

Ю. В. Огерчук,
к. е. н., доцент, доцент кафедри зовнішньоекономічної та митної діяльності,
Національний університет "Львівська політехніка"
ORCID ID: <https://orcid.org/0000-0002-8924-9130>
В. О. Клепец,
аспірант кафедри зовнішньоекономічної та митної діяльності,
Національний університет "Львівська політехніка"
ORCID ID: <https://orcid.org/0009-0007-7132-3367>
Р. І. Лебедь,
аспірант кафедри зовнішньоекономічної та митної діяльності,
Національний університет "Львівська політехніка"
ORCID ID: <https://orcid.org/0009-0005-9867-4111>

DOI: 10.32702/2306-6814.2026.7.318

БІОМЕТРИЗАЦІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ ЯК НОВИЙ ІНСТРУМЕНТ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Y. Oherchuk,
PhD in Economics, Associate Professor, Associate Professor of the Department
of Foreign Trade and Customs, Lviv Polytechnic National University
V. Klepets,
Postgraduate student, Lviv Polytechnic National University
R. Lebed,
Postgraduate student, Lviv Polytechnic National University

BIOMETRISATION OF PERSONNEL MANAGEMENT AS A NEW TOOL FOR ECONOMIC SECURITY OF AN ENTERPRISE

У статті досліджено біометризацію управління персоналом як сучасний інструмент підвищення економічної безпеки підприємства. Розкрито теоретичні підходи до трактування економічної безпеки підприємства та визначено роль кадрової складової у системі її забезпечення. Проаналізовано сутність біометричних технологій і напрями їх використання в HR-менеджменті, зокрема у системах обліку робочого часу, контролю доступу до матеріальних і цифрових ресурсів та автентифікації працівників у корпоративних інформаційних системах. Визначено економічні та управлінські переваги впровадження біометричних технологій, а також соціально-етичні, правові та інформаційні ризики їх використання. Обґрунтовано вплив біометризації на зниження кадрових і інформаційних загроз та підвищення прозорості управлінських процесів. Запропоновано матрицю ризиків використання біометричних HR-систем.

Introduction. The rapid digitalization of management processes and the growing need for reliable mechanisms of workforce control have intensified the interest of enterprises in biometric technologies as tools for strengthening economic security and improving personnel management. Biometric identification systems, based on unique physiological characteristics such as fingerprints or facial recognition, are increasingly used in attendance monitoring and workforce management. Their implementation allows organizations to enhance transparency in administrative procedures, reduce the risks of timekeeping manipulation, and improve the efficiency of labor resource utilization. At the same time, the use of biometric technologies raises important issues related to the protection of personal data, information security, and ethical aspects of employee monitoring.

Purpose. The purpose of the study is to determine the role of biometric technologies in strengthening the personnel component of enterprise economic security and to assess their potential for improving the efficiency of human resource management systems in modern organizations.

Results. The study demonstrates that the integration of biometric identification systems into enterprise management practices contributes to more accurate recording of employees' working time and reduces the possibility of unauthorized access or manipulation of attendance systems. Biometric technologies enhance workforce accountability, streamline HR administrative functions, and support more effective monitoring of labor discipline. At the same time, the analysis shows that the use of biometric data introduces additional

challenges associated with data protection, privacy risks, and compliance with international standards of information security and personal data protection. Effective application of biometric systems therefore requires the integration of technical, organizational, and legal mechanisms aimed at ensuring secure processing and storage of biometric information.

Conclusions. *The obtained results confirm that biometric technologies can serve as an effective instrument for strengthening the personnel component of enterprise economic security and improving the efficiency of personnel management processes. At the same time, the sustainable use of such technologies requires the development of comprehensive data protection mechanisms and adherence to international standards of information security, which ensures a balance between managerial efficiency and the protection of employees' rights in the digital environment.*

Ключові слова: кадрові ризики; HR-технології; контроль доступу; цифрова автентифікація; управління ризиками.

Key words: personnel risks; HR technologies; access control; digital authentication; risk management.

