УДК 005.96:004
JEL: D83; L86; M15; O32; Q55
DOI: https://doi.org/10.32983/2222-4459-2025-9-483-490

ВИКОРИСТАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ ТА ІННОВАЦІЙНИХ ПРАКТИК У ФОРМУВАННІ КУЛЬТУРИ БЕЗПЕКИ ПІДПРИЄМСТВА

©2025 КОЛОМІЄЦЬ Б. С.

УДК 005.96:004
JEL: D83; L86; M15; O32; Q55

Коломієць Б. С. Використання цифрових технологій та інноваційних практик у формуванні культури безпеки підприємства

Проаналізовано сучасні тенденції використання цифрових технологій та інноваційних практик у формуванні культури безпеки підприємства. Визначено основні напрями цифровізації системи безпеки, зокрема впровадження ERP-модулів, VR/AR-симуляторів, електронних платформ комунікації та інструментів штучного інтелекту. Окреслено переваги застосування цифрових рішень для оперативного моніторингу, прогнозування ризиків та підвищення залученості персоналу. Запропоновано концепцію інтеграції AI та аналітики даних у систему управління безпекою, що передбачає створення електронної бази інцидентів, впровадження відеоаналітики, чат-ботів і аналітичних дашбордів. Обґрунтовано доцільність використання міжнародних стандартів ISO 45001 та ESG-підходів для підвищення рівня корпоративної культури безпеки. Виявлено основні ризики цифровізації, серед яких питання кібербезпеки, вартість впровадження та опір персоналу, і визначено шляхи їх мінімізації через поетапне впровадження та навчання. Систематизовано інструменти, документи, KPI та очікувані результати у вигляді матриці, що дозволяє комплексно оцінити ефективність впроваджених рішень. Доведено, що цифрові технології та інноваційні практики є стратегічними чинниками формування сучасної безпекоорієнтованої культури управління підприємством. Узагальнено, що впровадження таких підходів сприяє зниженню кількості інцидентів, економії ресурсів, підвищенню прозорості управління та формуванню позитивного іміджу підприємства. Висвітлено практичні рекомендації щодо створення електронної бази інцидентів, розробки цифрової карти ризиків і впровадження чат-ботів для підтримки персоналу. Підкреслено важливість поєднання технологічних, організаційних і мотиваційних інструментів для досягнення сталого розвитку та конкурентоспроможності підприємства. Наголошено на перспективності подальших досліджень щодо вдосконалення цифрових інструментів і розширення практик їх застосування у сфері корпоративної безпеки.

Ключові слова: *безпека, культура безпеки, безпекоорієнтований менеджмент, цифрові технології, управління безпекою, формування культури безпеки підприємства.*
Табл.: *3.* ***Бібл.:*** *8.*

Коломієць Богдан Сергійович *– кандидат педагогічних наук, докторант, Полтавський університет економіки і торгівлі (вул. Івана Банка, 3, Полтава, 36003, Україна)*
E-mail: *Kolombogd1@gmail.com*
ORCID: *https://orcid.org/0000-0002-7723-6666*

UDC 005.96:004
JEL: D83; L86; M15; O32; Q55

Kolomiiets B. S. The Use of Digital Technologies and Innovative Practices in Shaping Enterprise Security Culture

Modern trends in the use of digital technologies and innovative practices in shaping enterprise security culture have been analyzed. The main directions of digitalizing the security system have been identified, including the implementation of ERP modules, VR/AR simulators, electronic communication platforms, and artificial intelligence tools. The advantages of applying digital solutions for operational monitoring, risk forecasting, and enhancing employee engagement have been outlined. A conception for integrating AI and data analytics into the security management system has been proposed, which involves creating an electronic incident database, implementing video analytics, chatbots, and analytical dashboards. The rationale for using international standards ISO 45001 and ESG approaches to improve the level of corporate security culture has been substantiated. The main risks of digitalization have been identified, including cybersecurity issues, implementation costs, and staff resistance, and ways to mitigate them have been established through phased implementation and training. Tools, documents, KPIs, and expected outcomes have been systematized in a matrix, enabling a comprehensive assessment of the effectiveness of the implemented solutions. It has been demonstrated that digital technologies and innovative practices are strategic factors in shaping a modern security-oriented corporate management culture. It has been concluded that adopting such approaches helps reduce the number of incidents, save resources, enhance management transparency, and build a positive corporate image. Practical recommendations have been provided for creating an electronic incident database, developing a digital risk map, and implementing chatbots to support staff. The importance of combining technological, organizational, and motivational tools to achieve sustainable development and enterprise competitiveness has been emphasized. The importance of further research on enhancing digital tools and expanding their application in the field of corporate security is highlighted.

