

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Західноукраїнський національний університет
Навчально-науковий інститут новітніх освітніх технологій
Кафедра менеджменту, публічного управління та персоналу

ЛЕВЕНЕЦЬ Олександр Олегович

Безпека персональних даних при цифровізації кадрового діловодства. /
Personal data security in the digitalization of personnel documentation

"спеціальність: 073 - Менеджмент
освітньо-професійна програма - Управління персоналом"

Кваліфікаційна робота

Виконав студент групи МЕНУПз-41
О. О. Левенець

Науковий керівник:
к.е.н., професор, Є. П. Качан

ТЕРНОПІЛЬ – 2026

ЗМІСТ

ВСТУП	3
РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ БЕЗПЕКИ ПЕРСОНАЛЬНИХ ДАНИХ У СИСТЕМІ КАДРОВОГО МЕНЕДЖМЕНТУ	7
1.1. Сутність, класифікація та роль персональних даних у системі управління персоналом	7
1.2. Цифровізація кадрового діловодства як напрям розвитку сучасного менеджменту	20
РОЗДІЛ 2. АНАЛІЗ СИСТЕМИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У ПРОЦЕСІ ЦИФРОВІЗАЦІЇ КАДРОВОГО ДІЛОВОДСТВА ПІДПРИЄМСТВА	31
2.1. Організаційно-управлінська характеристика системи кадрового діловодства підприємства	31
2.2. Оцінка рівня безпеки персональних даних та ризиків у цифровому HR-середовищі	41
РОЗДІЛ 3. УДОСКОНАЛЕННЯ СИСТЕМИ УПРАВЛІННЯ БЕЗПЕКОЮ ПЕРСОНАЛЬНИХ ДАНИХ У КАДРОВОМУ ДІЛОВОДСТВІ	41
3.1. Формування організаційно-управлінських механізмів забезпечення захисту персональних даних	49
3.2. Впровадження сучасних цифрових та управлінських рішень у сфері інформаційної безпеки персоналу	54
ВИСНОВКИ	62
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	65

ВСТУП

Актуальність теми безпеки персональних даних при цифровізації кадрового діловодства зумовлена глибокими трансформаційними процесами, що відбуваються у сфері управління персоналом. У сучасних умовах цифрова трансформація охоплює практично всі аспекти діяльності організацій, зокрема кадрові процеси. Перехід від паперового до електронного документообігу істотно підвищує ефективність управління персоналом.

Водночас цифровізація супроводжується зростанням обсягів обробки персональних даних працівників. Це, у свою чергу, актуалізує питання їх належного захисту. Персональні дані є чутливою інформацією, яка потребує особливої уваги з боку менеджменту. У кадровому діловодстві такі дані охоплюють широкий спектр відомостей про працівника. До них належать ідентифікаційні, соціальні, фінансові та професійні характеристики. Зберігання та обробка цих даних в електронному вигляді створює нові ризики. Зокрема, це ризики несанкціонованого доступу, витоку інформації та кібератак. У сучасних умовах кіберзагрози стають дедалі складнішими та масштабнішими. Організації змушені адаптуватися до нових викликів інформаційної безпеки.

Особливу роль у цьому процесі відіграє система управління персоналом. Саме HR-служби є основними користувачами та розпорядниками персональних даних. Тому на них покладається відповідальність за їх захист. Недостатній рівень безпеки персональних даних може призвести до серйозних наслідків. Серед них — фінансові втрати, юридична відповідальність та репутаційні ризики. В умовах посилення регуляторних вимог питання захисту даних набуває ще більшої актуальності. В Україні діє законодавство, що регулює обробку та захист персональних даних. Однак практична реалізація цих норм часто є недостатньо ефективною. Це зумовлює потребу у вдосконаленні управлінських підходів до забезпечення безпеки інформації.

Крім того, цифровізація кадрового діловодства передбачає використання різноманітних HRM-систем. Впровадження таких систем

вимагає комплексного підходу до захисту даних. Особливої уваги потребує управління доступом до інформації. Також важливим є питання підвищення цифрової грамотності персоналу. Людський фактор залишається одним із ключових джерел ризиків. Тому ефективне управління безпекою персональних даних повинно поєднувати технічні та організаційні заходи.

Актуальність теми зростає і в умовах дистанційної роботи та використання хмарних сервісів. Це розширює межі доступу до даних та ускладнює контроль за їх захистом. У таких умовах менеджмент має забезпечити баланс між доступністю інформації та її безпекою. Таким чином, дослідження безпеки персональних даних у процесі цифровізації кадрового діловодства є важливим як з теоретичної, так і з практичної точки зору. Воно спрямоване на підвищення ефективності управління персоналом та забезпечення захисту прав працівників. Саме це визначає високу актуальність обраної теми дослідження.

Проблеми впливу цифровізації на трансформацію HR-технологій висвітлені у працях Г. В. Бей та Г. В. Середи, тоді як питання застосування інформаційних технологій у кадровому менеджменті досліджуються О. С. Бурлаковим та М. І. Васильченком, Н. І. Васишиним. Окрему увагу автоматизації кадрового діловодства приділяють М. А. Горшков, В. Ю. Дейнека та І. В. Довжук, які аналізують сучасні програмні рішення та інструменти цифрового документообігу. Важливі аспекти правового забезпечення захисту персональних даних розкриті у працях Т. О. Гуржій, а також С. М. Гусарова та К. Ю. Мельник, які акцентують увагу на необхідності дотримання законодавчих норм у сфері обробки персональних даних працівників. Питання автоматизації управління персоналом та підвищення продуктивності праці досліджуються О. П. Кавтиш і О. В. Максимішиною, а концептуальні засади обліку праці – С. В. Коваль, С. В. Скрипник та І. В. Шепель.

Метою роботи є дослідження теоретичних і практичних засад забезпечення безпеки персональних даних у процесі цифровізації кадрового

діловодства, а також розробка обґрунтованих управлінських рекомендацій щодо підвищення рівня їх захисту в діяльності організації.

Для досягнення поставленої мети у роботі визначено такі **завдання**:

- розкрити сутність персональних даних та їх значення у системі управління персоналом;
- дослідити особливості цифровізації кадрового діловодства в сучасних організаціях;
- проаналізувати нормативно-правове забезпечення захисту персональних даних;
- здійснити оцінку організаційно-управлінських аспектів ведення кадрового діловодства на підприємстві;
- визначити основні ризики та загрози безпеці персональних даних у цифровому HR-середовищі;
- обґрунтувати напрями вдосконалення системи управління безпекою персональних даних у кадровому діловодстві.

Об'єктом дослідження є процес цифровізації кадрового діловодства в організації.

Предметом дослідження є сукупність управлінських, організаційних та інформаційних механізмів забезпечення безпеки персональних даних у системі кадрового діловодства в умовах цифрової трансформації.

У процесі виконання кваліфікаційної роботи використано сукупність загальнонаукових і спеціальних **методів дослідження**. Зокрема, застосовано методи аналізу та синтезу для узагальнення теоретичних підходів до визначення сутності персональних даних та їх ролі в системі управління персоналом. Метод порівняння використано для дослідження особливостей цифровізації кадрового діловодства та нормативно-правового забезпечення захисту інформації.

Системний підхід дозволив розглянути процес забезпечення безпеки персональних даних як комплексну управлінську систему, що включає організаційні, технічні та правові складові. Методи узагальнення та

класифікації застосовано для виявлення основних ризиків і загроз інформаційній безпеці. Елементи економічного та управлінського аналізу використано при дослідженні практичних аспектів функціонування кадрового діловодства на підприємстві. Також застосовано описовий метод для формування рекомендацій щодо вдосконалення системи захисту персональних даних.

Практичне значення отриманих результатів полягає у можливості їх використання для підвищення ефективності управління персоналом та забезпечення належного рівня захисту персональних даних у процесі цифровізації кадрового діловодства.

РОЗДІЛ 1

ТЕОРЕТИЧНІ ЗАСАДИ БЕЗПЕКИ ПЕРСОНАЛЬНИХ ДАНИХ У СИСТЕМІ КАДРОВОГО МЕНЕДЖМЕНТУ

1.1. Сутність, класифікація та роль персональних даних у системі управління персоналом

Сучасні дослідження у сфері захисту даних, приватності, інформаційної та кібербезпеки, що здійснюються представниками різних наукових напрямів, дедалі частіше акцентують увагу на необхідності формування комплексних міждисциплінарних підходів. Такі підходи мають інтегрувати існуючі наукові напрацювання, переосмислювати їх та узгоджувати з метою пошуку нових ефективних моделей забезпечення безпеки інформації.

Захист персональних даних працівників як у фізичному, так і в цифровому середовищі реалізується передусім на рівні організацій. Водночас діяльність організацій відбувається в умовах взаємодії різних середовищ — економічного, правового, ринкового та технологічного. Усі ці фактори необхідно враховувати при формуванні стратегії управління даними та впровадженні відповідних практик їх захисту.

Для більш глибокого розуміння проблематики забезпечення приватності в цифровому суспільстві доцільно звернутися до концептуальних моделей, розроблених фахівцями у цій сфері. Зокрема, виділяють шість ключових груп чинників, що впливають на створення надійної інфраструктури цифрової приватності. До них належать технічні, регуляторні, економічні, законодавчі, індивідуальні, а також соціально-культурні фактори. Кожен із цих чинників формує очікування користувачів щодо рівня захисту персональних даних у межах цифрових екосистем (табл. 1.1). Взаємозв'язок факторів забезпечення цифрової приватності представлено на рис. 1.1.

Дослідники також наголошують на необхідності розроблення комплексних програм наукових досліджень, які б охоплювали різні аспекти захисту даних, зокрема юридичний, етичний, технологічний, міжнародний і

кадровий. Особливої уваги потребує сфера приватності на робочому місці, де важливо розмежовувати інформаційну приватність та інші її види, зокрема просторову чи акустичну.

Таблиця 1.1

Фактори формування цифрової приватності та їх вплив на HR-системи
[21]

Група факторів	Зміст	Вплив на кадрове діловодство
Технічні	Рівень розвитку IT-інфраструктури	Визначають рівень захисту HR-систем
Законодавчі	Норми GDPR, національні акти	Регламентують обробку даних працівників
Регуляторні	Вимоги контролюючих органів	Формують політики безпеки
Економічні	Фінансові ресурси організації	Впливають на впровадження HRM-систем
Індивідуальні	Рівень цифрової грамотності працівників	Визначають ризик людського фактору
Соціокультурні	Рівень довіри та цифрової культури	Впливають на дотримання політик безпеки



Рис. 1.1. Модель факторів забезпечення цифрової приватності [17, с. 119]

Важливим аспектом є визначення кола зацікавлених сторін у процесі забезпечення захисту персональних даних. До них належать працівники,

роботодавці, державні інституції та суспільство загалом, які прямо або опосередковано беруть участь у формуванні та реалізації політики захисту даних.

Таким чином, аналіз сучасних регуляторних вимог до діяльності HR-служб у сфері захисту персональних даних, зокрема в країнах Європейського Союзу, а також вивчення тенденцій цифровізації систем управління персоналом, дозволяє виявити як нові можливості, так і значні виклики. У цьому контексті особливого значення набуває оцінка сучасних загроз та ризиків для інформаційної приватності в умовах глобалізованого цифрового середовища.