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

У сучасних умовах цифровізації економіки питання забезпечення економічної безпеки підприємств набуває особливої актуальності. Значна частина внутрішніх ризиків діяльності підприємства пов'язана з людським фактором, що проявляється у вигляді помилок персоналу, недобросовісних дій, маніпуляцій із даними обліку робочого часу або несанкціонованого доступу до інформаційних ресурсів. У зв'язку з цим зростає потреба у впровадженні сучасних інструментів управління персоналом, які дають змогу підвищити прозорість кадрових процесів та зменшити вплив людського фактору на систему економічної безпеки підприємства.

Одним із таких інструментів є біометричні технології, що забезпечують автоматизовану ідентифікацію працівників на основі їхніх унікальних фізіологічних або поведінкових характеристик. Використання біометрії у системах обліку робочого часу, контролю доступу та цифрової автентифікації дозволяє мінімізувати можливості зловживань, підвищити достовірність управлінської інформації та посилити контроль за використанням ресурсів підприємства. Разом з тим, впровадження біометричних технологій супроводжується низкою правових, соціальних, технологічних та інформаційних ризиків, пов'язаних із захистом персональних даних, довірою працівників та кібербезпекою.

У науковій літературі питання економічної безпеки підприємства та кадрової безпеки досліджувалися багатьма вітчизняними і зарубіжними науковцями, однак проблема системного використання біометричних технологій як інструменту підвищення економічної безпеки підприємства та оцінювання пов'язаних із ними ризиків залишається недостатньо розробленою. Це актуалізує необхідність комплексного аналізу можливостей і загроз біометризації управління персоналом та розроблення аналітичних інструментів оцінювання ризиків її впровадження.

МЕТОЮ СТАТТІ

Метою статті є дослідження ролі біометричних технологій у системі управління персоналом підприємства як інструменту забезпечення економічної безпеки, а також обґрунтування переваг і ризиків їх використання.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

У науковій літературі поняття економічної безпеки підприємства має довгу еволюцію та використовується у вигляді широкого спектра підходів. Так, економічна безпека розглядається як стан захищеності підприємства від впливу зовнішніх і внутрішніх загроз, що забезпечує стабільність його діяльності, фінансову стійкість і потенціал розвитку. Сучасні дослідники підкреслюють, що економічна безпека — це не лише відсутність загроз, а комплекс інтегрованих заходів, спрямованих на їх своєчасне виявлення, нейтралізацію та адаптацію до змін середовища діяльності підприємства [4].

Попри те, що економічна безпека, перш за все, розглядається як стан захищеності від загроз, її трактують також як ефективне використання ресурсів підприємства для підтримки стабільної діяльності. Часто це поняття розглядається і як здатність зберігати конкурентні переваги в умовах ринкової невизначеності [4]. Тобто економічна безпека підприємства є комплексною категорією, що включає економічні, організаційні й управлінські аспекти, а її трактування формується під впливом змін зовнішнього середовища та тенденцій глобальної економіки [17].

Однією з ключових складових економічної безпеки підприємства є кадрова безпека — економічно-управлінський механізм, що забезпечує захищеність підприємства від ризиків, пов'язаних із персоналом. Кадрова складова охоплює питання відбору, мотивації, кваліфікації, адаптації та утримання працівників, а також систему запобігання кадровим загрозам, які можуть мати економічні наслідки для підприємства [2].

Як зазначає Аблязова Н., кадрова безпека — це система управлінських заходів, що гарантує відповідність людського капіталу підприємства стратегічним цілям і мінімізує негативний вплив недоліків в управлінні персоналом на економічну стабільність підприємства [1]. Таким чином, кадрова безпека виступає фундаментальною внутрішньою складовою економічної безпеки, оскільки ефективне управління персоналом дає змогу знизити ризики, пов'язані з некомпетентністю, плинністю кадрів, конфліктами та іншими небажаними явищами [2].

Внутрішні загрози підприємства не менш вагомі, ніж зовнішні, оскільки численні ризики формуються саме



Рис. 1. Напрями використання біометрії в управлінських процесах

Джерело: сформовано авторами на основі [9, 14].