Keywords: *security, security culture, security-oriented management, digital technologies, security management, enterprise security culture formation.*
Tabl.: *3.* ***Bibl.:*** *8.*

Kolomiiets Bohdan S. *– Candidate of Sciences (Pedagogy), Candidate on Doctor Degree, Poltava University of Economics and Trade (3 Ivana Banka Str., Poltava, 36003, Ukraine)*
E-mail: *Kolombogd1@gmail.com*
ORCID: *https://orcid.org/0000-0002-7723-6666*

У сучасних умовах динамічного розвитку цифрових технологій і зростання ролі інноваційних практик питання формування ефективної культури безпеки на підприємствах набуває особливої актуальності. З одного боку, цифровізація бізнес-процесів відкриває нові можливості для підвищення ефективності управління, автоматизації рутинних операцій, оптимізації комунікацій та забезпечення прозорості діяльності. З іншого боку, впровадження цифрових технологій супроводжується виникненням нових ризиків, пов'язаних із кіберзагрозами, витоком конфіденційної інформації, порушенням приватності та іншими аспектами інформаційної безпеки.

Традиційні підходи до формування культури безпеки часто виявляються недостатньо ефективними в умовах цифрової трансформації, оскільки не враховують специфіку сучасних загроз та особливості взаємодії персоналу з цифровими інструментами. Відсутність належної культури безпеки може призвести до значних фінансових втрат, репутаційних ризиків та зниження конкурентоспроможності підприємства.

Таким чином, виникає необхідність дослідження теоретичних і практичних аспектів використання цифрових технологій та інноваційних практик у процесі формування культури безпеки підприємства. Особливої уваги потребує розробка ефективних механізмів інтеграції сучасних цифрових рішень у систему управління безпекою, а також формування у співробітників відповідального ставлення до питань безпеки в умовах цифрового середовища.

У сучасних дослідженнях Дуднєва Ю. Е. та Артем'єв О. О. розглядають комплаєнс-менеджмент як стратегічний інструмент забезпечення економічної безпеки бізнесу в умовах нестабільності, акцентуючи увагу на необхідності адаптації управлінських підходів до нових викликів [1]. Прохорова В. В. і Мушникова С. А. обґрунтовують коеволюційний підхід до управління економічною безпекою підприємств, що дозволяє враховувати динаміку зовнішніх і внутрішніх загроз [2]. Шимановська-Діанич Л. М. і Лозова О. В. підкреслюють важливість формування культури безпекоорієнтованого менеджменту в системі управління закладом освіти як умови досягнення цілей сталого розвитку, пропонуючи сучасні напрями та фреймворки для підвищення ефективності управління [3]. Дуднєва Ю. Е. та Артем'єв О. О. також аналізують особливості забезпечення економічної безпеки суб'єктів господарювання в умовах перманентної кризи, наголошуючи на необхідності адаптивного управління [4]. Отенко В. І., Віжунов А. О. та Устименко А. В. досліджують формування корпоративної безпеки за критерієм соціальної відповідальності бізнесу, що сприяє підвищенню довіри з боку стейкхолдерів [5]. Шимановська-Діанич Л. М., Педченко Н. С. і Лозова О. В. акцентують на проактивності в умовах діджиталізації економіки, що дозволяє вдосконалювати бізнес-процеси навіть під час воєнних викликів [6]. Кушнір О., Завада О., Сазонова Т. та інші автори розглядають моделювання організаційно-управлінської безпеки фінансового та кадрового забезпечення інноваційного агропідприємства, підкреслюючи роль цифрових інструментів у цьому процесі [7]. Притис В. І. визначає умови реалізації безпекоорієнтованого управління підприємствами з урахуванням існуючих загроз, що вимагає системного впровадження інноваційних практик [8].

Таким чином, аналіз сучасної літератури підтверджує актуальність інтеграції цифрових технологій, інноваційних підходів та міжнародних стандартів у систему формування культури безпеки підприємства.

Мета статті полягає у визначенні теоретичних засад і розробці практичних рекомендацій щодо впровадження цифрових технологій та інноваційних практик у процес формування культури безпеки на підприємствах. Особлива увага приділяється аналізу сучасних цифрових рішень, оцінці їхнього впливу на рівень безпеки організації, а також розробці ефективних підходів до інтеграції інновацій у систему корпоративної культури безпеки.