Нормативно-правове забезпечення захисту персональних даних в організаціях включає сукупність регуляторних актів, серед яких ключову роль відіграють Загальний регламент захисту даних (GDPR), національні законодавчі акти, норми трудового права та галузеві стандарти. Запровадження GDPR стало важливим стимулом для оновлення законодавства у сфері захисту даних у багатьох країнах світу.

У межах визначених правових рамок організації зобов'язані забезпечувати прозорість обробки даних, підзвітність, оцінку ризиків, а також своєчасне реагування на інциденти безпеки. Це створює основу для формування відповідальної практики управління персональними даними, яка переважно реалізується в межах діяльності HR-підрозділів та суміжних структур [7, с. 53].

Для кращого розуміння сучасних вимог до захисту персональних даних, яких мають дотримуватися системи управління персоналом в організаціях країн Європейського Союзу, а також суб'єкти, що здійснюють обробку даних громадян ЄС, доцільно виокремити основні нормативно-правові положення, закріплені у рамках GDPR.

Визначення правомірних підстав для обробки персональних даних працівників є ключовою вимогою сучасного законодавства у сфері захисту інформації. Зокрема, стаття 6 Загального регламенту захисту даних (GDPR)

встановлює вичерпний перелік законних підстав для обробки персональних даних, тоді як стаття 7 конкретизує вимоги щодо отримання та використання згоди суб'єкта даних. У контексті трудових відносин особливого значення набуває стаття 88 GDPR, яка надає державам-членам право визначати додаткові правила обробки персональних даних працівників з урахуванням специфіки трудового законодавства.

Важливим принципом сучасного підходу до захисту даних є концепція «захисту за проєктуванням та за замовчуванням», закріплена у статті 25 GDPR. Відповідно до цього принципу, організації зобов'язані впроваджувати технічні та організаційні заходи, що забезпечують мінімізацію обсягу оброблюваних даних і належний рівень їх захисту ще на етапі розроблення інформаційних систем.

Не менш важливою є вимога забезпечення прозорості обробки персональних даних. Згідно зі статтями 12–14 GDPR, роботодавець повинен надавати працівникам чітку, доступну та вичерпну інформацію щодо процесів обробки даних, включаючи мету збору, строки зберігання та права суб'єктів даних.

Суттєву роль відіграють також права працівників як суб'єктів персональних даних. Зокрема, стаття 15 гарантує право на доступ до власних даних та отримання інформації про їх обробку, тоді як стаття 20 передбачає можливість перенесення даних у структурованому, зручному для використання форматі. Крім того, стаття 17 закріплює так зване «право на забуття», що дозволяє вимагати видалення персональних даних у випадках, коли вони більше не є необхідними або обробляються незаконно.

Особливу увагу слід приділити механізмам відповідальності за порушення вимог захисту даних. Відповідно до статті 83 GDPR, наглядові органи мають право застосовувати значні адміністративні санкції, які можуть досягати 20 мільйонів євро або 4% від річного глобального обороту компанії. Такий рівень фінансових ризиків стимулює організації до посилення внутрішніх систем управління безпекою даних.

Запровадження GDPR у поєднанні з високими штрафними санкціями стало потужним чинником трансформації підходів до обробки персональних даних у країнах Європейського Союзу. Організації змушені впроваджувати нові політики, процедури та управлінські практики, спрямовані на забезпечення відповідності вимогам Регламенту. Серед таких заходів — реалізація принципів захисту даних за замовчуванням, розробка ефективних механізмів реагування на інциденти безпеки, проведення оцінки впливу на захист даних (DPIA), удосконалення процесів управління згодою та автоматизація обробки запитів суб'єктів даних.

Разом із тим, як зазначають дослідники Labadie та Legner (2023), значна кількість організацій стикається з труднощами у процесі імплементації вимог GDPR. Це пояснюється тим, що нові стандарти захисту персональних даних не можуть бути реалізовані лише шляхом адаптації існуючих підходів, а потребують глибокого переосмислення процесів зберігання, обробки та управління даними на рівні всієї організації.

Правове та регуляторне середовище впровадження сучасних цифрових технологій перебуває у постійному розвитку та адаптації в різних країнах світу. Це зумовлено необхідністю реагування на нові виклики, пов'язані з поширенням технологій штучного інтелекту, зростанням кіберзагроз та ускладненням цифрової інфраструктури. У цьому контексті в Європейському Союзі протягом останніх років було прийнято низку важливих нормативно-правових актів, які мають враховуватися організаціями при здійсненні своєї діяльності [9, с. 134].

Зокрема, одним із ключових документів є Закон про штучний інтелект, впровадження якого розпочалося у серпні 2024 року, а повноцінне застосування заплановано на квітень 2026 року. Цей акт розглядається як перша у світі комплексна правова система, спрямована на встановлення узгоджених правил для розвитку надійного та безпечного штучного інтелекту в межах ЄС. Його особливістю є ризик-орієнтований підхід, який визначає

різні вимоги для розробників і користувачів залежно від рівня потенційної небезпеки застосування технологій.

Основною метою цього закону є забезпечення захисту фундаментальних прав людини, зокрема права на приватність та безпеку персональних даних. У цьому контексті встановлюються підвищені вимоги до обробки інформації у системах штучного інтелекту, особливо тих, що відносяться до категорії високого ризику, включаючи HR-технології. Водночас зазначений акт функціонує у тісному взаємозв'язку з положеннями GDPR, доповнюючи їх у частині регулювання новітніх цифрових рішень.

Ще одним важливим нормативним документом є Закон про кіберстійкість (Cyber Resilience Act, CRA), який набув чинності 10 грудня 2024 року, а його повна імплементація передбачена до грудня 2027 року. Цей регламент встановлює обов'язкові вимоги до забезпечення кібербезпеки підключених цифрових продуктів, зокрема програмного забезпечення, пристроїв Інтернету речей та мережевого обладнання. CRA доповнює вже існуючі правові інструменти, зокрема Директиву NIS2, яка спрямована на зменшення кіберризиків у межах цифрового ланцюга постачання в ЄС.

Ключовими завданнями цього регламенту є зобов'язання виробників інтегрувати заходи кібербезпеки ще на етапі створення продуктів та забезпечувати їх протягом усього життєвого циклу. Крім того, передбачається формування єдиного підходу до регулювання кібербезпеки, що спрощує дотримання вимог для розробників як апаратного, так і програмного забезпечення. Важливим аспектом також є забезпечення прозорості щодо характеристик безпеки цифрових продуктів та створення умов для їх безпечного використання як бізнесом, так і кінцевими споживачами.

У свою чергу, українські фахівці підкреслюють необхідність подальшого вдосконалення національного законодавства у контексті євроінтеграційних процесів. Станом на кінець 2024 року Україна виконала близько 71% зобов'язань у рамках Угоди про асоціацію з Європейським Союзом у сфері науки, технологій, інновацій та цифрової інтеграції. Проте

актуальним залишається завдання подальшої гармонізації українського правового поля з нормами ЄС, особливо у сфері захисту персональних даних та регулювання використання технологій штучного інтелекту.

Цифровізація систем управління персоналом водночас виступає як важливий фактор підвищення ефективності діяльності організацій, так і джерело нових ризиків у сфері захисту та безпеки даних. Сучасні HR-екосистеми охоплюють широкий спектр цифрових платформ та інструментів, які забезпечують автоматизацію ключових кадрових процесів, зокрема підбору персоналу, адаптації працівників, навчання, оцінювання результатів діяльності, управління компенсаціями та пільгами, а також аналітики персоналу.

Функціонування таких систем базується на використанні хмарних технологій, мобільних застосунків і рішень на основі штучного інтелекту, що дозволяє забезпечити оперативність управлінських рішень і високий рівень персоналізації HR-процесів. Важливими складовими сучасної HR-екосистеми є інформаційні системи управління персоналом (HRIS), які виступають централізованими сховищами даних, системи управління талантами, платформи дистанційного навчання (LMS), рішення для управління компенсаціями та пільгами, інструменти залучення персоналу та аналітичні модулі, що використовують технології штучного інтелекту [18, с. 34].

Зазначені компоненти формують складну систему потоків даних у цифровому середовищі, що значно підвищує їхню вразливість до кіберзагроз. HR-системи обробляють значні обсяги персональної інформації, включаючи чутливі дані, що потребує особливої уваги до питань інформаційної безпеки (табл. 1.2).

Важливу роль у сучасних HR-екосистемах відіграють рішення типу SaaS (Software as a Service), які дозволяють організаціям використовувати функціонал HR-платформ без необхідності створення власної IT-інфраструктури. Прикладами таких систем є Workday, SAP SuccessFactors, Oracle HCM Cloud та інші. Вони забезпечують доступ до даних у режимі

реального часу, швидке оновлення функціоналу та підвищення ефективності управління персоналом. Водночас використання таких рішень супроводжується зростанням ризиків, пов'язаних із контролем доступу до даних та забезпеченням їх належного захисту.

Таблиця 1.2

Ключові ризики захисту персональних даних у цифровому HR-середовищі [28, с. 127]

Вид ризику	Сутність	Наслідки для організації
Кіберзагрози	Атаки (фішинг, віруси, зломи)	Витік або втрата даних
Людський фактор	Помилки працівників	Несанкціонований доступ
Недосконалість регулювання	Прогалини у законодавстві	Юридичні ризики
Використання ІІІ	Автоматизовані рішення	Дискримінація, непрозорість
Хмарні технології	Зберігання даних у SaaS	Втрата контролю над даними

В Україні процес цифровізації управління персоналом значно активізувався після 2020 року. Зокрема, у державному секторі впроваджуються системи електронного кадрового документообігу, зокрема через цифрові платформи «Дія» та «ЄКадри». Важливим кроком стало запровадження інтегрованої інформаційної системи управління людськими ресурсами в органах державної влади (HRMIS), яка почала функціонувати з 31 березня 2021 року за підтримки Європейського Союзу в межах програми EU4PFM.

Цифрова трансформація державної служби та управління людськими ресурсами є складовою євроінтеграційного курсу України та реалізується відповідно до європейських принципів державного управління, розроблених OECD/SIGMA. Крім того, вона є однією з умов отримання фінансової підтримки в рамках програми Ukraine Facility.

Паралельно приватний сектор активно впроваджує сучасні HRM-рішення, серед яких як національні платформи (BAS HRM, PeopleForce, Hurma, Kadro), так і міжнародні системи (Workday, SAP, SuccessFactors). Це свідчить про зростання ролі цифрових технологій у сфері управління

персоналом, водночас підсилюючи актуальність питань забезпечення безпеки персональних даних у цих процесах.

Поряд із очевидними перевагами цифровізації систем управління персоналом, організації, державні реєстри та комерційні структури дедалі частіше стають об'єктами кіберзагроз. Зокрема, за даними урядової команди реагування на комп'ютерні інциденти CERT-UA при Держспецзв'язку, у 2024 році було зафіксовано та опрацьовано 4315 кіберінцидентів. Це на 69,8% більше порівняно з попереднім роком, коли кількість атак становила 2541 випадок. Така динаміка свідчить про суттєве загострення ситуації у сфері кібербезпеки.

