну доцільність впровадження ролі;
- 5) сформулювати практичні рекомендації для інноваційних підприємств.

МЕТОДОЛОГІЯ ТА МОДЕЛЮВАННЯ ДОСЛІДЖЕННЯ

Для перевірки гіпотези авторами запропоновано інтегральну математичну модель оцінки ефективності управління даними для систем машинного навчання (ML), яка є функцією від якості даних, часу їхньої підготовки та рівня безпеки. В основу моделі покладено трикомпонентну структуру:

1. Показник якості даних (Dq), розроблений на базі багатовимірної концепції якості даних [29–31].
2. Показник часу підготовки та узгодження доступу (Ct), обґрунтований концепцією прихованого технічного боргу в ML-системах [32] і парадигмою операційного управління даними (DataOps) [33].

3. Показник рівня безпеки даних (Ds), побудований за аналогією з підходами кількісного оцінювання ризиків [34; 35].

За результатами узагальнення проаналізованих вище підходів та власних напрацювань запропонуємо інтегральну функцію такого вигляду:

$$f(y) = (Dq \cdot \alpha + Ct \cdot \beta) / Ds, \quad (1)$$

де: α, β – вагові коефіцієнти значущості для інноваційного підприємства, що визначаються методом аналітичної ієрархії (MAI) [36];

Dq – якість даних (інтегральний показник в умовних одиницях, що включає повноту, узгодженість і анованість) [29; 31];

Ct – час, витрачений на підготовку та узгодження доступу до даних (час підготовки даних, Time-to-Data), у людино-днях [32; 33];

Ds – експертна оцінка рівня безпеки даних за десятибальною шкалою [34; 35].

Калібрування коефіцієнтів α і β здійснювалось методом попарних порівнянь MAI [36; 37] на основі цільової експертної вибірки (*purposive sampling*) [39] із 7 фахівців-практиків інноваційних підприємств м. Києва:

- 1) технічних директорів (СТО);
- 2) керівників команд машинного навчання;
- 3) директорів з інформаційної безпеки (CISO).

Цільовий відбір обґрунтований тим, що для зважування параметрів операційної моделі управління даними необхідна функціональна компетенція відповідного профілю, а не статистично репрезентативна вибірка [39]. Кількість учасників відповідає рекомендованому для MAI діапазону 5–15 осіб [38]. Відповідно до вимог методу, узгодженість суджень підтверджена розрахунком коефіцієнта узгодженості ($CR < 0,10$) [36], що свідчить про внутрішню несуперечливість отриманих оцінок. Агрегування індивідуальних суджень здійснено методом геометричного середнього [40]. Усереднені значення склали $\alpha = 0,62$ та $\beta = 0,38$, що відображає пріоритет якості даних над швидкістю їх підготовки в умовах регульованих галузей.

Моделювання здійснювалось шляхом імітації діяльності IT-департаменту умовного інноваційного підприємства (вибірка: 5 крос-функціональних команд, у кожній – 1 керівник інженерної команди (*Engineering Manager*), 3 ML-інженери та 1 інженер з даних) протягом двох послідовних умовних періодів по 6 місяців.

Етап 1 (Control Group / Baseline). Робота за стандартною Agile-схемою. Запити на дані для III погоджуються через СТО та відділ безпеки послідовно (Waterfall-погодження в Agile-середовищі). Жодна окрема роль для управління життєвим циклом даних не виокремлена.

Етап 2 (Experimental Group). Впровадження ролі «AI Data Custodian», який модерує процеси через механізми впливу та попередньо підготовлені політики синтетичних даних (Synthetic Data Generation) і маскуванню. Custodian координує безпечні enclave-середовища відповідно до моделі Zero Trust [15], а ML-команди працюють із підготовленими, де-ідентифікованими копіями даних.

Оцінювалися такі метрики:

- 1) кількість інцидентів порушення конфіденційності (Data Breach та Near-miss);
- 2) середня швидкість доставки підготовленого датасету команді ML (Time-to-Data, у робочих днях);
- 3) відсоток неструктурованих / «сміттєвих» даних, що потрапили в середовище навчання;
- 4) середня точність ML-моделей на тестовій вибірці (проху-показник якості даних).

Для оцінки економічної доцільності модель була доповнена параметром мінімізації фінансових втрат від інцидентів безпеки (L_{risk}):

$$E = \sum C_{saved} - (S_{custodian} + I_{infra}) + L_{risk_avoided}, \quad (2)$$

де: C_{saved} – заощаджені кошти внаслідок скорочення простою ML-команд; $S_{custodian}$ – витрати на утримання нової штатної одиниці; I_{infra} – інвестиції в інструменти анонімізації та «пісочниці»; $L_{risk_avoided}$ – очікувана вартість уникнутих штрафів (зокрема, за GDPR – до 4% річного обороту [3]) і репутаційних втрат.