всередині організаційної структури та пов'язані з людським фактором, управлінськими рішеннями та експлуатацією власних ресурсів. Серед таких загроз окремої уваги потребують ризики неефективного управління персоналом (недолік кваліфікації, неадекватна мотивація), корупційні практики і шахрайство, внутрішні фінансові зловживання, помилки в організації виробничих і економічних процесів тощо. Внутрішні загрози часто є домінуючими джерелами економічних ризиків, оскільки саме через них підприємство може зазнати відчутних фінансових і репутаційних втрат. При цьому сучасні підходи до економічної безпеки передбачають не лише ідентифікацію таких загроз, а й розробку превентивних механізмів управління ними, що включає вдосконалення внутрішніх процедур, систем мотивації та контролю [3].

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

У науково-нормативному підході біометричні технології визначаються як методи автоматизованого розпізнавання особи на основі унікальних фізіологічних та поведінкових характеристик людини. Таке визначення закріплене, зокрема, у міжнародних стандартах ISO/IEC, де біометрія розглядається як складова інформаційних та управлінських систем безпеки [11].

За змістом застосування у HR-системах виділяють такі основні види біометричних технологій [8]:

- фізіологічні (відбитки пальців, розпізнавання обличчя, райдужної оболонки ока);
- поведінкові (динаміка натискання клавіш, манера користування пристроями);
- мультимодальні, що поєднують декілька біометричних ознак з метою підвищення надійності ідентифікації.

Систематизація напрямів використання біометрії в управлінських процесах дає змогу представити їх у вигляді логіко-структурної схеми, що відображає взаємозв'язок між HR-функціями та системою економічної без-

пеки (Рис. 1). Як видно з Рис. 1, біометричні технології інтегруються в управлінські процеси підприємства комплексно, охоплюючи облік робочого часу, контроль доступу та цифрову автентифікацію, що сприяє підвищенню прозорості управління й зміцненню економічної безпеки.

Порівняльний аналіз характеристик традиційного управління персоналом та управління із використанням біометрії дозволяє виявити їх принципові відмінності. Як видно з Табл. 1, управління персоналом із використанням біометрії забезпечує вищий рівень ідентифікаційної надійності та прозорості управлінських процесів порівняно з традиційними інструментами. Це зумовлює зниження внутрішніх ризиків та підвищення контрольованості кадрових процедур.

Отже, біометричні технології у HR сфері — це не просто засоби автоматизації обліку чи контролю доступу, а інструменти управлінського впливу, які безпосередньо інтегруються в інформаційні та кадрові системи підприємства. Через біометричну ідентифікацію забезпечується унікальна та незмінна прив'язка конкретного працівника до ключових дій і операцій, що унеможливує маніпуляцію персональними даними та спотворення управлінської інформації. Саме це створює основу для формування надійної системи внутрішнього контролю, яка є частиною загальної моделі економічної безпеки підприємства, де послідовно оцінюються ризики, автоматизуються процеси і навіть підвищується відповідальність працівників за свої дії [16].

У межах зазначеного механізму біометричні рішення виконують дві ключові управлінські функції:

- запобігання помилкам та шахрайству, пов'язаному з людським фактором;
- формування достовірних даних для прийняття управлінських рішень щодо ризиків, продуктивності та кадрової політики загалом. Такі дані стають основою для вчасного виявлення відхилень від нормальних бізнес процесів, що суттєво зміцнює позицію підприємства в контексті економічної безпеки.

Біометричні системи прямо впливають на три групи ризиків, що найчастіше вважаються критичними для еко-

Таблиця 1. Відмінності традиційного та біометризованого управління персоналом

Критерій	Традиційне управління	Біометризоване управління
Спосіб ідентифікації	Паролі, бейджі, табелі	Біометричні шаблони (відбиток, обличчя тощо)
Рівень передаваності ідентифікатора	Передавані (можлива підміна)	Непередавані, унікальні
Вразливість до зловживань	Висока	Низька
Людський фактор	Значний	Мінімізований
Рівень прозорості	Обмежений	Високий
Інтеграція з системою безпеки	Часткова	Комплексна (HR + інформаційна безпека + економічна безпека)

Джерело: сформовано авторами на основі [8, 11, 14].

номічної безпеки підприємства. По-перше, біометрія зменшує обман у системах обліку робочого часу (наприклад, "підміна відміток"), що призводить до більш точних розрахунків заробітної плати, зменшення переплат та зловживань. Такий ефект підтверджується емпіричними дослідженнями, де біометричні системи суттєво знижували випадки несанкціонованого виходу та відсутності на робочому місці, що позитивно впливало на продуктивність і зменшувало непрямі витрати підприємства.