Найбільш вразливими до кіберзлочинності залишаються органи місцевого самоврядування, державні установи, сектор безпеки та оборони, енергетика, телекомунікації, а також комерційні підприємства. Серед найпоширеніших типів кіберінцидентів домінують розповсюдження шкідливого програмного забезпечення, фішингові атаки, несанкціоновані підключення до систем, а також компрометація облікових записів і інформаційних ресурсів. Основною метою таких дій є отримання доступу до конфіденційної інформації, її викрадення, пошкодження або повне знищення інформаційних систем.

Важливим джерелом аналітичної інформації щодо сучасних викликів у сфері кібербезпеки є міжнародні дослідження, зокрема регулярні опитування керівників організацій, експертів з управління ризиками та інформаційної безпеки, які проводяться в межах заходів Всесвітнього економічного форуму. У рамках дослідження «Global Cybersecurity Outlook 2025» участь взяли представники різних галузей економіки, включаючи фінансовий сектор, енергетику, телекомунікації, медицину, виробництво та державне управління, з різних регіонів світу.

Результати цього дослідження свідчать про ускладнення глобального середовища кібербезпеки, що зумовлено поєднанням низки факторів, зокрема геополітичної напруги, стрімкого розвитку технологій, зростання рівня

кіберзлочинності, високої взаємозалежності інфраструктур і ланцюгів постачання, а також одночасного використання сучасних і застарілих систем захисту.

Геополітичні конфлікти суттєво впливають на оцінку ризиків у сфері кібербезпеки. Серед ключових загроз експерти виділяють кібершпигунство, а також втрату конфіденційної інформації, включаючи персональні дані. Зокрема, війна в Україні наочно демонструє вразливість критичної інфраструктури до комбінованих кібер- та фізичних атак.

Окремої уваги заслуговує проблема нерівномірного рівня кіберзахисту у різних регіонах світу. За результатами дослідження, 42% організацій у країнах Латинської Америки та 36% в Африці не впевнені у своїй готовності протистояти кіберзагрозам, тоді як у Європі та Північній Америці цей показник становить лише близько 15%.

Крім того, спостерігається суттєвий розрив між великими компаніями та малим і середнім бізнесом у сфері кіберстійкості. Малі підприємства стикаються з проблемами інформаційної безпеки у сім разів частіше, ніж великі організації, що значно підвищує їхню вразливість до кіберзлочинності.

Водночас висока інтегрованість сучасних економічних систем і ланцюгів постачання створює додаткові ризики. Навіть організації з високим рівнем захисту можуть зазнавати втрат через слабкі місця у системах своїх партнерів або контрагентів.

У звіті також підкреслюється, що новітні технології, такі як штучний інтелект, Інтернет речей та хмарні сервіси, з одного боку відкривають нові можливості для розвитку бізнесу, а з іншого — значно розширюють поверхню потенційних атак. Особливо небезпечним є використання інструментів штучного інтелекту кіберзлочинцями, що дозволяє підвищити швидкість, точність та масштабність атак, у тому числі спрямованих на злам баз даних і систем зберігання персональної інформації.

Аналітичний звіт «How Experts Think about Digital Privacy» містить результати глибинних інтерв'ю з провідними спеціалістами у сферах

кібербезпеки, права, цифрової етики та технологічного регулювання. У межах дослідження здійснено оцінку сучасного стану інформаційної приватності в умовах цифрового суспільства, а також окреслено ключові виклики, що постають у перспективі.

Поняття інформаційної приватності трактується як здатність особи самостійно визначати, хто, яким чином і з якою метою отримує доступ до її персональних даних. Вона ґрунтується на таких принципах, як контроль над інформацією, прозорість її обробки, добровільна згода та довіра між суб'єктом даних і організаціями, що їх використовують.

Експерти підкреслюють, що в сучасних умовах інформаційна приватність виходить за межі суто технічної проблематики і набуває комплексного характеру, охоплюючи технологічні, соціальні, економічні та політичні аспекти. Збільшення обсягів даних, активний розвиток штучного інтелекту та алгоритмічних систем, а також формування економіки, орієнтованої на дані, суттєво трансформують підходи до контролю над інформацією.

Особлива увага приділяється тому, що традиційні механізми отримання згоди суб'єктів даних втрачають ефективність у середовищах, де збір інформації відбувається постійно, часто без безпосередньої участі або усвідомленої взаємодії користувача. У звіті також зазначається, що навіть сучасні нормативно-правові інструменти не встигають адаптуватися до темпів розвитку технологій, що призводить до виникнення прогалин у системі захисту персональних даних [35, с. 113].

Важливим аспектом є етичний вимір проблеми. Зростає потреба у забезпеченні прозорості процесів збору та обробки даних, відповідального використання інформації, а також мінімізації ризиків дискримінації, які можуть виникати внаслідок автоматизованих рішень і алгоритмічної обробки даних.

У дослідженні виокремлено два основні підходи до оцінки майбутнього розвитку інформаційної приватності. Представники оптимістичного підходу

вважають, що посилення законодавчого регулювання, підвищення рівня обізнаності суспільства та впровадження технологій захисту приватності сприятимуть зміцненню балансу на користь користувачів.

Водночас прихильники більш песимістичного бачення наголошують на ризиках, пов'язаних із поширенням систем спостереження на основі штучного інтелекту, активним використанням біометричних даних, низьким рівнем обізнаності користувачів, а також опором бізнесу до посилення регуляторних вимог. У сукупності ці фактори можуть призвести до подальшого ослаблення захисту персональних даних.

Таким чином, сучасний стан інформаційної приватності характеризується як критичний етап розвитку, що вимагає переходу від формального дотримання нормативних вимог до реального забезпечення захисту даних. Подальша еволюція цієї сфери значною мірою залежатиме від узгоджених дій державних інституцій, бізнесу та суспільства щодо підвищення рівня відповідальності та пріоритетності захисту приватності.

Проведене дослідження свідчить, що проблема забезпечення захисту персональних даних працівників у системі управління персоналом, так само як і загальна проблема захисту персональної та чутливої інформації громадян у сучасному суспільстві, набуває особливої актуальності та суспільної значущості.

Аналіз динамічних змін у зовнішньому середовищі функціонування організацій, зокрема запровадження нових нормативно-правових актів у сфері захисту даних, а також активна цифровізація та впровадження інформаційних систем у HR-процеси, зумовлюють необхідність підвищення рівня професійних компетентностей. Це стосується як керівників і менеджерів, так і працівників організацій, а також потребує формування стратегічного підходу до управління інформаційною безпекою.

Результати опитувань експертів підтверджують, що захист персональних даних працівників дедалі більше інтегрується у загальну систему інформаційної безпеки та кіберстійкості організацій. Актуальність

цієї проблематики посилюється впливом глобальних геополітичних чинників, зокрема збройною агресією проти України, що підвищує ризики кіберзагроз для державних і приватних структур.

Згідно з результатами експертних оцінок щодо основних викликів кібербезпеки, пов'язаних із використанням генеративного штучного інтелекту (GenAI) у 2025 році, найбільше занепокоєння викликає розширення можливостей кіберзлочинців. Зокрема, 47% респондентів вказали на ризики, пов'язані з використанням GenAI для здійснення фішингових атак, створення шкідливого програмного забезпечення та поширення дипфейків.

Другим за значущістю викликом є ризик витоку даних, який відзначили 22% опитаних, що пов'язано з потенційним розкриттям персональної інформації через використання інструментів штучного інтелекту. Ще 17% респондентів звернули увагу на інші ризики, серед яких проблеми безпеки ланцюгів постачання програмного забезпечення, вразливості самих систем штучного інтелекту, а також правові питання, пов'язані з інтелектуальною власністю.

Крім того, 14% експертів відзначили ускладнення процесів управління кібербезпекою як окрему проблему, що зумовлено зростанням складності цифрових систем і необхідністю інтеграції нових технологій у вже існуючу інфраструктуру.

Отже, результати аналізу підтверджують, що сучасні виклики у сфері захисту персональних даних значною мірою пов'язані з розвитком цифрових технологій, зокрема штучного інтелекту, що вимагає від організацій впровадження комплексних підходів до забезпечення інформаційної безпеки.

1.2. Цифровізація кадрового діловодства як напрям розвитку сучасного менеджменту

Сучасні соціально-економічні трансформації змусили українські підприємства активно переходити до онлайн-формату ведення бізнесу та впроваджувати дистанційні форми організації праці для значної частини персоналу. Такі зміни стали новими та нетиповими для більшості працівників, що зумовило виникнення низки труднощів, пов'язаних із недостатнім досвідом віддаленої роботи, організацією трудового процесу та забезпеченням ефективної комунікації.

У зв'язку з цим актуалізується потреба у пошуку сучасних підходів, інструментів і технологічних рішень, які дозволяють ефективно реалізовувати HR-процеси в умовах дистанційної взаємодії. Одним із найбільш затребуваних інструментів у цьому контексті є HRM-системи, що забезпечують автоматизацію ключових функцій управління персоналом.

Аналіз функціональних можливостей сучасних HRM-рішень дає змогу узагальнити їх роль у забезпеченні автоматизації основних бізнес-процесів у сфері управління персоналом. До таких процесів належать управління продуктивністю працівників, кадрове планування та прогнозування потреб у персоналі, підбір і найм кадрів, оцінювання результатів діяльності, оформлення трудових відносин, нормування праці, облік та управління робочим часом [41, с. 182].

Попри значний науковий доробок вітчизняних і зарубіжних дослідників у сфері цифровізації бізнесу, дана проблематика залишається недостатньо вивченою. Зокрема, спостерігається фрагментарність наукових підходів до дослідження управління та розвитку дистанційних форм організації праці, а також забезпечення ефективності роботи персоналу в умовах цифрового середовища.

Якщо раніше процеси управління персоналом здебільшого здійснювалися у межах фізичного робочого простору, то сьогодні керівники

змушені організовувати виконання завдань у онлайн-середовищі. Це потребує нових управлінських компетентностей, яких часто бракує у практиці менеджменту.

У зв'язку з цим постає необхідність пошуку відповідей на ключові питання, зокрема щодо ефективної організації діяльності HR-підрозділів у дистанційному форматі, формування згуртованих віртуальних команд, підвищення продуктивності праці та досягнення високих результатів діяльності.

Водночас актуальним є визначення сучасних цифрових технологій і програмних рішень, які найбільш повно відповідають новим викликам і потребам організацій у сфері автоматизації процесів управління персоналом.

У сучасних умовах особливої актуальності набувають дослідження та порівняльний аналіз HRM-систем, представлених як на українському, так і на міжнародному ринках, а також оцінка ефективності їх впровадження в практику автоматизації бізнес-процесів управління персоналом.

Сучасна робоча сила стикається з низкою суттєвих викликів, зумовлених впливом глобальних кризових явищ, зокрема пандемії, яка суттєво трансформувала підходи до організації праці. HR-служби були змушені у короткі строки адаптуватися до нових умов, організовуючи діяльність персоналу в дистанційному форматі та забезпечуючи підтримку працівників, які працюють поза межами офісу.

Традиційні процедури підбору, відбору та адаптації персоналу перейшли у цифровий формат, що вимагало перегляду підходів до рекрутингу та управління людськими ресурсами. Крім того, багато підприємств були змушені застосовувати гнучкі режими роботи, включаючи скорочення робочого часу, що також вплинуло на ефективність управління персоналом. Одночасно загострилася проблема дефіциту кваліфікованих кадрів, що підвищує конкуренцію на ринку праці.