Сучасний розвиток освітньої сфери вимагає від підприємств переходу від традиційних методів управління безпекою до використання цифрових технологій та інноваційних практик, що забезпечують вищий рівень контролю, комунікацій, навчання та відповідальності. Інтеграція цифрових інструментів у систему менеджменту безпеки дозволяє оперативно виявляти ризики, формувати бази знань і розвивати в персоналу нові компетенції.

Розглянемо більш детально ці інструменти та необхідні документи, які б закріплювали їх використання в компанії.

1. Цифрові системи моніторингу та звітності.

ERP-модулі з управління безпекою (*Safety Management Systems*) – вбудовані рішення в корпоративні системи управління, які дозволяють вести облік інцидентів, контролювати виконання інструктажів, формувати звіти для керівництва.

Електронний інцидент-репортинг – можливість повідомляти про небезпечні ситуації чи ризики через мобільний додаток або корпоративний чат.

Дашборди показників безпеки – інтерактивні панелі, які відображають кількість інцидентів, рівень проходження навчань, кількість поданих пропозицій працівниками.

Документи:

– регламент використання електронної системи інцидент-репортингу;

– положення про систему моніторингу показників безпеки;

– форма електронного звіту про небезпечну подію.

2. VR/AR-технології в навчанні персоналу.

VR-симулятори дозволяють відтворювати небезпечні виробничі ситуації (падіння з висоти, обрив електропроводки, пожежа) та відпрацьовувати алгоритми поведінки в безпечних умовах.

AR-додатки можуть застосовуватись для підказок у реальному часі (наприклад, через смартфон чи окуляри працівник отримує інструкції з техніки безпеки при роботі з конкретним обладнанням).

Використання таких технологій підвищує ефективність навчання у 2–3 рази порівняно з традиційними інструктажами.

Документи:

– програма впровадження VR/AR-тренажерів у навчальний процес;

– методичні рекомендації з використання симуляторів під час тренінгів.

3. Інноваційні методи комунікацій та зворотного зв'язку.

Цифрові опитувальники (Google Forms, SurveyMonkey, корпоративні платформи) для регулярної оцінки рівня культури безпеки.

Електронна «скринька ідей» для пропозицій працівників щодо покращення умов безпеки.

Онлайн-платформи для навчання (Moodle, Coursera, власні LMS) з курсами з безпеки.

Документи:

– регламент щорічного електронного анкетування персоналу;

– положення про систему подання електронних пропозицій.

4. Інтеграція міжнародних стандартів та ESG-підходів.

ISO 45001 – система управління охороною праці та безпекою працівників. Вона дозволяє структурувати процеси та забезпечує відповідність міжнародним вимогам.

ESG-стандарти (*Environmental, Social, Governance*) – включення показників безпеки праці в нефінансову звітність підприємства як складової соціальної відповідальності.

Практика «Zero Harm» – політика нульової толерантності до інцидентів, що активно використовується міжнародними будівельними корпораціями.

Документи:

– корпоративна політика «Zero Harm»;

– звіт з ESG із розділом про безпеку праці;

– стандарт підприємства «Управління безпекою праці на основі ISO 45001».

5. Використання штучного інтелекту та аналітики даних.

AI-системи для прогнозування ризиків на основі даних про попередні інциденти.

Аналіз відеоспостереження для виявлення небезпечної поведінки працівників у реальному часі.

Чат-боти для швидкого консультування працівників з питань безпеки.

Документи:

– регламент застосування AI для моніторингу ризиків;

– протокол використання чат-бота як інструменту підтримки персоналу.

Використання цифрових технологій та інноваційних практик є необхідною умовою розвитку сучасної безпекоорієнтованої культури управління. Інтеграція ERP-модулів, VR/AR-симуляторів, електронних систем комунікації, міжнародних стандартів ISO 45001 та ESG-підходів дозволяє підвищити ефективність управління безпекою, забезпечити прозорість і залученість персоналу. У результаті підприємство отримує зниження кількості інцидентів, економію витрат і формування позитивного іміджу серед партнерів та інвесторів (*табл. 1*).

Актуальність застосування AI у сфері безпеки пояснюється тим, що в сучасних умовах воєнних ризиків, нестабільності ринків та кадрових викликів підприємства будівельної галузі стикаються з підвищеною кількістю небезпечних ситуацій. Традиційні методи моніторингу (журнали обліку, паперові звіти) є інертними та не дозволяють оперативно реагувати на загрози. Використання штучного інтелекту та аналітики великих даних дає можливість:

- прогнозувати ризики на основі попередніх інцидентів і поведінкових даних;
- виявляти небезпечні дії працівників у режимі реального часу;
- аналізувати відео з камер спостереження для автоматичного визначення порушень правил;
- отримувати швидкий доступ до статистики та рекомендацій для керівників.