Підставляючи орієнтовні значення для підприємства з 5 ML-командами:

$C_{saved} \approx 300\,000\text{--}440\,000$ дол. США на рік (вивільнені людино-години);

$S_{custodian} \approx 48\,000\text{--}66\,000$ дол. США на рік (заробітна плата на рівні 15–25% вище за Senior ML-інженера [38]);

$I_{infra} \approx 15\,000\text{--}25\,000$ дол. США одноразово (ліцензії на інструменти анонімізації та enclave-середовищ).

Таким чином, сукупні витрати першого року складають орієнтовно 63 000–91 000 дол. США. При річній економії 300 000–440 000 дол. США точка беззбитковості досягається через:

$$T = (S_{custodian} \cdot (M / 12) + I_{infra}) / (C_{saved} / 12) \approx 4\text{--}5 \text{ місяців},$$

де M – кількість місяців до кінця першого року. $L_{risk_avoided}$ у цьому розрахунку не враховується, що робить оцінку консервативною: зниження кількості подій Near-miss з 12 до 2 статистично еквівалентне уникненню щонайменше одного значного інциденту на рік, потенційна вартість якого для підприємства з оборотом 50 млн євро може перевищувати 2 млн євро у вигляді GDPR-штрафів [3].

Результати моделювання показали, що інвестиції в упровадження ролі Custodian окупуються протягом перших 4–5 місяців роботи завдяки радикальному зниженню ризику штрафів за витік даних і підвищенню продуктивності розробки. Загальна архітектура інформаційних потоків після впровадження ролі та протоколу представлена на *рис. 1*.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Згенеровані в процесі моделювання дані показали чітку кореляцію між зміною організаційної структури та підвищенням ефективності розробки систем машинного навчання. Узагальнені результати по двох етапах наведені в *табл. 2*.

Таблиця 2

Порівняння ключових метрик за етапами моделювання

Метрика	Етап 1 (Baseline)	Етап 2 (з ADC)	Δ , %
Час до отримання даних (Time-to-Data), робочих днів	14,5	4,2	–71,0%
Інциденти безпеки (Breach + Near-miss)	12	2	–83,3%
Частка неструктурованих даних у середовищі ML	22%	5%	–77,3%
Середня точність ML-моделей (F1)	0,74	0,86	+16,2%
Інтегральний показник $f(y)$	3,12	1,04	–66,7%

Джерело: складено авторами.

У базовому періоді середній час погодження та отримання доступу до якісних даних складав 14,5 робочих днів. Через складну бюрократію інженери часто використовували неочищені або слабо анонімізовані дані, що призвело до фіксації 12 інцидентів потенційного витоку інтелектуальної власності в середовища тестування. Відсоток неструктурованих/сміттєвих даних становив 22%.

Після імплементації ролі «AI Data Custodian», який взяв на себе повноваження з оркестрації процесів очищення, маскуванню та надання доступу до синтетичних копій даних:

- ✦ час доступу до підготовлених даних скоротився до 4,2 днів (оптимізація на ~71%);
- ✦ кількість інцидентів безпеки знизилася до 2, оскільки Custodian упровадив автоматичні фільтри на виході з Production баз даних;
- ✦ частка неструктурованих даних впала до 5%, що суттєво підвищило точність роботи створених ML-моделей (середній F1-score зріс із 0,74 до 0,86).

СХЕМА ІНФОРМАЦІЙНИХ ПОТОКІВ: ВПРОВАДЖЕННЯ РОЛІ "AI DATA CUSTODIAN" & ПРОТОКОЛУ "DATA-SEC-AIOPS"