Досвід пандемії засвідчив, що сучасні HR-процеси мають бути цифровізованими для забезпечення їхньої гнучкості та адаптивності до змін

зовнішнього середовища. Зокрема, пошук роботи дедалі більше переміщується в онлайн-простір, де кандидати очікують наявності привабливих вакансій та активної цифрової присутності компаній.

Цифрова трансформація HR-процесів, що базується на використанні соціальних, мобільних, аналітичних і хмарних технологій, дозволяє суттєво скоротити обсяги паперового документообігу, підвищити оперативність прийняття управлінських рішень, зменшити трудомісткість процедур та забезпечити мобільність HR-функцій. У результаті це сприяє підвищенню рівня залученості персоналу, покращенню його утримання та загальному зростанню ефективності діяльності підприємства [40].

Результати міжнародних досліджень підтверджують важливість цифрової трансформації для розвитку HR-функції. Зокрема, за даними Gartner, 58% HR-директорів і керівників служб персоналу визначають трансформаційні процеси, включаючи цифрові, як пріоритетний напрям діяльності. Водночас результати опитування Dell Technologies, проведеного серед респондентів із 17 країн, свідчать, що 91% молодих фахівців враховують рівень розвитку цифрових технологій у компанії при виборі місця роботи. Крім того, 80% опитаних вважають, що автоматизація та цифрові інструменти сприяють формуванню більш справедливого та прозорого робочого середовища.

У найближчій перспективі цифрова трансформація суттєво змінить функціонування HR-підрозділів. Автоматизація дозволяє мінімізувати виконання рутинних операцій та зосередити увагу HR-менеджерів на стратегічних завданнях. Для забезпечення конкурентоспроможності фахівці з управління персоналом повинні розвивати цифрові компетентності та адаптуватися до нових умов цифрового середовища.

Окрім цього, важливою стає роль HR-менеджерів у формуванні корпоративної культури в дистанційному форматі. Вони відповідають за розвиток цифрової культури організації, встановлення норм та правил

внутрішніх комунікацій, а також підтримання ефективної взаємодії між працівниками в умовах віртуального середовища.

Аналізуючи вплив цифрової трансформації на HR-процеси, варто відзначити суттєві структурні зміни, що відбулися в сучасних організаціях. У постпандемічний період HR-менеджери опинилися перед подвійним викликом: необхідністю змінювати власні підходи до роботи та одночасно трансформувати організацію праці, робочі місця і кадрові процеси загалом.

Фахівці з управління персоналом, які володіють цифровими компетентностями, відкриті до використання новітніх платформ і здатні оперативно адаптуватися до змін, мають суттєвий вплив як на ефективність бізнесу, так і на професійний розвиток працівників. У цьому контексті особливого значення набуває обізнаність HR-менеджерів щодо сучасних цифрових інструментів автоматизації, які дозволяють підвищити результативність HR-процесів.

Цифровізація управління персоналом спричинила трансформацію багатьох напрямів діяльності, сформувавши нове цифрове робоче середовище. Вона змінила функціональне наповнення HR-підрозділів і бізнес-процеси шляхом активного впровадження інноваційних технологій, програмних продуктів та цифрових інструментів.

Зокрема, процес підбору персоналу значно спростився завдяки використанню автоматизованих рішень. Сучасні цифрові сервіси дозволяють HR-фахівцям централізовано обробляти резюме, автоматично розсилати повідомлення кандидатам, розміщувати вакансії на різних платформах, аналізувати відгуки та здійснювати первинний відбір претендентів. Розвиток спеціалізованого рекрутингового програмного забезпечення став важливим чинником еволюції цифрових HR-процесів.

У процесі взаємодії з кандидатами все більшого поширення набувають чат-боти, інтегровані в сучасні месенджери. Вони виконують функції первинного скринінгу, проводять базове інтерв'ю, відповідають на запитання кандидатів, фіксують їх відповіді та можуть ідентифікувати ключові критерії

відбору. У разі позитивного результату такі системи автоматично запрошують кандидатів до наступних етапів відбору, що дозволяє суттєво економити час HR-фахівців.



Рис. 1.2. Основні напрями впливу цифровізації на HR-процеси підприємства [33]

Суттєвих змін зазнали й процеси навчання та розвитку персоналу. Сучасні організації активно впроваджують цифрові платформи навчання, системи мікронавчання, удосконалені LMS та рішення на основі штучного інтелекту, які здатні рекомендувати навчальні програми, формувати індивідуальні траєкторії розвитку та автоматизувати процес навчання. Крім того, розвиваються платформи, що дозволяють працівникам самостійно створювати та обмінюватися навчальним контентом.

Важливим напрямом трансформації є підвищення рівня залученості працівників. Сучасні цифрові рішення забезпечують можливість проведення опитувань у режимі реального часу, аналізу настроїв персоналу, дослідження

внутрішніх комунікацій та збору зворотного зв'язку. Використання інструментів на основі штучного інтелекту дозволяє формувати рекомендації щодо покращення організаційної культури та управління персоналом.

Окремої уваги заслуговують системи самообслуговування персоналу, які орієнтовані на потреби працівників. Вони надають можливість отримувати доступ до інформації про оплату праці, подавати заявки на відпустку, переглядати кадрові дані та самостійно керувати окремими аспектами трудових відносин.

Зростання обсягів інформації та складності бізнес-процесів зумовлює необхідність використання інструментів для організації віддаленої співпраці. Такі системи забезпечують доступ до корпоративних ресурсів, дозволяють розмежовувати права доступу, координувати роботу над документами та здійснювати взаємодію між учасниками процесів у режимі реального часу.

Цифрові технології також сприяють переходу до безперервного управління продуктивністю працівників. Йдеться не про відмову від традиційного оцінювання, а про формування постійного процесу встановлення цілей, коучингу, оцінювання результатів та надання зворотного зв'язку, що відповідає сучасним вимогам гнучкого управління персоналом.

Незважаючи на стрімкі процеси цифрової трансформації, стратегічні цілі діяльності HR-підрозділів залишаються незмінними. Вони полягають у залученні висококваліфікованих і талановитих працівників, формуванні їхньої лояльності, забезпеченні високого рівня залученості та задоволеності працею, а також створенні сприятливого робочого середовища і можливостей для професійного та кар'єрного зростання.

Водночас суттєво змінюється роль HR-фахівців у процесі впровадження інновацій. Якщо раніше вони переважно виступали споживачами готових технологічних рішень, розроблених ІТ-компаніями, то сьогодні HR-менеджери дедалі частіше виступають ініціаторами змін і новаторами. Вони активно експериментують із новими підходами до управління

продуктивністю, удосконалюють стратегії навчання персоналу, впроваджують сучасні методи рекрутингу та розвитку людського капіталу.

Цифровізація бізнес-процесів у сфері управління персоналом значно прискорює розвиток HR-технологій та трансформацію підходів до управління командами. Вона передбачає широке використання сучасних цифрових інструментів, зокрема чат-ботів, соціальних мереж, мобільних застосунків, а також інтеграцію автоматизованих систем управління персоналом, зокрема HRM-систем.

HRM-системи являють собою комплексні автоматизовані рішення, що забезпечують інтеграцію та оптимізацію широкого спектра HR-процесів. Вони охоплюють усі етапи життєвого циклу працівника в організації — від адміністрування відпусток і лікарняних, нарахування заробітної плати до процесів адаптації, навчання, розвитку компетентностей і кар'єрного просування [20, с. 84].

Таким чином, цифровізація сприяла впровадженню сучасних інформаційних систем, які дозволяють централізовано управляти персоналом і автоматизувати ключові бізнес-процеси. Серед найбільш поширених рішень можна виокремити такі системи, як SAP HCM, Oracle HCM, Dynamics 365 Human Resources, Workable, Huma, PeopleForce, BambooHR, Zoho People та BAS ERP «Управління персоналом», які активно використовуються як у міжнародній, так і в українській практиці.

Сучасні HRM-системи суттєво відрізняються за своїми функціональними можливостями та рівнем складності. На ринку представлені як базові програмні продукти, орієнтовані на виконання окремих функцій, зокрема кадрового обліку, так і комплексні рішення, які забезпечують автоматизацію широкого спектра HR-процесів, включаючи рекрутинг, адаптацію персоналу, оцінювання результатів діяльності та навчання працівників. Такі системи можуть функціонувати як самостійні програмні продукти або бути інтегрованими в загальні системи автоматизації бізнесу.

При виборі HRM-системи особливу увагу необхідно приділяти її функціональним характеристикам та рівню захисту інформації. З точки зору функціоналу, кожна організація має визначити пріоритетні для себе напрями використання системи та обрати рішення, яке максимально відповідає її потребам.

Аналіз сучасних HRM-рішень свідчить, що найбільш повно вони охоплюють такі процеси управління персоналом, як підбір персоналу, управління продуктивністю, кадрове діловодство, розвиток трудової кар'єри, управління робочим часом, HR-аналітика та автоматизація основних кадрових процедур. Водночас окремі процеси реалізуються лише частково, зокрема кадрове планування, прогнозування потреб у персоналі, оцінювання працівників, визначення компетентнісних вимог, оформлення трудових відносин, адаптація персоналу, оперативне управління підрозділами, а також мотивація і стимулювання.

Разом із тим, існують напрями HR-діяльності, які недостатньо представлені у функціоналі більшості HRM-систем. До них належать аналіз робіт, управління навчанням персоналу, організація робочих місць, нормування праці, забезпечення безпеки праці та управління витратами на персонал.

Практика українських підприємств свідчить, що потенціал цифровізації HR-процесів використовується не повною мірою. Найбільш поширеними інструментами залишаються соціальні мережі, платформи для пошуку роботи, месенджери та електронна пошта, без яких реалізація HR-функцій фактично неможлива. Водночас частина працівників демонструє психологічні бар'єри щодо адаптації до нових цифрових умов, що пов'язано зі страхами, невпевненістю або упередженнями [20, с. 84].

Реалізація цифрової трансформації у сфері управління персоналом є важливим стратегічним завданням для підприємств. Однак оцінювання її ефективності залишається складним процесом, і багато організацій приділяють цьому недостатню увагу. У результаті фокус зміщується на

впровадження інновацій, тоді як питання визначення ключових показників ефективності (KPI) часто залишаються поза увагою.

Водночас саме наявність системи моніторингу та оцінювання дозволяє своєчасно виявляти недоліки у процесах цифровізації та коригувати управлінські рішення. Складність формування універсальних показників ефективності пояснюється тим, що рівень цифрової зрілості організацій суттєво відрізняється: одні лише розпочинають впровадження цифрових інструментів, інші модернізують застарілі системи, а деякі поступово інтегрують нові рішення у вже існуючу інфраструктуру.

Методи оцінювання ефективності цифровізації HR-процесів наразі недостатньо розроблені, що зумовлює актуальність подальших досліджень у цьому напрямі. Водночас для практичної діяльності підприємств важливо мати чітке уявлення про результати впровадження цифрових рішень.