Приклади застосування:

- *AI-прогнозування ризиків:* система аналізує історію інцидентів і визначає, які підрозділи чи процеси є найбільш уразливими.

Таблиця 1

Цифрові технології та інноваційні практики у формуванні культури безпеки підприємства

Напрям	Приклади застосування	Відповідні документи
Системи моніторингу	ERP-модулі з безпеки, електронний інцидент-репортинг, дашборди показників	Регламент інцидент-репортингу; положення про моніторинг; електронна форма звіту
VR/AR-навчання	VR-симуляції небезпечних ситуацій; AR-підказки під час роботи з обладнанням	Програма впровадження VR/AR; методичні рекомендації з використання симуляторів
Комунікації	Електронні опитувальники; онлайн «скринька ідей»; платформи дистанційного навчання	Регламент анкетування; положення про електронні пропозиції
Міжнародні стандарти	Впровадження ISO 45001; політика «Zero Harm»; включення безпеки у звіти ESG	Стандарт підприємства; політика «Zero Harm»; ESG-звіт
AI та аналітика	AI-прогнозування ризиків; аналіз відеоспостереження; чат-боти для консультацій	Регламент застосування AI; протокол використання чат-бота

Джерело: складено автором.

- *Аналіз відеоспостереження:* алгоритми розпізнають відсутність каски, неправильне використання обладнання, перебування в небезпечних зонах.
- *Чат-бот з охорони праці:* у месенджері працівник може миттєво отримати інструкції або повідомити про небезпеку.

Тому, на нашу думку, підприємствам варто зробити зараз таке:

1. Створити електронну базу інцидентів для накопичення даних, які згодом використовуватимуться для AI-аналітики.

2. Розробити «цифрову карту ризиків» підприємства, де будуть вказані найбільш небезпечні дільниці та види робіт.

3. Запровадити пілотний проєкт відеоаналітики на критично небезпечних майданчиках (наприклад, роботи на висоті, кранові операції).

4. Впровадити чат-бот для персоналу, який дозволить швидко отримувати відповіді на типові питання з безпеки та повідомляти про ризики.

5. Підготувати внутрішній документ «Концепція використання AI та аналітики даних у сфері безпеки», що визначить етапи впровадження, відповідальних осіб та очікувані результати.

Очікувані результати для підприємства:

- скорочення кількості інцидентів завдяки ранньому попередженню;
- економія ресурсів через зменшення витрат на лікарняні та компенсації;
- підвищення прозорості управління та довіри працівників;
- формування сучасного іміджу підприємства як інноваційної та соціально відповідальної компанії.

Таким чином, AI та аналітика – це не далеке майбутнє, а реальний інструмент, який підприємству варто почати впроваджувати вже зараз і ґрунтуватись на запропонованій нами концепції використання штучного інтелекту та аналітики даних у сфері безпеки на підприємстві.

КОНЦЕПЦІЯ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ТА АНАЛІТИКИ ДАНИХ У СФЕРІ БЕЗПЕКИ ПІДПРИЄМСТВА

1. Загальні положення.

Мета документа: визначення напрямів та етапів впровадження AI й аналітики в систему управління безпекою.

Обґрунтування актуальності: потреба у зниженні виробничих ризиків, зменшенні витрат на лікарняні та компенсації, підвищенні прозорості управління.

Сфера застосування: усі структурні підрозділи підприємства.

2. Цілі та завдання.

Підвищення ефективності моніторингу небезпечних ситуацій.

Прогнозування ризиків на основі історичних даних.

Автоматизація збору та обробки інформації про інциденти.

Забезпечення доступності консультацій із питань безпеки для всіх працівників.

3. Напрями використання AI та аналітики.

Прогнозування ризиків (аналіз даних про інциденти, виявлення закономірностей).

Відеоаналітика (розпізнавання небезпечної поведінки або порушень правил).

Чат-бот з безпеки (консультації працівників, повідомлення про ризики).

Аналітичні дашборди для керівництва.

4. Етапи впровадження.

Створення бази даних інцидентів (3–6 місяців).

Пілотний проєкт відеоаналітики на найбільш ризикових дільницях (6–12 місяців).

Запуск чат-бота для персоналу (до 1 року).

Розробка інтегрованого дашборду безпеки (до 1,5 років).

Повна інтеграція AI-рішень у систему менеджменту (до 2 років).

5. Відповідальні особи.

Директор підприємства – загальне керівництво та фінансування.

Служба охорони праці – адміністрування бази даних, аналіз результатів.

Відділ ІТ – технічна реалізація, підтримка цифрових систем.