По-друге, завдяки унікальній фізіологічній ідентифікації дані про дії працівників стають захищеними від спотворень, що знижує ризики несанкціонованого доступу до критичної інформації чи систем. Така ідентифікація є більш захищеним методом порівняно з традиційними паролями чи картками, які легко копіюються або втрачаються.

Отже, одним із ключових наслідків впровадження біометричних технологій є підвищення прозорості управлінських процесів, так як біометричні системи забезпечують фіксацію подій у реальному часі, що усуває ручні втручання та людські похибки. Управлінські рішення, побудовані на таких даних, є об'єктивніші і менш схильні до спотворення [16].

Ще однією, не менш важливою, перевагою є можливість аналітичної обробки відповідних масивів даних з біометричних систем: наприклад, виявлення закономірностей у відвідуваності, продуктивності чи ризиковій поведінці працівників. Це дає змогу менеджерам приймати рішення на основі доказових даних, а не інтуїції чи неповної інформації.

Окрім вище перелічених переваг, дані біометричних систем підсилюють відповідальність лінійних менеджерів перед вищим керівництвом, оскільки будь-яка маніпуля-

ція або невідповідність може бути легко виявлена через автоматизовані звіти. Загалом, управлінська прозорість зменшує інформаційні асиметрії, підвищує довіру між рівнями персоналу і керівництвом підприємства, а також зміцнює загальну систему внутрішнього контролю, що є невід'ємною частиною економічної безпеки. Таким чином, ефективність біометризації управління персоналом залежить від збалансованого поєднання технологічних можливостей із дотриманням принципів захисту персональних даних, етичних стандартів та прозорої управлінської політики підприємства (див. Рис. 2).

Інтеграція біометричних технологій у систему управління персоналом повинна здійснюватися не як ізольований IT-проект, а як невід'ємна складова комплексної системи економічної та інформаційної безпеки підприємства. Відповідно до вимог міжнародних стандартів управління інформаційною безпекою, впровадження таких рішень має базуватися на принципах системності, ризик-орієнтованості та пропорційності. Відтак, згідно із Міжнародним стандартом системи управління інформаційною безпекою (ISO/IEC 27001:2022), будь-які технологічні засоби контролю доступу повинні впроваджуватися після оцінювання ризиків, визначення загроз і встановлення відповідних контрольних заходів [11].

Не менш важливим є принцип мінімізації даних, закріплений у відповідному Регламенті Європейського Парламенту та Ради ЄС від 27.04.2016 (ст. 5 і 9), згідно з яким обробка біометричних даних допускається лише в обсязі, необхідному для досягнення конкретної мети. Це формує баланс між ефективністю контролю та захистом прав працівників [13].