Доцільними показниками оцінювання ефективності можуть бути, зокрема, співвідношення кількості придбаних ліцензій до фактичної кількості користувачів системи, що дозволяє оцінити рівень її впровадження. Наприклад, високий відсоток використання ліцензій свідчить про ефективну інтеграцію системи у діяльність підприємства, тоді як низький рівень використання вказує на проблеми у процесі цифровізації.

Важливим є також аналіз рівня автоматизації HR-процесів, який відображає масштаб впровадження системи, глибину її освоєння персоналом та повноту використання функціональних можливостей.

Крім того, ефективність цифровізації може оцінюватися через вплив на фінансові результати підприємства, зокрема зростання доходів або підвищення операційної ефективності. Окрему увагу слід приділяти оцінці зменшення трудомісткості HR-процесів, що може визначатися шляхом порівняння витрат часу до та після впровадження автоматизованих рішень.

Важливим показником є також рівень задоволеності користувачів HRM-системи. Успішність впровадження цифрових інструментів значною мірою залежить від готовності персоналу до їх використання, а також від

сформованої корпоративної культури, що враховує аспекти цифрової взаємодії та інформаційної безпеки.

На початкових етапах впровадження цифрових рішень особливу увагу необхідно приділяти підтримці працівників у процесі змін. Для цього доцільно здійснювати регулярний моніторинг рівня задоволеності користувачів, виявляти проблемні аспекти впровадження системи та забезпечувати ефективний зворотний зв'язок, зокрема шляхом проведення опитувань і створення каналів комунікації для оперативного вирішення проблем.

Цифровий HR інтегрує такі технологічні компоненти, як соціальні мережі, мобільні застосунки, аналітичні інструменти та хмарні сервіси, формуючи нову платформу для підвищення ефективності діяльності працівників і покращення досвіду кандидатів. Водночас, незважаючи на наявність різноманітних технологічних рішень, організації повинні самостійно розробляти комплексні стратегії цифрового управління персоналом, адаптовані до власних потреб і специфіки діяльності [31, с. 70].

Впровадження програмного забезпечення для цифровізації HR-процесів передбачає використання спеціалізованих платформ, які поєднують функціональні можливості різних категорій HR-систем. HRM-системи виступають інтегрованими модульними рішеннями, що забезпечують централізоване управління інформацією про персонал та охоплюють ключові функції управління людськими ресурсами.

Такі системи дозволяють організаціям ефективно управляти процесами підбору персоналу, оцінювання результативності працівників, їх навчання та розвитку, забезпечуючи при цьому оптимізацію бізнес-процесів і формування аналітичної звітності. Завдяки модульній структурі HRM-системи можуть бути гнучко налаштовані відповідно до потреб конкретної організації.

Потреба у впровадженні HRM-систем зумовлена низкою важливих чинників, серед яких особливе місце займає необхідність ефективного управління витратами на персонал, які становлять значну частину загальних витрат підприємства. Крім того, важливими є забезпечення ефективності

бізнес-процесів, дотримання вимог законодавства у сфері трудових відносин та підвищення якості управління людським капіталом.

Використання HRM-систем дозволяє вирішувати складні управлінські завдання, впроваджувати гнучкі підходи до нарахування заробітної плати та організації кадрового документообігу, а також підвищувати ефективність використання трудових ресурсів. У результаті впровадження таких систем підприємства отримують можливість зменшити часові витрати на виконання рутинних операцій, забезпечити збереження даних у хмарних середовищах та автоматизувати значну частину HR-процесів, що позитивно впливає на фінансові результати діяльності.

HRM-системи сьогодні належать до ключових корпоративних інформаційних рішень, які застосовуються організаціями різних масштабів і галузей економіки. Водночас питання розроблення універсальних підходів до оцінювання ефективності цифровізації управління персоналом залишається недостатньо опрацьованим, що визначає перспективність подальших наукових досліджень у цьому напрямі.

РОЗДІЛ 2

АНАЛІЗ СИСТЕМИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У ПРОЦЕСІ ЦИФРОВІЗАЦІЇ КАДРОВОГО ДІЛОВОДСТВА ПІДПРИЄМСТВА

2.1. Організаційно-управлінська характеристика системи кадрового діловодства підприємства

У сучасних умовах розвитку економіки, що характеризуються високим рівнем конкуренції, динамічністю ринкового середовища та активною цифровізацією бізнес-процесів, особливого значення набуває ефективне управління персоналом підприємства. Важливим елементом цієї системи виступає кадрове діловодство, яке забезпечує належне документальне оформлення трудових відносин, систематизацію інформації про працівників та створення інформаційної бази для прийняття управлінських рішень.

Об'єктом дослідження є товариство з обмеженою відповідальністю «МК БЕТОН», яке здійснює діяльність у сфері виробництва та постачання бетонної та залізобетонної продукції. Підприємство функціонує на регіональному ринку будівельних матеріалів, забезпечуючи потреби будівельних компаній, інфраструктурних об'єктів та приватних замовників. Специфіка діяльності підприємства зумовлює необхідність ефективного управління трудовими ресурсами, оскільки виробничі процеси потребують високого рівня організації праці, координації дій працівників та дотримання технологічних стандартів.

Організаційна структура ТОВ «МК БЕТОН» має лінійно-функціональний характер і включає керівництво підприємства, виробничі підрозділи, відділ постачання, відділ збуту, бухгалтерію, а також службу управління персоналом. Така структура забезпечує чіткий розподіл повноважень і відповідальності між підрозділами, що сприяє підвищенню ефективності управління підприємством у цілому.

Організаційну побудову системи управління персоналом ТОВ «МК БЕТОН» доцільно подати графічно на рис. 2.1.



Рис. 2.1. Організаційна структура системи управління персоналом ТОВ «МК БЕТОН» [22]

Система управління персоналом ТОВ «МК БЕТОН» є комплексною і охоплює всі ключові HR-процеси, зокрема планування потреби в персоналі, підбір і найм працівників, їх адаптацію, навчання та розвиток, оцінювання результатів діяльності, формування системи мотивації та стимулювання, а також управління трудовими відносинами. Важливою складовою цієї системи є кадрове діловодство, яке забезпечує документальне супроводження кожного з цих процесів.

Управління персоналом на підприємстві здійснюється із застосуванням адміністративних, економічних і соціально-психологічних методів. Адміністративні методи реалізуються через систему внутрішніх нормативних документів, наказів і розпоряджень. Економічні методи передбачають використання системи оплати праці, преміювання та матеріального стимулювання. Соціально-психологічні методи спрямовані на формування сприятливого соціально-психологічного клімату, підвищення рівня мотивації працівників та їх залученості до діяльності підприємства.

Отже, кадрове діловодство на ТОВ «МК БЕТОН» виступає не лише інструментом документального оформлення трудових відносин, але й важливою складовою системи управління персоналом, яка забезпечує ефективне функціонування підприємства. Основні складові системи кадрового діловодства ТОВ «МК БЕТОН» доцільно узагальнити в таблиці 2.1.

Таблиця 2.1

Основні елементи системи кадрового діловодства ТОВ «МК БЕТОН»**[22]**

Елемент системи	Зміст	Значення для управління персоналом
Нормативна база	КЗпП України, Закон України «Про захист персональних даних», внутрішні положення	Забезпечує правомірність кадрових процедур
Кадрова служба	Служба управління персоналом, бухгалтерія, керівництво	Виконує функції оформлення та обліку кадрів
Кадрові документи	Накази, трудові договори, особові картки, табелі, графіки відпусток	Формують інформаційну основу HR-процесів
Кадрові процеси	Прийняття, переведення, звільнення, облік часу, звітність	Забезпечують рух персоналу на підприємстві
Інформаційні засоби	Електронні таблиці, HR-модулі, бухгалтерські програми	Підвищують оперативність і точність роботи
Засоби захисту даних	Контроль доступу, резервне копіювання, антивірусний захист	Сприяють безпеці персональних даних

Кадрове діловодство на ТОВ «МК БЕТОН» організовано відповідно до чинного законодавства України, зокрема Кодексу законів про працю України, Закону України «Про захист персональних даних», а також інших нормативно-правових актів, що регламентують ведення кадрової документації.

Основним структурним підрозділом, відповідальним за ведення кадрового діловодства, є служба управління персоналом. У разі обмеженої чисельності персоналу функції кадрового діловодства можуть частково виконуватися бухгалтерією або безпосередньо керівництвом підприємства.

До основних функцій кадрового діловодства на підприємстві належать:

- оформлення прийняття працівників на роботу;
- ведення особових справ і облікових документів;
- підготовка наказів з кадрових питань;
- ведення обліку робочого часу;
- оформлення відпусток, відряджень та інших кадрових процедур;
- ведення кадрової звітності;

— забезпечення зберігання кадрових документів.

На підприємстві формується та ведеться повний пакет кадрової документації. Зокрема, оформлюються трудові договори або контракти, ведуться особові картки працівників, складається штатний розпис, формуються графіки відпусток, ведуться табелі обліку робочого часу, а також розробляються внутрішні положення та інструкції.

Процес кадрового діловодства має чітко визначену послідовність. Наприклад, при прийнятті працівника на роботу здійснюється збір необхідних документів (паспорт, ідентифікаційний код, документи про освіту), укладається трудовий договір, видається наказ про прийняття на роботу, вносяться відповідні записи до кадрових документів, формується особова справа працівника.

Особлива увага на підприємстві приділяється забезпеченню конфіденційності персональних даних працівників. Доступ до кадрових документів мають лише уповноважені особи. Використовуються організаційні заходи захисту інформації, зокрема розмежування доступу до документів, а також технічні засоби захисту електронних даних.

В умовах цифрової трансформації економіки ТОВ «МК БЕТОН» поступово впроваджує сучасні інформаційні технології у сфері управління персоналом. Цифровізація кадрового діловодства передбачає перехід від традиційних паперових носіїв інформації до електронних систем обробки та зберігання даних. Взаємозв'язок кадрових процесів, цифрових інструментів та засобів захисту персональних даних на ТОВ «МК БЕТОН» представлено на рис. 2.2.

На підприємстві використовуються програмні рішення для автоматизації кадрових процесів, що дозволяє значно підвищити ефективність роботи кадрової служби. Зокрема, застосовуються системи обліку персоналу, електронного документообігу, а також бухгалтерські програми, інтегровані з HR-функціями.

Кадрове діловодство ТОВ «МК БЕТОН»		
Напрями управління персоналу: прийняття на роботу •особові справи •табелі обліку часу •кадрова звітність •відпустки і відрядження	Цифровізація управління персоналу: електронні бази даних •HR-модулі •бухгалтерські програми •електронний документообіг	Захист персональних даних: контроль доступу •антивірусний захист •резервне копіювання •внутрішні політики безпеки

Рис. 2.2. Схема цифровізації кадрового діловодства та захисту персональних даних у ТОВ «МК БЕТОН»*

* Складено автором за даними [22]

Впровадження цифрових технологій забезпечує низку переваг, серед яких:

- скорочення часу на обробку кадрової інформації;
- підвищення точності та достовірності даних;
- оперативний доступ до інформації;
- можливість автоматичного формування звітності;
- підвищення прозорості управлінських процесів.

Водночас цифровізація кадрового діловодства супроводжується новими викликами, пов'язаними із забезпеченням безпеки персональних даних. Зокрема, зростає ризик несанкціонованого доступу до інформації, витоку даних, кібератак та інших загроз інформаційній безпеці.