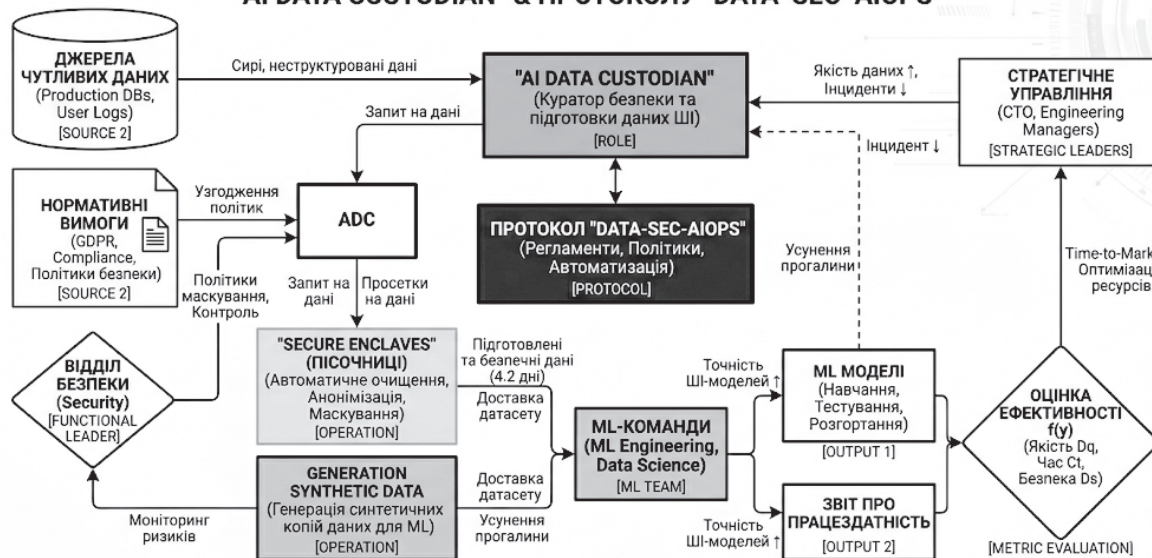


Рис. 1. Графічна модель оптимізованих інформаційних потоків

Примітка: Центральним вузлом є роль AI Data Custodian, яка через протоколи Data-Sec-AIOPS забезпечує паралельну взаємодію з техлідами (CTO) та безпекою (Security), створюючи ізольовані середовища для ML-команд.

Джерело: авторська розробка.

Ключовим спостереженням стало те, що управління через вплив (*Management by Influence*) виявилося ефективнішим за пряме директивне управління. Custodian, не маючи інженерів у прямому підпорядкуванні, створив рамкові умови (*Frameworks*), які функціональні лідери добровільно інтегрували у свої спринти, оскільки це прискорило загальний *Time-to-Market* їхніх продуктів. Цей патерн узгоджується з концепцією «*Servant Leadership*» і принципами LeSS-фреймворку для масштабованого Agile.

Економічний ефект від впровадження ролі AI Data Custodian розраховувався через показник альтернативної вартості (*Opportunity Cost*) і прямої економії фонду оплати праці. Скорочення часу очікування даних з 14,5 до 4,2 днів для команди з 5 ML-інженерів дозволяє вивільнити приблизно 515 людино-годин на рік на один проєкт. При середній ставці фахівця вищого/середнього рівня (*Senior/Middle*) це еквівалентно прямій економії витрат у розмірі 15 000–22 000 дол. США на одну команду щоквартально. Для підприємства з 5 командами річна економія становить орієнтовно 300 000–440 000 дол. США.

Крім того, прискорення доставки рішення (*Time-to-Market*) на 71% дозволяє підприємству раніше розпочати монетизацію ML-сервісу, що в умовах висококонкурентного ринку є критичним чинником випередження конкурентів.

Окремою статтею економії є уникнуті регуляторні штрафи: один потенційний інцидент GDPR-рівня для середнього підприємства з оборотом 50 млн євро може коштувати до 2 млн євро штрафу (4% обороту) [3], тож зниження кількості Near-miss подій із 12 до 2 еквівалентне статистично очікуваному уникненню принаймні одного значного інциденту на рік.

ПРАКТИЧНІ РЕКОМЕНДАЦІЇ ЩОДО ВПРОВАДЖЕННЯ РОЛІ AI DATA CUSTODIAN

На основі результатів моделювання й аналізу референсних впроваджень у європейських і північноамериканських підприємствах сформовано покрокову дорожню карту впровадження ролі AI Data Custodian, орієнтовану на інноваційні підприємства з ML-портфоліо понад 3 продуктові команди.

Фаза 1. Діагностика (1–2 місяці). Проведення аудиту поточного життєвого циклу даних: інвентаризація джерел чутливих даних (Production DBs, User Logs, third-party API), мапування існуючих процесів узгодження доступу, виявлення «тіньових» каналів передачі даних до ML-команд. Інструментарій: data discovery платформи (Microsoft Purview, OneTrust, Collibra).

Фаза 2. Дизайн ролі та процесів (1 місяць). Формалізація посадової інструкції AI Data Custodian, опис матриці відповідальності RACI, інтеграція ролі в існуючу організаційну структуру

(рекомендовано: підпорядкування СТО або СОО з пунктирною лінією до CISO). Розробка протоколу Data-Sec-AIOps як сукупності SLA, політик і автоматизованих перевірок.

Фаза 3. Технологічне забезпечення (2–3 місяці). Розгортання інфраструктури безпечних enclave-середовищ. Референсні платформи: Databricks Unity Catalog, Snowflake Data Clean Rooms, AWS Clean Rooms, Privacera, Immuta. Налаштування інструментів синтетичної генерації даних (Mostly AI, Gretel, Tonic.ai). Інтеграція з SIEM/SOC для моніторингу аномалій доступу.

Фаза 4. Пілот на 1–2 командах (3 місяці). Запуск пілотного впровадження на обмеженому периметрі. Збирання базових метрик (Time-to-Data, кількість інцидентів, NPS ML-команд щодо швидкості доступу до даних). Налагодження циклу безперервного вдосконалення.

Фаза 5. Масштабування (6+ місяців). Поширення моделі на всі ML-команди, формування Center of Excellence для управління даними III, інтеграція з програмою кібербезпекової зрілості за моделями CMMI або NIST CSF 2.0.