HR-відділ – інтеграція чат-бота у процеси адаптації та навчання.

6. Очікувані результати.

Зменшення кількості інцидентів щонайменше на 20% протягом першого року.

Підвищення рівня задоволеності працівників системою безпеки (за результатами опитувань).

Зниження витрат на компенсації та простої на 10–15%.

Формування позитивного іміджу компанії як інноваційної та соціально відповідальної.

7. Контроль і моніторинг.

Щоквартальні звіти служби охорони праці про результати впровадження.

Щорічний аудит системи безпеки із залученням зовнішніх експертів.

Коригування Концепції відповідно до результатів і нових технологічних можливостей.

Етапи впровадження штучного інтелекту та аналітики в систему безпеки підприємства представлені в *табл. 2.*

Отже, запровадження штучного інтелекту та аналітики даних у систему безпекоорієнтованого управління підприємством є сучасним і стратегічно важливим кроком. Використання цифрової бази інцидентів, відеоаналітики, чат-ботів та інтегрованих дашбордів дозволяє перейти від реактивного до проактивного управління безпекою. Це забезпечує не лише зниження кількості інцидентів та економію витрат, а й формування довіри працівників, підвищення ефективності управлінських рішень та створення позитивного іміджу інноваційної компанії.

Цифровізація безпеки має очевидні переваги, проте вона супроводжується і ризиками. Насамперед це питання кіберзахисту, оскільки дані про інциденти чи персонал можуть стати об'єктом атак. Вартість впровадження сучасних цифрових інструментів (VR-симулятори, AI-системи) також є суттєвим фактором, який потрібно враховувати у фінансовому плануванні. Додатковим викликом може стати опір персоналу або складність у вико-

Таблиця 2

Етапи впровадження штучного інтелекту та аналітики в систему безпеки підприємства

Етап	Термін реалізації	Основні дії	Очікувані результати
1. Створення бази даних інцидентів	3–6 місяців	Формування електронного журналу інцидентів; стандартизація форм звітності	Накопичення даних для аналітики; підвищення прозорості обліку
2. Пілотний проєкт відеоаналітики	6–12 місяців	Встановлення камер на критичних дільницях; підключення AI для розпізнавання ризиків	Виявлення небезпечної поведінки в реальному часі; оперативне реагування
3. Запуск чат-бота з безпеки	до 1 року	Розробка та інтеграція чат-бота в месенджери; створення бази типових питань і відповідей	Швидкий доступ працівників до консультацій; зручний канал повідомлення про ризики
4. Аналітичний дашборд	до 1,5 років	Створення інтегрованої панелі показників; налаштування KPI з безпеки	Контроль ключових індикаторів; ухвалення управлінських рішень на основі даних
5. Повна інтеграція AI-рішень	до 2 років	Об'єднання всіх інструментів у єдину систему; регулярний аудит	Зниження інцидентів на ≥ 20%; підвищення ефективності менеджменту безпеки

Джерело: складено автором.

ристанні нових технологій, що вимагає організації навчання. Подолати ці ризики можливо через поетапне впровадження, пілотні проєкти та паралельне підвищення цифрових компетенцій персоналу.

Запровадження цифрових інструментів у сфері безпеки супроводжується ***ризиками,*** які необхідно враховувати.

Кібербезпека – витік даних про працівників та інциденти може стати репутаційним ризиком.

Вартість впровадження – придбання ліцензійного ПЗ, VR/AR-обладнання потребує інвестицій.

Опір персоналу – працівники можуть не довіряти цифровим системам або відчувати складність у користуванні.

Необхідність навчання – впровадження AI і VR вимагає додаткових компетенцій у персоналу.

Шляхи мінімізації:

- використання захищених серверів і систем резервного копіювання;
- поетапне впровадження (пілотні проєкти);
- навчальні програми для працівників;
- стимулювання довіри через прозорість і залучення персоналу.

Таким чином, використання цифрових технологій та інноваційних практик у формуванні безпекоорієнтованої культури управління є ключовим чинником підвищення ефективності системи безпеки на підприємстві. ERP-модулі, електронний інцидент-репортинг, VR/AR-тренажери, цифрові опитувальники та онлайн-платформи навчання забезпечують інтерактивність і оперативність у роботі з ризиками. Інтеграція міжнародних стандартів ISO 45001 та ESG-підходів дозволяє підняти рівень культури безпеки до міжнародного рівня, а застосування AI та аналітики даних відкриває нові можливості прогнозування та попередження інцидентів.

Інноваційні рішення є не лише технічними інструментами, а й стратегічними факторами, що формують нову модель управління безпекою, засновану на превентивності, прозорості та залученості персоналу.