З метою мінімізації таких ризиків на підприємстві впроваджуються сучасні засоби захисту інформації, включаючи системи контролю доступу, антивірусний захист, резервне копіювання даних, а також внутрішні політики безпеки інформації.

Кадрове діловодство на ТОВ «МК БЕТОН» виконує не лише облікову, а й важливу управлінську функцію. Воно забезпечує керівництво підприємства необхідною інформацією про персонал, що використовується для прийняття управлінських рішень.

На основі даних кадрового діловодства здійснюється аналіз кадрового складу підприємства, оцінка плинності кадрів, визначення потреби в персоналі, формування кадрового резерву, планування заходів щодо розвитку персоналу.

Ефективність кадрового діловодства залежить від рівня його організації, кваліфікації працівників кадрової служби, а також ступеня впровадження сучасних інформаційних технологій. Важливими принципами організації кадрового діловодства є системність, точність, оперативність, достовірність і конфіденційність інформації.

Управління кадровим діловодством передбачає розробку внутрішніх регламентів і процедур, контроль за дотриманням законодавства, організацію зберігання та архівування документів, а також постійне вдосконалення процесів управління персоналом.

Незважаючи на позитивні тенденції розвитку системи кадрового діловодства на ТОВ «МК БЕТОН», існують певні проблеми, що потребують вирішення. Серед них: недостатній рівень автоматизації окремих процесів, обмеженість фінансових ресурсів для впровадження сучасних інформаційних систем, ризики порушення безпеки персональних даних, а також недостатній рівень цифрових компетентностей працівників. Переваги цифровізації кадрового діловодства та наявні проблеми її впровадження на ТОВ «МК БЕТОН» наведено в таблиці 2.2.

Таблиця 2.2

Переваги та проблеми цифровізації кадрового діловодства ТОВ «МК БЕТОН»*

№ з/п	Характеристика	Прояв на підприємстві
1.	Скорочення часу обробки документів	Автоматизація кадрових операцій
2.	Точність інформації	Зменшення кількості технічних помилок
3.	Доступність даних	Швидкий доступ до кадрової інформації
4.	Ризик несанкціонованого доступу	Імовірність витоку персональних даних
5.	Обмежена автоматизація окремих процесів	Частина операцій виконується традиційно
6.	Недостатній рівень цифрових компетентностей	Потреба в навчанні працівників

* Складено автором за даними [22]

З метою підвищення ефективності системи кадрового діловодства доцільно впроваджувати сучасні HRM-системи, удосконалювати політику захисту персональних даних, підвищувати рівень цифрової грамотності працівників, інтегрувати кадрові інформаційні системи з іншими бізнес-процесами підприємства, а також здійснювати регулярний аудит інформаційної безпеки.

Важливою складовою ефективного функціонування системи кадрового діловодства на ТОВ «МК БЕТОН» є інформаційно-аналітичне забезпечення, яке передбачає збір, обробку, зберігання та використання даних про персонал підприємства. У сучасних умовах управління людськими ресурсами інформація виступає стратегічним ресурсом, що дозволяє приймати обґрунтовані управлінські рішення та забезпечувати конкурентоспроможність підприємства.

Інформаційна база кадрового діловодства підприємства формується з використанням різних джерел, зокрема первинних кадрових документів, електронних баз даних, результатів оцінювання персоналу, звітної документації та аналітичних матеріалів. Усі ці дані систематизуються та використовуються для аналізу кадрового потенціалу підприємства,

визначення ефективності використання трудових ресурсів, а також прогнозування потреби в персоналі.

На ТОВ «МК БЕТОН» інформаційно-аналітичне забезпечення кадрового діловодства реалізується через використання сучасних програмних засобів, які дозволяють автоматизувати процеси обліку персоналу, формування звітності та аналізу кадрових показників. Зокрема, застосовуються електронні таблиці, бухгалтерські програми та спеціалізовані HR-модулі, що забезпечують інтеграцію кадрової інформації з фінансовими та виробничими процесами підприємства.

Аналітична функція кадрового діловодства передбачає проведення регулярного аналізу таких показників, як чисельність персоналу, структура кадрів за віком, стажем, кваліфікацією, рівень плинності кадрів, рівень зайнятості та продуктивності праці. Результати такого аналізу використовуються для розробки заходів щодо оптимізації кадрової політики підприємства.

Особливе значення має використання аналітичних інструментів для оцінювання ефективності управління персоналом. Це дозволяє виявляти проблемні аспекти в організації праці, визначати резерви підвищення продуктивності та розробляти стратегії розвитку кадрового потенціалу підприємства.

Таким чином, інформаційно-аналітичне забезпечення кадрового діловодства на ТОВ «МК БЕТОН» є важливим інструментом підвищення ефективності управління персоналом та забезпечення стратегічного розвитку підприємства.

В умовах цифровізації кадрового діловодства особливої актуальності набуває проблема забезпечення захисту персональних даних працівників. На ТОВ «МК БЕТОН» ця діяльність здійснюється відповідно до вимог законодавства України та міжнародних стандартів у сфері інформаційної безпеки.

Система захисту персональних даних на підприємстві базується на комплексному підході, що включає організаційні, технічні та правові заходи. До організаційних заходів належать розробка внутрішніх політик і положень щодо обробки персональних даних, визначення відповідальних осіб за їх захист, а також проведення інструктажів і навчання працівників.

Технічні заходи передбачають використання сучасних засобів захисту інформації, таких як системи контролю доступу, антивірусне програмне забезпечення, засоби шифрування даних, резервне копіювання інформації та захист мережевої інфраструктури.

Правові заходи включають дотримання вимог законодавства щодо обробки персональних даних, укладення відповідних договорів із працівниками, а також забезпечення реалізації їх прав як суб'єктів персональних даних.

На підприємстві особлива увага приділяється забезпеченню конфіденційності інформації, що міститься в кадрових документах. Доступ до персональних даних обмежений колом уповноважених осіб, а всі операції з даними фіксуються та контролюються.

Водночас, враховуючи зростання кіберзагроз, підприємство стикається з необхідністю постійного вдосконалення системи захисту інформації. Це передбачає регулярне оновлення програмного забезпечення, проведення аудитів інформаційної безпеки, а також впровадження нових технологій захисту даних.

Таким чином, організація захисту персональних даних у системі кадрового діловодства ТОВ «МК БЕТОН» є важливим напрямом діяльності, який забезпечує не лише дотримання законодавства, але й підвищення рівня довіри працівників до підприємства.

Оцінка ефективності системи кадрового діловодства є необхідною умовою її вдосконалення та адаптації до сучасних вимог управління персоналом. На ТОВ «МК БЕТОН» така оцінка здійснюється на основі аналізу як кількісних, так і якісних показників.

До основних критеріїв ефективності кадрового діловодства належать: своєчасність оформлення кадрових документів, точність і достовірність інформації, рівень автоматизації процесів, дотримання вимог законодавства, а також рівень захищеності персональних даних.

Кількісні показники включають швидкість обробки документів, кількість помилок у кадровій документації, рівень плинності кадрів, а також витрати на ведення кадрового діловодства. Якісні показники відображають рівень задоволеності працівників умовами праці, ефективність комунікації між підрозділами, а також рівень довіри до системи управління персоналом.

Аналіз ефективності кадрового діловодства дозволяє виявити сильні та слабкі сторони системи, визначити напрями її вдосконалення та розробити відповідні управлінські рішення.

На ТОВ «МК БЕТОН» спостерігається позитивна динаміка розвитку системи кадрового діловодства, що пов'язано із впровадженням цифрових технологій та підвищенням рівня організації управлінських процесів. Водночас існує потреба у подальшій автоматизації процесів, удосконаленні системи захисту персональних даних та підвищенні кваліфікації працівників.

Оцінка ефективності кадрового діловодства є важливим інструментом управління, що дозволяє забезпечити його відповідність сучасним вимогам та підвищити ефективність діяльності підприємства в цілому.

Отже, кадрове діловодство на ТОВ «МК БЕТОН» є важливою складовою системи управління персоналом, яка забезпечує документальне оформлення трудових відносин, формує інформаційну базу для управління персоналом та сприяє підвищенню ефективності діяльності підприємства.

Сучасні процеси цифровізації створюють нові можливості для вдосконалення кадрового діловодства, однак водночас підвищують вимоги до забезпечення безпеки персональних даних. Це зумовлює необхідність впровадження комплексного підходу до управління кадровою інформацією, який поєднує організаційні, технічні та правові заходи захисту даних.

2.2. Оцінка рівня безпеки персональних даних та ризиків у цифровому HR-середовищі

У сучасних умовах цифрової трансформації управління персоналом питання захисту персональних даних працівників набуває не лише правового, а й виразного управлінського значення. Для підприємств виробничого профілю, діяльність яких пов'язана з поєднанням офісних, виробничих, транспортно-логістичних та облікових процесів, безпека персональних даних є складовою загальної системи організаційної стійкості. Саме до таких підприємств належить ТОВ «МК БЕТОН», яке функціонує у сфері виготовлення виробів із бетону для будівництва, виробництва бетонних розчинів, вантажного транспорту, оренди техніки та супутніх видів діяльності. Така багатoproфільність означає, що підприємство обробляє значний масив кадрової, фінансової, виробничої та логістичної інформації, частина якої прямо пов'язана з персональними даними працівників.

Для оцінювання рівня безпеки персональних даних у цифровому HR-середовищі ТОВ «МК БЕТОН» доцільно виходити з того, що кадрова інформація на підприємстві не існує ізольовано. Вона інтегрується в систему бухгалтерського обліку, внутрішнього документообігу, охорони праці, табелювання робочого часу, організації перевезень, медичних і санітарно-гігієнічних вимог, а також у процеси взаємодії з державними органами контролю. Наявність у підприємства реєстрації як платника податків і єдиного внеску, участь у перевірках, ліцензійна діяльність та публічні закупівлі означають, що обробка даних має регулярний, комплексний і багатоканальний характер.

Особливість оцінювання безпеки персональних даних у ТОВ «МК БЕТОН» полягає також у тому, що кадрове середовище підприємства має змішаний характер. З одного боку, це класичні HR-процеси: оформлення прийняття на роботу, ведення особових справ, кадрових наказів, табелів, графіків відпусток, обліку трудових переміщень. З іншого боку, на

підприємстві діє виробничо-транспортний компонент, що передбачає роботу водіїв, операторів спеціальної техніки, працівників виробничих майданчиків, технічного персоналу, керівників і бухгалтерських працівників. Така структура ускладнює контроль доступу до інформації, адже різні категорії персоналу мають різну потребу в доступі до документів, систем та облікових даних.

На базовому рівні рівень безпеки персональних даних у цифровому HR-середовищі визначається тим, наскільки підприємство здатне забезпечити конфіденційність, цілісність і доступність кадрової інформації. Конфіденційність означає обмеження доступу до персональних даних лише для уповноважених осіб. Цілісність передбачає захист інформації від спотворення, втрати або несанкціонованої зміни. Доступність означає можливість використання даних для законних кадрових і управлінських процедур без порушення режиму захисту. Для ТОВ «МК БЕТОН» ці три компоненти є особливо важливими, оскільки підприємство має порівняно невелику чисельність працівників — 40 осіб станом на 31.12.2025, а отже, кадрові функції часто концентруються в обмеженому колі посадових осіб, що підвищує значення правильної організації доступу і контролю.