Ключовими компетенціями AI Data Custodian є: глибоке розуміння життєвого циклу ML-моделі (від збору даних до моніторингу в продакшені), практичний досвід роботи з регуляторними фреймворками (GDPR, AI Act, HIPAA), сертифікації CIPP/E або CIPM від IAPP, навички крос-функціональної комунікації. Розрахункова заробітна плата для українського ринку – на 15–25% вище за Senior ML Engineer, що відображає унікальність профілю.

KPI, за якими доцільно вимірювати ефективність ролі: 1) Time-to-Data; 2) Mean Time to Detect data anomaly (MTTD); 3) частка ML-моделей, що пройшли формальну приватність-оцінку (Privacy Impact Assessment); 4) індекс задоволеності ML-команд швидкістю надання даних; 5) кількість критичних інцидентів безпеки на рік.

ОБГОВОРЕННЯ

Результати дослідження мають низку обмежень. *По-перше*, моделювання здійснювалось на синтетичній вибірці з п'яти крос-функціональних команд, що відповідає масштабу середнього інноваційного підприємства, але потребує верифікації на даних великих корпорацій (10+ команд) і малих стартапів (1–2 команди). *По-друге*, експертне калібрування коефіцієнтів α і β виконане для умов українського ринку 2025–2026 рр., тому при застосуванні моделі в інших юрисдикціях потрібне повторне калібрування. *По-третє*, дослідження не охоплює специфіку галузей з підвищеними регуля-

торними вимогами (медицина, фінанси, оборона), де роль Custodian може потребувати додаткових повноважень.

Перспективними напрямками подальшої роботи є: емпірична валідація моделі на реальних кейсах українських інноваційних підприємств; розробка специфікації автоматизованої системи підтримки прийняття рішень для AI Data Custodian; інтеграція моделі з вимогами Регламенту (ЄС) 2024/1689 (AI Act).

ВИСНОВКИ

У ході дослідження розроблено та верифіковано організаційно-управлінську модель удосконалення систем управління інноваційними підприємствами, спрямовану на забезпечення конфіденційності даних в умовах активного впровадження машинного навчання. Встановлено, що традиційні організаційні структури створюють вузькі місця, де потреби розробки III конфліктують із вимогами кібербезпеки, а наявні підходи в науковій літературі покривають лише технічний і юридичний виміри, залишаючи поза увагою організаційно-управлінську інтеграцію.

Для вирішення цієї проблеми сформульовано гіпотезу про необхідність виокремлення спеціалізованої управлінської ролі – AI Data Custodian – та супровідного процесного протоколу Data-Sec-AIOps. Імітаційне моделювання процесів розробки на вибірці з п'яти крос-функціональних команд протягом двох піврічних періодів підтвердило висунуту гіпотезу: впровадження ролі привело до скорочення Time-to-Data на 71%, зниження кількості інцидентів безпеки на 83%, зменшення частки неструктурованих даних на 77% і зростання середньої точності ML-моделей на 16%.

Запропонована модель управління дозволяє підприємствам безпечно масштабувати свої інноваційні розробки на базі штучного інтелекту, уникаючи репутаційних і фінансових втрат від недооцінки цінності своїх інформаційних активів. Окрім операційних переваг, дослідження довело стратегічну економічну вигоду: перехід від реактивного блокування даних до проактивного управління через роль Custodian перетворює «безпеку даних» з витратної статті (Cost Center) на фактор прискорення прибутку (Profit Center). Це дозволяє інноваційним підприємствам масштабувати кількість ML-проектів без лінійного зростання штату відділу кібербезпеки, досягаючи ефекту масштабу.

Практичним результатом дослідження є дорожня карта впровадження ролі AI Data Custodian, побудована з п'яти фаз (діагностика – дизайн – технологічне забезпечення – пілот – масштабуван-

ня), а також система із п'яти КРІ для вимірювання її ефективності. Запропонований підхід може бути використаний як методологічна основа для побудови систем data governance на українських інноваційних підприємствах, що інтегруються в європейський регуляторний простір згідно з вимогами GDPR та AI Act. ■