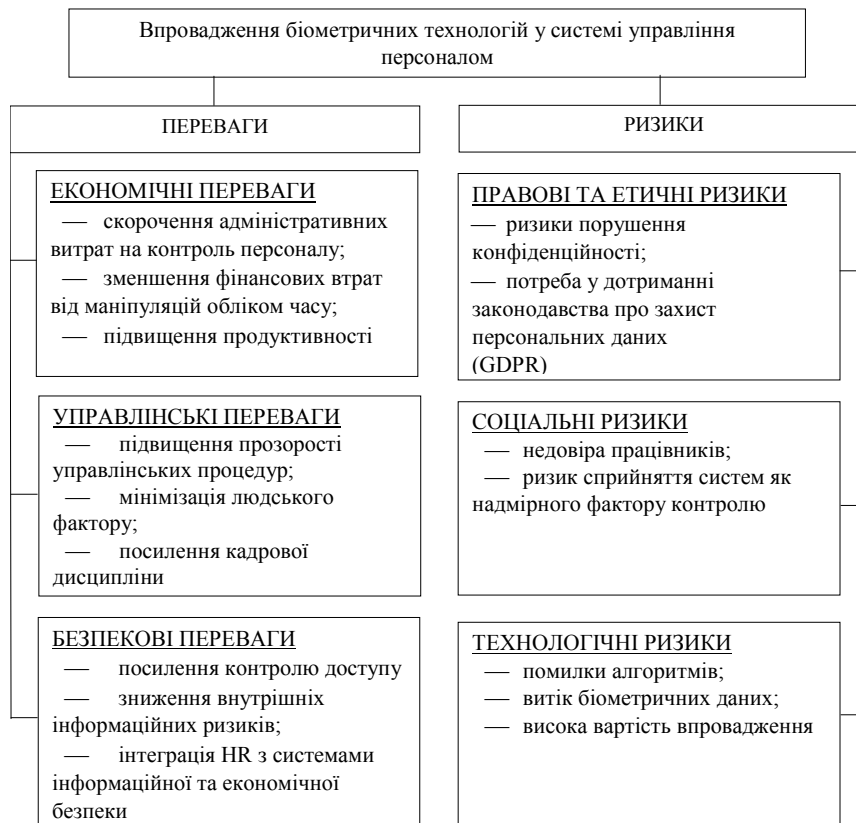


Рис. 2. Переваги та ризики впровадження біометричних технологій у системі управління персоналом

Джерело: сформовано авторами на основі [5, 6, 8, 15].

Y, ймовірність високий середній низький	необхідність періодичного оновлення ПЗ; дрібні технічні збоїв	опір персоналу; недовіра до технології	кібератаки на системи автентифікації
	тимчасові труднощі адаптації персоналу до нових технологій; додаткові витрати	технічні помилки ідентифікації; висока вартість впровадження	порушення законодавства щодо захисту персональних даних
	моральне старіння обладнання	технологічна залежність від постачальників	витік біометричних даних; юридичні ризики
	низький	середній	високий

X, вплив

Рис. 3. Матриця ризиків використання біометричних HR-систем

Узагальнення теоретичних підходів до оцінювання ризиків біометричних систем та аналіз сучасних практик їх використання в управлінні персоналом дали змогу сформувати матрицю ризиків біометризації HR-процесів (див. Рис. 3). Запропонована матриця систематизує потенційні загрози впровадження біометричних технологій за рівнем ймовірності їх виникнення та масштабом можливих наслідків для діяльності підприємства. Доцільність використання такого аналітичного інструменту зумовлена тим, що біометризація управління персоналом, поряд із значними управлінськими та економічними перевагами, пов'язана з низкою технічних, інформаційних, правових та соціальних ризиків. Їх своєчасна ідентифікація та оцінювання є необхідною передумовою інтеграції біометричних технологій у систему економічної безпеки підприємства.

Побудована матриця дозволяє не лише виявити ключові ризики використання біометричних систем у HR-управлінні, але й визначити пріоритетні напрями їх мінімізації. Вона може застосовуватися як інструмент підтримки управлінських рішень під час планування впровадження біометричних технологій, а також як складова системи ризик-менеджменту підприємства.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Впровадження біометричних технологій у систему управління персоналом формує нові можливості для підвищення рівня економічної безпеки підприємства, зокрема у сфері контролю трудової дисципліни, обліку робочого часу та запобігання внутрішнім порушенням. Використання біометричної ідентифікації забезпечує більш високий рівень достовірності даних про присутність працівників, мінімізує ризики маніпулювання системами обліку робочого часу та сприяє підвищенню прозорості управлінських процесів.

Інтеграція біометричних систем у кадрову політику підприємства створює додаткові механізми зміцнення кадрової складової економічної безпеки та підвищує ефективність адміністративних процедур управління персоналом. Водночас використання таких технологій супроводжується новими викликами, пов'язаними із захистом персональних даних, забезпеченням інформаційної безпеки та дотриманням етичних стандартів використання біометричної інформації.

Таким чином, ефективне використання біометричних систем можливе за умови формування комплексного механізму управління, який поєднує технічні, організаційні та правові інструменти захисту даних відповідно до міжнародних стандартів інформаційної безпеки та нормативних вимог щодо захисту персональної інформації. Реалізація такого підходу сприяє підвищенню рівня довіри працівників до цифрових систем управління та забезпечує баланс між ефективністю контролю трудових процесів і дотриманням прав людини у сфері обробки персональних даних.

Отримані результати підтверджують доцільність використання біометричних технологій як одного з інструментів зміцнення економічної безпеки підприємства та підвищення ефективності управління персоналом у умовах цифровізації управлінських процесів.