Для того, щоб систематизувати всі складові формування безпекоорієнтованої культури, було складено матрицю (*табл. 3*), яка демонструє взаємозв'язок між інструментами, документами, KPI та очікуваними результатами. Така узагальнена модель дозволяє побачити комплексність підходу: від мотиваційних заходів і комунікацій до інтеграції цінностей у стратегію розвитку підприємства. Матриця підкреслює, що культура безпеки – це не окремі розрізнені дії, а цілісна система управління, яка поєднує людський, організаційний та технологічний виміри.

ВИСНОВКИ

Використання цифрових технологій та інноваційних практик у формуванні культури безпеки підприємства забезпечує перехід від традиційних, малоефективних підходів до сучасної, інтегрованої системи управління ризиками. Це дозволяє оперативно виявляти та попереджати інциденти, підвищувати прозорість і залученість персоналу.

Інтеграція ERP-модулів, VR/AR-технологій, електронних систем комунікації, міжнародних стандартів (ISO 45001, ESG) та інструментів штучного інтелекту створює комплексну екосистему

Таблиця 3

Системний підхід до формування безпекоорієнтованої культури управління підприємства

Складові культури безпеки	Інструменти	Документи	KPI	Очікуваний ефект
Мотивація	Премії, звання, відзнаки	Положення, накази	% працівників, які отримали відзнаки	Зростання зацікавленості
Комунікація	Safety-meetings, чати, бюлетені	Регламент нарад, шаблони бюлетенів	Частота нарад, охоплення повідомлень	Прозорість, швидкість обміну
Навчання	Тренінги, VR/AR, атестації	Програма навчання, накази	% охоплення навчанням	Зниження інцидентів
Цінності та стратегія	Політика, кодекс, ESG	Корпоративна політика, кодекс	Інтеграція у стратегію	Культура довіри
Лідерство	Участь керівництва	Накази, KPI менеджерів	% участі керівників	Партнерська модель
Контроль та зворотний зв'язок	Дашборди, опитування, «скринька ідей»	Регламент моніторингу, анкети	Пропозиції працівників, частота інцидентів	Постійне вдосконалення

Джерело: складено автором.

безпеки, де кожен співробітник стає активним учасником процесу. AI та аналітика даних дозволяють не лише фіксувати інциденти, а й прогнозувати ризики, аналізувати поведінкові патерни, автоматизувати моніторинг і надавати персоналізовані рекомендації, що підвищує ефективність управлінських рішень.

Впровадження цифрових інструментів супроводжується певними ризиками (кібербезпека, вартість, опір персоналу), однак їх можна мінімізувати через поетапне впровадження, навчання працівників, використання захищених систем і залучення персоналу до процесу змін. Системний підхід до формування культури безпеки передбачає поєднання мотиваційних, організаційних і технологічних інструментів, що забезпечує сталий розвиток підприємства, зниження кількості інцидентів, економію ресурсів та формування позитивного іміджу. Запропонована концепція впровадження AI та аналітики даних у систему безпеки підприємства є практичним інструментом для підвищення ефективності моніторингу, прогнозування ризиків і формування сучасної безпекоорієнтованої культури.

Отже, цифровізація та інновації у сфері безпеки – це не лише вимога часу, а й стратегічна перевага для підприємств, які прагнуть до сталого розвитку, конкурентоспроможності та соціальної відповідальності. ■