БІБЛІОГРАФІЯ

1. IDC. Worldwide Global DataSphere Forecast, 2024–2028: AI Everywhere, But Upsurge in Data Will Take Time. International Data Corporation, 2024.
2. IBM Security & Ponemon Institute. Cost of a Data Breach Report 2024. Armonk, NY : IBM Corporation, 2024. URL: https://www-api.ibm.com/adobe/assets/urn:aaid:aem:c4711149-da99-4654-9114-8ee524108540/original/as/cost_of_a_data_breach_report_2024.pdf
3. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation). *Official Journal of the European Union*. 2016. L 119. P. 1–88. URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>
4. Mayer-Schönberger V., Cukier K. Big Data: A Revolution That Will Transform How We Live, Work, and Think. Boston : Houghton Mifflin Harcourt, 2013. 256 p.
5. Park K. Samsung bans use of generative AI tools like ChatGPT after April internal data leak. *TechCrunch*. 2 May 2023. URL: <https://techcrunch.com/2023/05/02/samsung-bans-use-of-generative-ai-tools-like-chatgpt-after-april-internal-data-leak/>
6. McMahan H. B., Moore E., Ramage D., et al. Communication-Efficient Learning of Deep Networks from Decentralized Data. *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (AISTATS)*. PMLR, 2017. Vol. 54. P. 1273–1282. URL: <https://proceedings.mlr.press/v54/mcmahan17a/mcmahan17a.pdf>
7. Bonawitz K., Ivanov V., Kreuter B., et al. Practical Secure Aggregation for Privacy-Preserving Machine Learning. *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS)*. 2017. P. 1175–1191. DOI: <https://doi.org/10.1145/3133956.3133982>
8. Dwork C., Roth A. The Algorithmic Foundations of Differential Privacy. *Foundations and Trends in Theoretical Computer Science*. 2014. Vol. 9. Iss. 3–4. P. 211–487. DOI: <https://doi.org/10.1561/04000000042>
9. Abadi M., Chu A., Goodfellow I., McMahan H. B., et al. Deep Learning with Differential Privacy. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS)*. 2016. P. 308–318. DOI: <https://doi.org/10.1145/2976749.2978318>
10. Shokri R., Stronati M., Song C., Shmatikov V. Membership Inference Attacks Against Machine Learning Models. *2017 IEEE Symposium on Security and Privacy (SP)*. 2017. P. 3–18. DOI: <https://doi.org/10.1109/SP.2017.41>
11. Papernot N., McDaniel P., Sinha A., Wellman M. P. SoK: Security and Privacy in Machine Learning. *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*. 2018. P. 399–414. DOI: <https://doi.org/10.1109/EuroSP.2018.00035>
12. Goodfellow I. J., Shlens J., Szegedy C. Explaining and Harnessing Adversarial Examples. *International Conference on Learning Representations (ICLR)*. 2015. DOI: <https://doi.org/10.48550/arXiv.1412.6572>
13. Biggio B., Roli F. Wild patterns: Ten years after the rise of adversarial machine learning. *Pattern Recognition*. 2018. Vol. 84. P. 317–331. DOI: <https://doi.org/10.1016/j.patcog.2018.07.023>
14. Carlini N., Tramèr F., Wallace E., et al. Extracting Training Data from Large Language Models. *30th USENIX Security Symposium*. 2021. P. 2633–2650. DOI: <https://doi.org/10.48550/arXiv.2012.07805>
15. Rose S., Borchert O., Mitchell S., Connolly S. Zero Trust Architecture. *NIST Special Publication 800-207*. Gaithersburg, MD : National Institute of Standards and Technology, 2020. DOI: <https://doi.org/10.6028/NIST.SP.800-207>
16. Hoofnagle C. J., van der Sloot B., Borgesius F. Z. The European Union general data protection regulation: what it is and what it means. *Information & Communications Technology Law*. 2019. Vol. 28. Iss. 1. P. 65–98. DOI: <https://doi.org/10.1080/13600834.2019.1573501>
17. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union*. 12 July 2024. URL: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>
18. Veale M., Borgesius F. Z. Demystifying the Draft EU Artificial Intelligence Act – Analysing the good, the bad, and the unclear elements of the proposed approach. *Computer Law Review International*. 2021. Vol. 22. Iss. 4. P. 97–112. DOI: <https://doi.org/10.9785/cr-2021-220402>
19. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. Geneva : International Organization for Standardization, 2022.
20. ISO/IEC 27701:2019. Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines. Geneva : ISO, 2019.
21. NIST. Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST AI 100-1. Gaithersburg, MD : National Institute of Standards and Technology, 2023. DOI: <https://doi.org/10.6028/NIST.AI.100-1>
22. Закон України «Про захист персональних даних» від 01.06.2010 р. № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>

23. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р. № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>
24. Floridi L., Cows J. A Unified Framework of Five Principles for AI in Society. *Harvard Data Science Review*. 2019. Vol. 1. Iss. 1. DOI: <https://doi.org/10.1162/99608f92.8cd550d1>
25. Brundage M., Avin S., Clark J., Toner H., et al. The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. *arXiv:1802.07228*. 2018. DOI: <https://doi.org/10.48550/arXiv.1802.07228>
26. Davenport T. H., Ronanki R. Artificial Intelligence for the Real World. *Harvard Business Review*. 2018. Vol. 96. Iss. 1. P. 108–116. URL: https://academichelptoday.com/assets/documents/Artificial_Intelligence_for_the_Real_World_-_HBR.pdf
27. O'Neil C. Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. New York : Crown Publishing Group, 2016. 272 p.
28. Zuboff S. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York : PublicAffairs, 2019. 704 p.
29. Wang R. Y., Strong D. M. Beyond Accuracy: What Data Quality Means to Data Consumers. *Journal of Management Information Systems*. 1996. Vol. 12. Iss. 4. P. 5–33. DOI: <https://doi.org/10.1080/07421222.1996.11518099>
30. ISO/IEC 25012:2008. Data Quality Model. Geneva : International Organization for Standardization, 2008. 22 p.
31. Pipino L. L., Lee Y. W., Wang R. Y. Data Quality Assessment. *Communications of the ACM*. 2002. Vol. 45. Iss. 4. P. 211–218. DOI: <https://doi.org/10.1145/505248.506010>
32. Sculley D., Holt G., Golovin D., Davydov E., et al. Hidden Technical Debt in Machine Learning Systems. *NIPS'15: Proceedings of the 29th International Conference on Neural Information Processing Systems*. 2015. Vol. 2. P. 2503–2511. URL: <https://dl.acm.org/doi/10.5555/2969442.2969519>
33. Ereth J. DataOps – Towards a Definition. *Proceedings of the 20th International Conference on Enterprise Information Systems (ICEIS)*. 2018. Vol. 1. P. 267–276. URL: <https://ceur-ws.org/Vol-2191/paper13.pdf>
34. NIST SP 800-30 Rev. 1. Guide for Conducting Risk Assessments. Gaithersburg : National Institute of Standards and Technology, 2012. 95 p. DOI: <https://doi.org/10.6028/NIST.SP.800-30r1>
35. Mell P., Scarfone K., Romanosky S. A Complete Guide to the Common Vulnerability Scoring System Version 2.0. FIRST.org, 2007. 24 p.
36. Saaty T. L. The Analytic Hierarchy Process: Planning, Priority Setting, Resource Allocation. New York : McGraw-Hill, 1980. 287 p.
37. Saaty T. L. Decision Making with the Analytic Hierarchy Process. *International Journal of Services Sciences*. 2008. Vol. 1. No. 1. P. 83–98. DOI: <https://doi.org/10.1504/IJSSCI.2008.017590>
38. Saaty T. L., Vargas L. G. Models, Methods, Concepts & Applications of the Analytic Hierarchy Process. 2nd ed. New York : Springer, 2012. 346 p. DOI: <https://doi.org/10.1007/978-1-4614-3597-6>
39. Patton M. Q. Qualitative Research & Evaluation Methods. 3rd ed. Thousand Oaks : Sage Publications, 2002. 598 p.
40. Forman E., Peniwati K. Aggregating Individual Judgments and Priorities with the Analytic Hierarchy Process. *European Journal of Operational Research*. 1998. Vol. 108. Iss. 1. P. 165–169. DOI: [https://doi.org/10.1016/S0377-2217\(97\)00244-0](https://doi.org/10.1016/S0377-2217(97)00244-0)

REFERENCES

- Abadi M., Chu A., Goodfellow I. & McMahan H. B. (2016). Deep Learning with Differential Privacy. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS)* (p. 308–318). <https://doi.org/10.1145/2976749.2978318>
- Biggio B. & Roli F. (2018). Wild patterns: Ten years after the rise of adversarial machine learning. *Pattern Recognition*, 84, 317–331. <https://doi.org/10.1016/j.patcog.2018.07.023>
- Bonawitz K., Ivanov V. & Kreuter B. (2017). Practical Secure Aggregation for Privacy-Preserving Machine Learning. *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS)* (p. 1175–1191). <https://doi.org/10.1145/3133956.3133982>
- Brundage M., Avin S., Clark J. & Toner H. (2018). The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. *arXiv:1802.07228*. <https://doi.org/10.48550/arXiv.1802.07228>
- Carlini N., Tramèr F. & Wallace E. (2021). Extracting Training Data from Large Language Models. *30th USENIX Security Symposium* (p. 2633–2650). <https://doi.org/10.48550/arXiv.2012.07805>
- Davenport T. H. & Ronanki R. (2018). Artificial Intelligence for the Real World. *Harvard Business Review*, 1(96), 108–116. https://academichelptoday.com/assets/documents/Artificial_Intelligence_for_the_Real_World_-_HBR.pdf
- Dwork C. & Roth A. (2014). The Algorithmic Foundations of Differential Privacy. *Foundations and Trends in Theoretical Computer Science*, 3–4(9), 211–487. <https://doi.org/10.1561/04000000042>
- Ereth J. (2018). DataOps – Towards a Definition. *Proceedings of the 20th International Conference on Enterprise Information Systems (ICEIS)* (p. 267–276). <https://ceur-ws.org/Vol-2191/paper13.pdf>
- Floridi L. & Cows J. (2019). A Unified Framework of Five Principles for AI in Society. *Harvard Data Science Review*, 1(1). <https://doi.org/10.1162/99608f92.8cd550d1>
- Forman E. & Peniwati K. (1998). Aggregating Individual Judgments and Priorities with the Analytic Hierarchy