Література:

- Аблязова Н. Кадрова безпека в системі управління підприємством. Економіка та суспільство. 2020. № 22. DOI: <https://doi.org/10.32782/2524-0072/2020-22-64>
- Насруллаєв Р. С., Зелень В. В. Організаційно-кадровий механізм економічної безпеки підприємства. Актуальні проблеми інноваційної економіки та права. 2024. № 18. С. 93—97. DOI: <https://doi.org/10.36887/2524-0455-2024-5-18>
- Шмалій Л. В., Ількевич М. В. Управління економічною безпекою підприємства. Економіка, менеджмент, бізнес. 2020. № 4. С. 68—73. URL: <https://journals.dut.edu.ua/index.php/emb/article/view/2520/2421>
- Шуміло О., Калініченко Л., Шип К. Аналіз визначень поняття "економічна безпека підприємства". Економіка і управління: зб. наук. пр. ДУІТ. 2019. Вип. 46. С. 126—134. URL: <https://em.dut.in.ua/index.php/home/article/view/105/101>
- Ajunwa I., Crawford K., Schultz J. Limitless worker surveillance. California Law Review. 2017. Vol. 105, No. 3. P. 735—776. DOI: <https://doi.org/10.15779/Z38BR8MF94>
- Ball K. Workplace surveillance: An overview. Labor History. 2010. Vol. 51, No. 1. P. 87—106. DOI: <https://doi.org/10.1080/00236561003654776>
- Carpenter D., McLeod A., Hicks C., Maasberg M. Privacy and biometrics: An empirical examination of employee concerns. Information Systems Frontiers. 2018. Vol. 20. P. 91—110. DOI: <https://doi.org/10.1007/s10796-016-9667-5>

8. Digital Identity Guidelines (NIST SP 800-63-3). Gaithersburg: National Institute of Standards and Technology, 2017. URL: <https://pages.nist.gov/800-63-3/>

9. Gartner. Market Guide for Workforce Management Applications. Stamford: Gartner Inc. URL: <https://www.gartner.com/en/documents/4005184>

10. ISO/IEC 2382-37:2022. Information technology — Vocabulary — Part 37: Biometrics. Geneva: International Organization for Standardization, 2022. URL: <https://www.iso.org/obp/ui/#iso:std:iso-iec:2382-37:ed-1:v1:en>

11. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Geneva: International Organization for Standardization, 2022. URL: <https://www.iso.org/standard/82875.html>

12. Nurhuda A., Safitri N. The use of biometrics in public services and the risk of privacy violations. *Jurnal Hukum Siber dan Regulasi Teknologi*. 2026. Vol. 1, No. 1. P. 46—55. URL: <https://journal.sah.co.id/index.php/JHSRT/article/view/12>

13. 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 and on the free movement of such 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>

14. Security and Privacy Controls for Information Systems and Organizations (NIST SP 800-53 Rev. 5). Gaithersburg: National Institute of Standards and Technology, 2020. URL: <https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final>

15. The Global Risks Report 2024. Geneva: World Economic Forum, 2024. URL: <https://www.weforum.org/reports/global-risks-report-2024>

16. Ussher-Eke D., Okoh O. F., Ijiga O. M. The role of biometric and IoT-based attendance systems in streamlining HR administrative functions, enhancing workforce accountability, and reducing labor inefficiencies. *International Journal for Multidisciplinary Research*. 2025. Vol. 7, No. 4. URL: <https://www.ijfmr.com/papers/2025/4/52237.pdf>

17. Zahorodnia A. Essence and evolution of the concept "economic security of the enterprise". *Ukrainian Journal of Applied Economics and Technology*. 2022. № 3. DOI: <https://doi.org/10.36887/2415-8453-2022-3-2>

References:

1. Ablyazova, N. (2020), "Personnel security in the enterprise management system", *Ekonomika ta suspilstvo*, vol. 22 <https://doi.org/10.32782/2524-0072/2020-22-64>.

2. Nasrullaiev, R. S. and Zeleniak, V. V. (2024), "Organizational and personnel mechanism of economic security of the enterprise", *Aktualni problemy innovatsiinoi ekonomiky ta prava*, vol. 18, pp. 93—97 <https://doi.org/10.36887/2524-0455-2024-5-18>.