БІБЛІОГРАФІЯ

1. Дуднєва Ю. Е., Артем'єв О. О. Комплаєнс-менеджмент як стратегічний інструмент забезпечення економічної безпеки бізнесу в умовах нестабільності. *Бізнес Інформ*. 2025. № 1. С. 406–413. DOI: https://doi.org/10.32983/2222-4459-2025-1-406-413
2. Прохорова В. В., Мушникова С. А. Коеволюційна основа управління економічною безпекою підприємств. *Бізнес Інформ*. 2020. № 12. С. 440–445. DOI: https://doi.org/10.32983/2222-4459-2020-12-440-445
3. Шимановська-Діанич Л. М., Лозова О. В. Формування культури безпекоорієнтованого менеджменту в системі управління закладом освіти як умова досягнення цілей сталого розвитку: напрями, заходи та фрейморк. *Вісник Львівського торговельно-економічного університету. Серія «Економічні науки»*. 2025. № 82. С. 28–35. DOI: https://doi.org/10.32782/2522-1205-2025-82-04
4. Дуднєва Ю., Артем'єв О. Економічна безпека суб'єктів господарювання в умовах перманентної кризи. *Адаптивне управління: теорія і практика. Серія «Економіка»*. 2023. Вип. 17. DOI: https://doi.org/10.33296/2707-0654-17(34)-09
5. Отенко В. І., Віжунов А. О., Устименко А. В. Формування корпоративної безпеки за критерієм соціальної відповідальності бізнесу. *Бізнес Інформ*. 2025. № 1. С. 462–470. DOI: https://doi.org/10.32983/2222-4459-2025-1-462-470
6. Шимановська-Діанич Л. М., Педченко Н. С., Лозова О. В. Проактивність в умовах діджиталізації економіки: удосконалення бізнес-ппроцесів вітчизняних підприємств під час війни. *Науковий вісник Полтавського університету економіки і торгівлі. Серія «Економічні науки»*. 2024. Вип. 2. С. 109–116. DOI: https://doi.org/10.37734/2409-6873-2024-2-16
7. Кушнір О., Завада О., Сазонова Т. та ін. Моделювання організаційно-управлінської безпеки фінансового та кадрового забезпечення інноваційного агропідприємства. *Financial and Credit Activity Problems of Theory and Practice*. 2024. Т. 5. № 58. С. 534–552. DOI: https://doi.org/10.55643/fcaptp.5.58.2024.4590
8. Притис В. І. Умови реалізації безпекоорієнтованого управління підприємствами з урахуванням існуючих загроз. *Бізнес Інформ*. 2020. № 3. С. 453–459. DOI: https://doi.org/10.32983/2222-4459-2020-3-453-459

REFERENCES

Dudnieva, Yu., & Artemiev, O. (2023). Ekonomichna bezpeka subiektiv hospodariuvannia v umovakh permanentnoi kryzy [Economic security of economic entities in the conditions of a permanent crisis]. *Adaptyvne upravlinnia: teoriia i praktyka. Seriia «Ekonomika», 17*, 1–9. https://doi.org/10.33296/2707-0654-17(34)-09

Dudnieva, Yu. E., & Artemiev, O. O. (2025). Komplaiens-menedzhment yak stratehichnyi instrument zabezpechennia ekonomichnoi bezpeky biznesu v umovakh nestabilnosti [Compliance management as a strategic tool for ensuring the economic security of business in conditions of instability]. *Biznes Inform, 1*, 406–413. https://doi.org/10.32983/2222-4459-2025-1-406-413

Kushnir, O., Zavada, O., Sazonova, T., & in. (2024). Modeliuvannia orhanizatsiino-upravlinskoi bezpeky finansovoho ta kadrovoho zabezpechennia innovatsiinoho ahropidpryiemstva [Modeling of organizational and managerial security of financial and personnel support of an innovative agricultural enterprise]. *Financial and Credit Activity Problems of Theory and Practice, 5*(58), 534–552. https://doi.org/10.55643/fcaptp.5.58.2024.4590

Otenko, V. I., Vizhunov, A. O., & Ustymenko, A. V. (2025). Formuvannia korporatyvnoi bezpeky za kryteriiem sotsialnoi vidpovidalnosti biznesu [Formation of corporate security according to the criterion of social responsibility of business]. *Biznes Inform, 1*, 462–470. https://doi.org/10.32983/2222-4459-2025-1-462-470

Prokhorova, V. V., & Mushnykova, S. A. (2020). Koevoliutsiina osnova upravlinnia ekonomichnoiu bezpekoiu pidpryiemstv [Coevolutionary basis of economic security management of enterprises]. *Biznes Inform, 12*, 440–445. https://doi.org/10.32983/2222-4459-2020-12-440-445

Prytys, V. I. (2020). Umovy realizatsii bezpekooriientovanoho upravlinnia pidpryiemstvamy z urakhuvanniam isnuiuchykh zahroz [Conditions for the implementation of security-oriented management of enterprises, taking into account existing threats]. *Biznes Inform, 3*, 453–459. https://doi.org/10.32983/2222-4459-2020-3-453-459

Shymanovska-Dianych, L. M., & Lozova, O. V. (2025). Formuvannia kultury bezpekooriientovanoho menedzhmentu v systemi upravlinnia zakladom osvity yak umova dosiahnennia tsilei staloho rozvytku: napriamy, zakhody ta freimork [Formation of a culture of safety-oriented management in the educational institution management system as a condition for achieving sustainable development goals: directions, measures and framework]. *Visnyk Lvivskoho torhovelno-ekonomichnoho universytetu. Seriia «Ekonomichni nauky», 82*, 28–35. https://doi.org/10.32782/2522-1205-2025-82-04