Важливим індикатором середовища ризику є загальний профіль підприємства. Звіт фіксує 13 зареєстрованих видів діяльності, що саме по собі не є порушенням, однак у системі комплаєнс-аналізу позначається як фактор потенційного ризику. Окрім цього, у 2026 році щодо підприємства заплановано та/або проведено 6 перевірок, а в реєстрі перевірок згадані, зокрема, Державна служба України з питань праці та Державна екологічна інспекція України. Це свідчить про підвищену увагу контролюючих органів до операційного середовища підприємства, а відтак — про необхідність підвищених стандартів точності та захищеності кадрових і супровідних даних.

Таблиця 2.3

**Ключові компоненти оцінювання безпеки персональних даних у
цифровому HR-середовищі ТОВ «МК БЕТОН»***

Компонент оцінювання	Зміст	Прояв на ТОВ «МК БЕТОН»	Потенційний ризик
Конфіденційність	Обмеження доступу до персональних даних	Дані працівників обробляються кадровою службою, бухгалтерією, керівництвом	Надмірне коло доступу, витік інформації
Цілісність	Захист від зміни або спотворення даних	Використання електронних та паперових документів	Помилки внесення, дублювання, несанкціоноване редагування
Доступність	Можливість своєчасного доступу до даних	Дані потрібні для табелювання, звітності, нарахування оплати праці	Втрата доступу через технічний збій
Правомірність обробки	Відповідність законодавству	Оформлення трудових відносин, звітність, взаємодія з держорганами	Порушення вимог щодо згоди, зберігання та використання
Технічна захищеність	Наявність ІТ-засобів захисту	Електронний документообіг, бухгалтерські та облікові програми	Кібератаки, віруси, несанкціонований вхід
Організаційна керованість	Регламентація доступу та відповідальності	Концентрація HR-функцій у вузькому колі осіб	Людський фактор, недостатній контроль

* Складено автором за даними [22]

Оцінюючи безпеку персональних даних на підприємстві, слід враховувати і характер його матеріально-технічної бази. У звіті зафіксовано наявність спеціалізованого автотранспорту, зокрема бетонорозмішувачів, бетононасоса, вантажних автомобілів, а також ліцензії на міжнародні перевезення вантажів. Це означає, що в кадровому середовищі додатково циркулюють дані, пов'язані з водіями, допусками, кваліфікацією, режимами праці та відпочинку, відрядженнями, маршрутами, а іноді й медичними та безпековими аспектами. Розширення кола даних ускладнює систему захисту, оскільки вимагає точнішої класифікації інформації за рівнями доступу.

Одним із найбільш вірогідних ризиків для ТОВ «МК БЕТОН» є ризик несанкціонованого доступу до персональних даних унаслідок поєднання паперових і цифрових каналів обробки інформації. Для підприємств, які перебувають на етапі поступової цифровізації, характерним є паралельне використання особових справ, паперових наказів, табелів, первинної кадрової документації та електронних облікових систем. За відсутності чіткої моделі розмежування доступу це створює ризик, коли одна й та сама інформація міститься у кількох місцях, має різних відповідальних осіб і не контролюється централізовано.

Наступний істотний ризик пов'язаний з людським фактором. На практиці саме працівники є одночасно і носіями персональних даних, і користувачами систем, у яких ці дані обробляються. Низький рівень цифрової грамотності, недотримання правил зберігання паролів, передача доступів іншим особам, використання особистих пристроїв для службових операцій, надсилання документів через незахищені канали зв'язку — усе це формує підвищену вразливість HR-середовища. Для ТОВ «МК БЕТОН» цей ризик може бути посиленним через змішаний персональний склад, де не всі працівники мають однаковий досвід використання цифрових інструментів.

Не менш важливим є ризик фрагментарної автоматизації. Підприємство має ознаки активного розвитку: зростання імпорتنих операцій у 2024–2025 роках, покращення ринкових позицій, збільшення частки ринку та наявність тендерної активності. Це означає, що масштаби діяльності зростають, а разом із ними зростає й обсяг даних, які потребують системного адміністрування. Якщо цифровізація HR-процесів відстає від темпів розвитку бізнесу, виникає ситуація, коли частина операцій уже потребує автоматизації, а фактично обслуговується ручними або напівручними процедурами. Це призводить до дублювання даних, затримок в оновленні записів, підвищення ймовірності помилок і складності аудиту.

Як видно з рис. 2.3, ризики безпеки персональних даних у цифровому HR-середовищі ТОВ «МК БЕТОН» формуються не лише технічними

чинниками, а й організаційними, поведінковими та зовнішньорегуляторними обставинами.

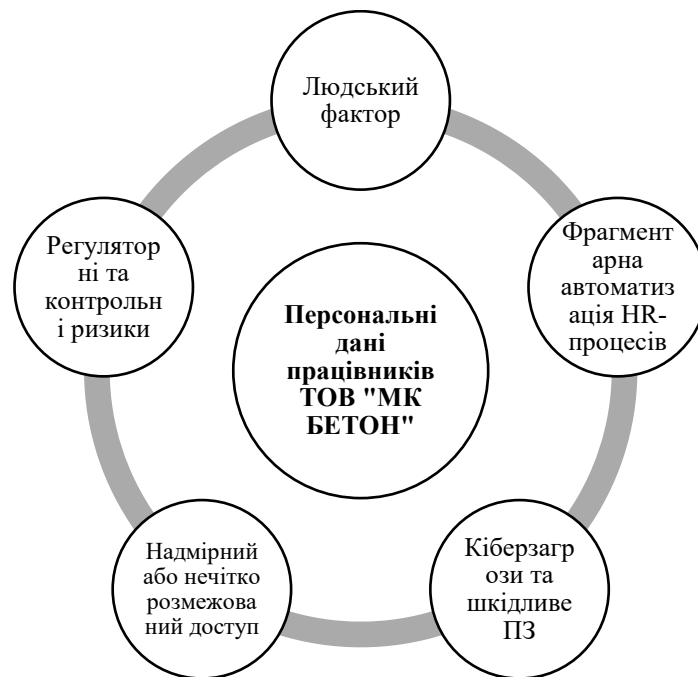


Рис. 2.3. Основні джерела ризиків безпеки персональних даних у цифровому HR-середовищі ТОВ «МК БЕТОН»*

* Складено автором за даними [22]

Для оцінювання загального рівня захищеності персональних даних доцільно також враховувати зовнішній регуляторний тиск. У випадку ТОВ «МК БЕТОН» він посилюється через наявність перевірок, публічних закупівель, ліцензійної діяльності, транспортної складової та взаємодії з податковими органами. За таких умов помилки в кадровому діловодстві або в захисті персональних даних можуть мати не лише внутрішні, а й зовнішні наслідки — від претензій працівників до ускладнення проходження перевірок чи підтвердження відповідності ліцензійним вимогам.

Окремий блок ризиків становлять кіберзагрози. Навіть якщо підприємство не є великою корпорацією, воно залишається потенційною ціллю фішингових атак, зараження шкідливим програмним забезпеченням, зламів поштових скриньок або компрометації бухгалтерських і кадрових

файлів. Для виробничого підприємства середнього масштабу найбільш імовірними є саме масові, а не таргетовані атаки: фальшиві листи від контрагентів, підроблені повідомлення від податкових органів, заражені вкладення, підміна реквізитів у листуванні. Небезпека полягає в тому, що через такі канали можуть бути викрадені документи з персональними даними працівників, копії паспортів, ідентифікаційні коди, інформація про зарплату, банківські реквізити чи дані про трудові переміщення.

Суттєвий ризик створює і відсутність повної сегментації доступу до інформації. Якщо одна й та сама особа має одночасно доступ до кадрових, бухгалтерських і окремих управлінських даних, то в разі помилки або компрометації такого облікового запису наслідки будуть комплексними. Для ТОВ «МК БЕТОН» це особливо актуально з огляду на відносно компактний масштаб підприємства, де кілька ключових осіб можуть поєднувати декілька функцій. У таких умовах необхідно чітко розмежовувати ролі: хто формує кадрові документи, хто перевіряє, хто затверджує, хто має право лише переглядати інформацію, а хто — вносити зміни.

Наявна у звіті інформація дає підстави оцінити середовище діяльності ТОВ «МК БЕТОН» як достатньо динамічне. У 2025 році підприємство мало 40 працівників, активні імпорتنі операції на рівні 4,6–4,7 млн грн, 3 виграні публічні закупівлі на 412 тис. грн, а також покращення ринкових позицій: місце на ринку — 97, частка ринку — 0,19 %, відносний приріст виручки за рік — 61,10 %. Така динаміка означає, що система HR-обліку й захисту даних не може залишатися статичною; вона повинна розвиватися синхронно з операційним зростанням підприємства.

Значущим для оцінки ризиків є також фінансовий аспект. За даними аналітичного блоку звіту, у 2025 році коефіцієнт автономії підприємства становив 34 %, поточна ліквідність — 71,8 %, чиста маржа — 4,5 %, рентабельність активів — 8 %, а MarketIndex — A/3.01. Це дає підстави стверджувати, що підприємство працює активно, але не в умовах надлишкового запасу ресурсів. Тому система безпеки персональних даних для

ТОВ «МК БЕТОН» має будуватися не на дорогих надмірних рішеннях, а на принципі економічно обґрунтованої достатності: критичні ризики повинні перекриватися в першу чергу, а заходи безпеки мають бути співмірними масштабом підприємства.

Таблиця 2.4

Оцінка основних ризиків безпеки персональних даних у цифровому HR-середовищі ТОВ «МК БЕТОН»*

Ризик	Імовірність	Потенційний вплив	Загальна оцінка
Несанкціонований доступ до кадрових даних	Висока	Високий	Критичний
Помилки персоналу при обробці даних	Висока	Середній	Значний
Витік даних через електронну пошту або месенджери	Середня	Високий	Значний
Втрата даних через технічний збій	Середня	Високий	Значний
Кібератаки на облікові системи	Середня	Високий	Значний
Недотримання правових вимог щодо персональних даних	Середня	Середній/високий	Значний
Надмірна концентрація доступу в окремих посадових осіб	Висока	Середній	Значний
Недостатній рівень цифрових компетентностей	Середня	Середній	Помірний

* Складено автором за даними [22]

У практичному вимірі це означає, що для ТОВ «МК БЕТОН» доцільно виділити кілька пріоритетів. По-перше, необхідно формалізувати політику обробки персональних даних працівників у межах внутрішнього положення. По-друге, слід запровадити матрицю доступу до кадрових даних, де кожна категорія користувачів матиме чітко визначений рівень прав. По-третє, потрібно забезпечити резервне копіювання електронних кадрових документів і захист робочих станцій, на яких обробляється HR-інформація. По-четверте, важливо проводити регулярні інструктажі для працівників, які мають доступ до персональних даних. По-п'яте, доцільно запровадити внутрішній аудит безпеки кадрових процесів не рідше одного разу на рік.