- Process. *European Journal of Operational Research*, 1(108), 165–169.
[https://doi.org/10.1016/S0377-2217\(97\)00244-0](https://doi.org/10.1016/S0377-2217(97)00244-0)
- Goodfellow I. J., Shlens J. & Szegedy C. (2015). Explaining and Harnessing Adversarial Examples. *International Conference on Learning Representations (ICLR)*.
<https://doi.org/10.48550/arXiv.1412.6572>
- Hoofnagle C. J., van der Sloot B. & Borgesius F. Z. (2019). The European Union general data protection regulation: what it is and what it means. *Information & Communications Technology Law*, 1(28), 65–98.
<https://doi.org/10.1080/13600834.2019.1573501>
- IBM Security & Ponemon Institute. (2024). *Cost of a Data Breach Report 2024*. Armonk, NY: IBM Corporation. https://www-api.ibm.com/adobe/assets/urn:aaid:aem:c4711149-da99-4654-9114-8ee524108540/original/as/cost_of_a_data_breach_report_2024.pdf
- IDC (2024). *Worldwide Global DataSphere Forecast, 2024–2028: AI Everywhere, But Upsurge in Data Will Take Time*. International Data Corporation.
- International Organization for Standardization (2008). *ISO/IEC 25012:2008. Data Quality Model*. Geneva: International Organization for Standardization.
- International Organization for Standardization (2022). *ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements*. Geneva: International Organization for Standardization.
- ISO (2019). *ISO/IEC 27701:2019. Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines*. Geneva: ISO.
- Mayer-Schönberger V. & Cukier K. (2013). *Big Data: A Revolution That Will Transform How We Live, Work, and Think*. Boston: Houghton Mifflin Harcourt.
- McMahan H. B., Moore E. & Ramage D. (2017). Communication-Efficient Learning of Deep Networks from Decentralized Data. *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (AISTATS)* (p. 1273–1282). PMLR. <https://proceedings.mlr.press/v54/mcmahan17a/mcmahan17a.pdf>
- Mell P., Scarfone K. & Romanosky S. (2007). *A Complete Guide to the Common Vulnerability Scoring System Version 2.0*. FIRST.org.
- National Institute of Standards and Technology (2012). *NIST SP 800-30 Rev. 1. Guide for Conducting Risk Assessments*. Gaithersburg: National Institute of Standards and Technology.
<https://doi.org/10.6028/NIST.SP.800-30r1>
- NIST (2023). *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*. Gaithersburg, MD: National Institute of Standards and Technology.
<https://doi.org/10.6028/NIST.AI.100-1>
- Official Journal of the European Union. (2024, July 12). *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>
- Official Journal of the European Union. (2016, April 27). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation)*. <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>
- O’Neil C. (2016). *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. New York: Crown Publishing Group.
- Papernot N., McDaniel P., Sinha A. & Wellman M. P. (2018). SoK: Security and Privacy in Machine Learning. 2018 *IEEE European Symposium on Security and Privacy (EuroS&P)* (p. 399–414).
<https://doi.org/10.1109/EuroSP.2018.00035>
- Park K. (2023, May 2). *Samsung bans use of generative AI tools like ChatGPT after April internal data leak*. TechCrunch. <https://techcrunch.com/2023/05/02/samsung-bans-use-of-generative-ai-tools-like-chatgpt-after-april-internal-data-leak/>
- Patton M. Q. (2002). *Qualitative Research & Evaluation Methods*. Thousand Oaks: Sage Publications.
- Pipino L. L., Lee Y. W. & Wang R. Y. (2002). Data Quality Assessment. *Communications of the ACM*, 4(45), 211–218.
<https://doi.org/10.1145/505248.506010>
- Rose S., Borchert O., Mitchell S. & Connelly S. (2020). *Zero Trust Architecture*. Gaithersburg, MD: National Institute of Standards and Technology.
<https://doi.org/10.6028/NIST.SP.800-207>
- Saaty T. L. (1980). *The Analytic Hierarchy Process: Planning, Priority Setting, Resource Allocation*. New York: McGraw-Hill.
- Saaty T. L. (2008). Decision Making with the Analytic Hierarchy Process. *International Journal of Services Sciences*, 1(1), 83–98.
<https://doi.org/10.1504/IJSSCI.2008.017590>
- Saaty T. L. & Vargas L. G. (2012). *Models, Methods, Concepts & Applications of the Analytic Hierarchy Process*. New York: Springer.
<https://doi.org/10.1007/978-1-4614-3597-6>
- Sculley D., Holt G., Golovin D. & Davydov E. (2015). Hidden Technical Debt in Machine Learning Systems. *NIPS’15: Proceedings of the 29th International Conference on Neural Information Processing Systems* (p. 2503–2511). <https://dl.acm.org/doi/10.5555/2969442.2969519>
- Shokri R., Stronati M., Song C. & Shmatikov V. (2017). Membership Inference Attacks Against Machine Learning Models. 2017 *IEEE Symposium on Security and Privacy (SP)* (p. 3–18).
<https://doi.org/10.1109/SP.2017.41>
- Veale M. & Borgesius F. Z. (2021). Demystifying the Draft EU Artificial Intelligence Act – Analysing the good, the bad, and the unclear elements of the proposed approach. *Computer Law Review International*, 4(22), 97–112.
<https://doi.org/10.9785/cr-2021-220402>

- Wang R. Y. & Strong D. M. (1996). Beyond Accuracy: What Data Quality Means to Data Consumers. *Journal of Management Information Systems*, 4(12), 5–33. <https://doi.org/10.1080/07421222.1996.11518099>
- zakon.rada.gov.ua. (2010, June 1). Zakon Ukrainy «Pro zakhyst personalnykh danykh» [Law of Ukraine "On Personal Data Protection"]. <https://zakon.rada.gov.ua/laws/show/2297-17#Text>
- zakon.rada.gov.ua. (2017, October 5). Zakon Ukrainy «Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy» [Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine"]. <https://zakon.rada.gov.ua/laws/show/2163-19#Text>
- Zuboff S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs.