Shymanovska-Dianych, L. M., Pedchenko, N. S., & Lozova, O. V. (2024). Proaktyvnist v umovakh didzhytalizatsii ekonomiky: udoskonalennia biznes-pprotsesiv vitchyznianykh pidpryiemstv pid chas viiny [Proactivity in the context of digitalization of the economy: improving the business processes of domestic enterprises during the war]. *Naukovyi visnyk Poltavskoho universytetu ekonomiky i torhivli. Seriia «Ekonomichni nauky», 2*, 109–116. https://doi.org/10.37734/2409-6873-2024-2-16

УДК 005.95/.96:004.9
JEL: M12; M15; O33
DOI: https://doi.org/10.32983/2222-4459-2025-9-490-497

МЕХАНІЗМИ УПРАВЛІННЯ ПЕРСОНАЛОМ В УМОВАХ ЦИФРОВІЗАЦІЇ З ВИКОРИСТАННЯМ ERP-СИСТЕМИ ODOO

©2025 **ПОВІДАЙЧИК М. М., ПОПИК М. М.**

УДК 005.95/.96:004.9
JEL: M12; M15; O33

Повідайчик М. М., Попик М. М. Механізми управління персоналом в умовах цифровізації з використанням ERP-системи ODoo

У статті розглянуто особливості управління персоналом підприємства в умовах цифровізації та глобалізації. Показано, що HR-процеси потребують інтеграції, прозорості та аналітичної підтримки для забезпечення мобільності кадрів, організації віддаленої роботи та дотримання вітчизняних трудових стандартів. Обґрунтовано доцільність використання ERP-системи Odoo як комплексного інструмента управління людськими ресурсами, що поєднує модульність, інтегративність та широкі аналітичні можливості. Охарактеризовано ключові HR-модулі Odoo (Employees, Recruitment, Attendances, Payroll, Appraisals, Time Off), їх взаємозв'язок із фінансовими, проєктними та CRM-компонентами, а також роль у формуванні єдиного інформаційного простору компанії. Особливу увагу приділено моделюванню та оптимізації HR-процесів у середовищі Odoo, що сприяють підвищенню ефективності кадрової діяльності, зниженню витрат, забезпеченню прозорості управлінських процедур і розвитку стратегічного потенціалу людського капіталу. Зроблено порівняльний аналіз деяких ERP-систем (SAP, Oracle), у якому охарактеризовано Odoo за ключовими критеріями: вирізняється доступною вартістю, оскільки має безкоштовну версію Community та гнучку підписку; цільова аудиторія Odoo охоплює як малий, середній, так і великий бізнес; за гнучкістю Odoo демонструє високу модульність: функціонал Odoo охоплює широкий спектр модулів (CRM, HRM, фінанси, склад, виробництво тощо); впровадження Odoo є відносно простим і швидким; інтерфейс Odoo сучасний і зручний; у сфері підтримки та інтеграцій Odoo пропонує активну спільноту та численні інтеграції з онлайн-сервісами. Обґрунтовано, що застосування сучасних методів моделювання надає нові можливості. Так, використання BPMN забезпечує візуалізацію процедур (наприклад, рекрутингу чи адаптації), IDEF0 дає змогу описати функціональну структуру HR-менеджменту, а ARIS забезпечує інтеграцію кадрових процесів із фінансовими, логістичними та виробничими. Зроблено висновок, що використання Odoo у сфері HR є важливим чинником підвищення конкурентоспроможності підприємства.

Ключові слова: *управління персоналом, ERP-система, Odoo, HR-процеси, цифровізація, моделювання, оптимізація, людський капітал.*
Рис.*: 1.* ***Табл.:*** *3.* ***Бібл.:*** *9.*

Повідайчик Михайло Михайлович *– доктор педагогічних наук, доцент, професор кафедри кібернетики і прикладної математики, Ужгородський національний університет (пл. Народна, 3, Ужгород, 88000, Україна)*
E-mail: *mykhailo.povidaichyk@uzhnu.edu.ua*
ORCID: *https://orcid.org/0000-0003-1554-2067*

Попик Мар'яна Михайлівна *– кандидат економічних наук, доцент, доцент кафедри туристичної інфраструктури та готельно-ресторанного господарства, Ужгородський національний університет (пл. Народна, 3, Ужгород, 88000, Україна)*
E-mail: *mariana.popyk@uzhnu.edu.ua*
ORCID: *https://orcid.org/0000-0003-1693-7896*
Researcher ID: *https://www.webofscience.com/wos/author/record/F-7178-2019*
Scopus Author ID: *https://www.scopus.com/authid/detail.uri?authorId=57223371140*