3. Shmalii, L. V. and Ilkevych, M. V. (2020), "Management of economic security of the enterprise", *Ekonomika, menedzhment, biznes*, vol. 4, pp. 68—73, Available at: <https://journals.dut.edu.ua/index.php/emb/article/view/2520/2421> (Accessed 19 Mar 2026).

4. Shumylo, O., Kalinichenko, L. and Shyp, K. (2019), "Analysis of definitions of the concept of 'economic security of the enterprise'", *Ekonomika i upravlinnia: zbirnyk naukovykh*

prats DUIT, vol. 46, pp. 126—134, Available at: <https://em.duit.in.ua/index.php/home/article/view/105/101> (Accessed 19 Mar 2026).

5. Ajunwa, I., Crawford, K. and Schultz, J. (2017), "Limitless worker surveillance", *California Law Review*, vol. 105, no. 3, pp. 735—776 <https://doi.org/10.15779/Z38BR8MF94>.

6. Ball, K. (2010), "Workplace surveillance: An overview", *Labor History*, vol. 51, no. 1, pp. 87—106 <https://doi.org/10.1080/00236561003654776>.

7. Carpenter, D., McLeod, A., Hicks, C. and Maasberg, M. (2018), "Privacy and biometrics: An empirical examination of employee concerns", *Information Systems Frontiers*, vol. 20, pp. 91—110 <https://doi.org/10.1007/s10796-016-9667-5>.

8. National Institute of Standards and Technology (2017), Digital Identity Guidelines (NIST SP 800-63-3), Gaithersburg, Available at: <https://pages.nist.gov/800-63-3/> (Accessed 19 Mar 2026).

9. Gartner (2025), "Market Guide for Workforce Management Appl", Stamford, Available at: <https://www.gartner.com/en/documents/4005184> (Accessed 19 Mar 2026).

10. International Organization for Standardization (2022), ISO/IEC 2382-37:2022 Information technology — Vocabulary — Part 37: Biometrics, Geneva, Available at: <https://www.iso.org/obp/ui/#iso:std:iso-iec:2382-37:ed-1:v1:en> (Accessed 19 Mar 2026).

11. International Organization for Standardization (2022), ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements, Geneva, Available at: <https://www.iso.org/standard/82875.html> (Accessed 19 Mar 2026).

12. Nurhuda, A. and Safitri, N. (2026), "The use of biometrics in public services and the risk of privacy violations", *Jurnal Hukum Siber dan Regulasi Teknologi*, vol. 1, no. 1, pp. 46—55, Available at: <https://journal.sah.co.id/index.php/JHSRT/article/view/12> (Accessed 19 Mar 2026).

13. European Parliament and Council of the European Union (2016), "Regulation (EU) 2016/679 (General Data Protection Regulation)", Official Journal of the European Union, L 119, pp. 1—88, Available at: <https://eur-lex.europa.eu/eli/reg/2016/679/oj> (Accessed 19 Mar 2026).

14. National Institute of Standards and Technology (2020), Security and Privacy Controls for Information Systems and Organizations (NIST SP 800-53 Rev. 5), Gaithersburg, Available at: <https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final> (Accessed 19 Mar 2026).

15. World Economic Forum (2024), The Global Risks Report 2024, Geneva, Available at: <https://www.weforum.org/reports/global-risks-report-2024> (Accessed 19 Mar 2026).

16. Ussher-Eke, D., Okoh, O. F. and Ijiga, O. M. (2025), "The role of biometric and IoT-based attendance systems in streamlining HR administrative functions, enhancing workforce accountability, and reducing labor inefficiencies", *International Journal for Multidisciplinary Research*, vol. 7, no. 4, Available at: <https://www.ijfmr.com/papers/2025/4/52237.pdf> (Accessed 19 Mar 2026).

17. Zahorodnia, A. (2022), "Essence and evolution of the concept 'economic security of the enterprise'", *Ukrainian Journal of Applied Economics and Technology*, vol. 3 <https://doi.org/10.36887/2415-8453-2022-3-2>.

Отримано редакцією журналу / Received: 19.03.26

Професійно рецензовано / Revised: 30.03.26

Схвалено до друку / Accepted: 09.04.26