Дослідження не отримувало зовнішнього фінансування. Автори заявляють про відсутність конфлікту інтересів. Під час підготовки рукопису автори використовували інструмент генеративного штучного інтелекту Google Gemini для пошуку наукових статей і джерел за темою дослідження. Усі знайдені джерела автори самостійно перевірили, проаналізували та опрацювали. Інструмент ШІ не використовувався для генерації наукових результатів, висновків чи тексту статті. Відповідальність за зміст рукопису повністю несуть автори.

Стаття надійшла до редакції / Received: 07.07.2026
Статтю прийнято до публікації / Accepted: 20.07.2026
Оприлюднено / Published: 20.08.2026

УДК 005.95/.96:331.5
JEL: J81; M12; M54
DOI: <https://doi.org/10.32983/2222-4459-2026-7-562-574>

ГНУЧКІ ФОРМИ ОРГАНІЗАЦІЇ ПРАЦІ В ІТ-СЕКТОРІ УКРАЇНИ ПІД БЕЗПЕКОВИМ ШОКОМ: ДЕВІАНТНИЙ ВИПАДОК І НАСЛІДКИ ДЛЯ МЕНЕДЖМЕНТУ ПЕРСОНАЛУ

©2026 БОНДАР В. Ю.

УДК 005.95/.96:331.5
JEL: J81; M12; M54

Бондар В. Ю. Гнучкі форми організації праці в ІТ-секторі України під безпековим шоком: девіантний випадок і наслідки для менеджменту персоналу

Актуальність дослідження зумовлена практичною прогалиною: управлінські рецепти, вибудовані навколо світової гібридної рівноваги гнучких форм організації праці, зокрема політики повернення до офісу, спираються на передумови, що не виконуються в українському ІТ-секторі, тоді як систематичного опису того, чим слід керуватися натомість, наукова література не пропонує. Мета статті – розкрити механізм відхилення траєкторії гнучких форм організації праці в ІТ-секторі України від глобальної моделі їх поширення під впливом послідовних шоків різної природи та обґрунтувати наслідки цього відхилення для системи менеджменту персоналу. Дослідження виконано за логікою аналізу девіантного випадку із застосуванням чотирьох методів: порівняльного аналізу траєкторій на відкритих вторинних рядах для України та основних груп країн; критеріального фазового зіставлення рядів, вимірюваних у різних одиницях; типологічного порівняння санітарного та безпекового шоків; матричної перевірки апіорної моделі диференційованої чутливості підсистем менеджменту персоналу. Установлено, що українська траєкторія відрізняється від світової не параметрами, а типом: замість послідовності «стрибок – корекція – плато» сектор демонструє послідовність «стрибок – закріплення – поглиблення», а момент розходження збігається з безпековим шоком 2022 року. Механізм закріплення концептуалізовано як подвійний хрестовик, у якому безпековий шок усуває стабільну точку повернення та зрощує дистанційність із релокацією персоналу. Показано функціональну мутацію гнучкості: до оптимізаційної функції надбудовуються функції безперервності бізнесу та фізичної безпеки персоналу, що підтверджує квазіекспериментальне зіставлення підгруп фахівців за кордоном. Наукова новизна полягає в обґрунтуванні того, що зона чутливості підсистеми менеджменту персоналу є функцією від профілю шоку, а не сталою її властивістю. Практична цінність результатів – у трактуванні гнучкості як інфраструктурної властивості операційної стійкості та в діагностиці профілю шоку як відправної точки пріоритетизації управлінських зусиль.

Ключові слова: менеджмент персоналу; гнучкі форми організації праці; підсистеми менеджменту персоналу; дистанційна робота; трансформація системи менеджменту персоналу; HR-процеси; компанії ІТ-сфери.

Табл.: 4. Бібл.: 23.

Бондар Володимир Юрійович – аспірант, Міжрегіональна Академія управління персоналом (вул. Фрометівська, 2, Київ, 03039, Україна)
E-mail: volod.bon@gmail.com
ORCID: <https://orcid.org/0009-0006-2057-8194>

UDC 005.95/.96:331.5
JEL: J81; M12; M54

Bondar V. Yu. Flexible Work Arrangements in the Ukrainian IT Sector under the Security Shock:

A Deviant Case and Its Implications for Staff Management

The relevance of the study is driven by a practical gap: managerial prescriptions built around the global hybrid equilibrium, including return-to-office policies, rest on premises that do not hold in Ukraine, while the literature offers no systematic account of what should guide Ukrainian HR systems instead. The aim of