Важливо підкреслити, що оцінка рівня безпеки персональних даних не зводиться лише до констатації наявних проблем. Її метою є формування основи для подальшого вдосконалення цифрового HR-середовища. У випадку

ТОВ «МК БЕТОН» можна зробити висновок, що підприємство має базові передумови для організації належного захисту: чіткий юридичний статус, формалізовану структуру власності, визначених уповноважених осіб, активну господарську діяльність, легальний транспортний і ліцензійний профіль, відсутність інформації про санкційні списки та списки спостереження. Водночас поєднання зростання бізнес-активності, розширення цифрових операцій, наявності перевірок і фрагментарності кадрових процесів формує середовище підвищеного інформаційного ризику.

Отже, рівень безпеки персональних даних у цифровому HR-середовищі ТОВ «МК БЕТОН» можна оцінити як середній із тенденцією до підвищення ризиків у разі подальшого розширення діяльності без належного посилення внутрішніх контрольних механізмів. Основними загрозами виступають несанкціонований доступ до кадрових даних, людський фактор, фрагментарна автоматизація, недостатня сегментація доступу та кіберризика. Водночас ці ризики є керованими за умови впровадження системного підходу до інформаційної безпеки, який поєднуватиме організаційні, технічні та правові інструменти захисту.

РОЗДІЛ 3

УДОСКОНАЛЕННЯ СИСТЕМИ УПРАВЛІННЯ БЕЗПЕКОЮ ПЕРСОНАЛЬНИХ ДАНИХ У КАДРОВОМУ ДІЛОВОДСТВІ

3.1. Формування організаційно-управлінських механізмів забезпечення захисту персональних даних

У сучасних умовах цифровізації управління персоналом питання формування ефективних організаційно-управлінських механізмів забезпечення захисту персональних даних набуває стратегічного значення для підприємств. Інформація про працівників, яка формується, обробляється та зберігається у процесі кадрового діловодства, є важливим ресурсом, що забезпечує функціонування системи управління персоналом, однак водночас виступає об'єктом підвищених ризиків, пов'язаних із витоком, спотворенням або несанкціонованим використанням даних.

Для підприємства виробничого профілю, яким є ТОВ «МК БЕТОН», проблема захисту персональних даних має комплексний характер. Це зумовлено поєднанням традиційних кадрових процедур із цифровими інструментами обробки інформації, а також багатофункціональністю діяльності підприємства, що охоплює виробничі, транспортно-логістичні, управлінські та облікові процеси. У таких умовах формування організаційно-управлінських механізмів захисту персональних даних має ґрунтуватися на системному підході, який передбачає інтеграцію правових, організаційних, технічних та кадрових заходів.

Передусім, слід зазначити, що організаційно-управлінський механізм захисту персональних даних являє собою сукупність взаємопов'язаних елементів, які забезпечують створення, функціонування та розвиток системи захисту інформації на підприємстві. До таких елементів належать нормативно-правова база, організаційна структура управління, внутрішні регламенти, система контролю, інформаційні технології, а також кадровий потенціал, що забезпечує реалізацію політики захисту даних.

Формування такого механізму на ТОВ «МК БЕТОН» має починатися з визначення базових принципів захисту персональних даних. До них належать законність обробки інформації, цільове використання даних, мінімізація обсягу оброблюваної інформації, обмеження строків зберігання, забезпечення конфіденційності, цілісності та доступності даних. Дотримання цих принципів створює основу для побудови ефективної системи управління інформаційною безпекою.

Одним із ключових етапів формування організаційно-управлінського механізму є розроблення та впровадження внутрішніх нормативних документів, які регламентують порядок обробки персональних даних. На ТОВ «МК БЕТОН» доцільно передбачити створення таких документів, як положення про обробку та захист персональних даних, політика інформаційної безпеки, інструкції для працівників щодо роботи з персональними даними, регламент доступу до інформаційних ресурсів, а також порядок реагування на інциденти інформаційної безпеки.

Важливим складником організаційного механізму є визначення відповідальних осіб за захист персональних даних. У структурі підприємства доцільно закріпити функції контролю за обробкою персональних даних за службою управління персоналом у взаємодії з бухгалтерією та керівництвом підприємства. При цьому необхідно чітко розмежувати повноваження щодо доступу до інформації, її обробки, зберігання та передачі (табл. 3.1).

Наступним важливим аспектом є формування ефективної системи управління доступом до персональних даних. Для ТОВ «МК БЕТОН» це означає впровадження принципу диференційованого доступу, відповідно до якого кожен працівник має доступ лише до тієї інформації, яка необхідна для виконання його посадових обов'язків. Такий підхід дозволяє мінімізувати ризики витоку інформації та забезпечує контроль за використанням персональних даних.

Таблиця 3.1

**Основні елементи організаційно-управлінського механізму захисту
персональних даних на ТОВ «МК БЕТОН»***

Елемент	Характеристика	Практичне значення
Нормативне забезпечення	Внутрішні положення, інструкції, політики	Формує правову основу захисту
Організаційна структура	Розподіл функцій між підрозділами	Забезпечує контроль і відповідальність
Інформаційні технології	HR-системи, облікові програми	Автоматизує процеси
Контроль і аудит	Внутрішній моніторинг і перевірки	Виявляє порушення
Навчання персоналу	Інструктажі, підвищення кваліфікації	Знижує ризики помилок
Система реагування	Алгоритми дій при інцидентах	Мінімізує наслідки порушень

* Складено автором самостійно.

Наступним важливим аспектом є формування ефективної системи управління доступом до персональних даних. Для ТОВ «МК БЕТОН» це означає впровадження принципу диференційованого доступу, відповідно до якого кожен працівник має доступ лише до тієї інформації, яка необхідна для виконання його посадових обов'язків. Такий підхід дозволяє мінімізувати ризики витоку інформації та забезпечує контроль за використанням персональних даних.

У межах цього механізму доцільно впровадити рольову модель доступу, яка передбачає визначення категорій користувачів (керівництво, кадрова служба, бухгалтерія, виробничий персонал) та встановлення відповідних прав доступу для кожної категорії. Це дозволяє систематизувати інформаційні потоки та забезпечити прозорість управлінських процесів.

Важливу роль у забезпеченні захисту персональних даних відіграє цифровізація кадрового діловодства. Використання сучасних інформаційних систем дозволяє автоматизувати процеси обробки даних, зменшити вплив людського фактора, забезпечити контроль за змінами інформації та підвищити рівень її захищеності. Однак цифровізація також створює нові ризики,

пов'язані з кіберзагрозами, що потребує впровадження додаткових заходів безпеки.

Суттєвим напрямом формування організаційного механізму є створення системи внутрішнього контролю за дотриманням вимог щодо захисту персональних даних. На ТОВ «МК БЕТОН» доцільно впровадити регулярний моніторинг стану кадрового діловодства, перевірку правильності оформлення документів, аналіз доступу до інформації, а також оцінювання рівня інформаційної безпеки.

Не менш важливим є формування культури захисту інформації серед працівників. Це передбачає проведення навчання, інструктажів, роз'яснювальної роботи щодо правил обробки персональних даних, відповідальності за їх порушення та наслідків недотримання вимог безпеки. Для підприємства з чисельністю близько 40 працівників це є особливо актуальним, оскільки людський фактор відіграє ключову роль у забезпеченні інформаційної безпеки.

Таблиця 3.2

**Основні напрями щодо забезпечення захисту персональних даних на
ТОВ «МК БЕТОН»***

Напрямок	Зміст	Наслідок
Розробка політик	Визначення правил обробки даних	Підвищення правової визначеності
Контроль доступу	Впровадження ролей і прав	Зниження ризику витоку
Навчання персоналу	Проведення інструктажів	Підвищення відповідальності
Автоматизація процесів	Впровадження HR-систем	Зменшення помилок
Аудит безпеки	Перевірка відповідності	Виявлення слабких місць
Резервне копіювання	Захист від втрати даних	Забезпечення безперервності

* Складено автором самостійно.

Особливого значення набуває впровадження системи реагування на інциденти інформаційної безпеки. На підприємстві повинні бути визначені алгоритми дій у випадку витоку даних, втрати інформації, кібератак або інших порушень. Це дозволяє оперативно мінімізувати негативні наслідки та

забезпечити відновлення нормального функціонування системи управління персоналом.

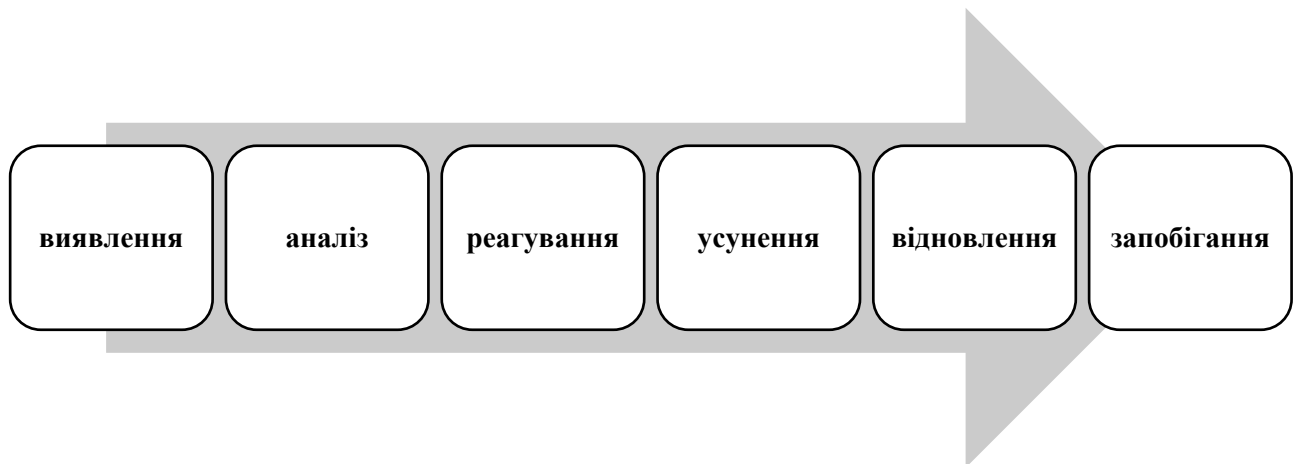


Рис. 3.1. Процес управління інцидентами безпеки персональних даних*

* Складено автором самостійно.

Отже, формування організаційно-управлінських механізмів забезпечення захисту персональних даних на ТОВ «МК БЕТОН» є комплексним процесом, що охоплює всі аспекти діяльності підприємства. Ефективність цього процесу залежить від узгодженості дій усіх підрозділів, рівня цифровізації, якості управлінських рішень та рівня підготовки персоналу.

Узагальнюючи, можна зробити висновок, що впровадження системного підходу до захисту персональних даних дозволить підвищити ефективність управління персоналом, забезпечити відповідність законодавчим вимогам, мінімізувати ризики та створити передумови для сталого розвитку підприємства.

3.2. Впровадження сучасних цифрових та управлінських рішень у сфері інформаційної безпеки персоналу

У сучасних умовах цифрової трансформації економіки питання забезпечення інформаційної безпеки персоналу стає одним із ключових напрямів удосконалення системи управління підприємством. Стрімкий розвиток інформаційних технологій, розширення використання цифрових платформ у кадровому діловодстві, автоматизація бізнес-процесів і зростання обсягів обробки персональних даних обумовлюють необхідність впровадження сучасних цифрових та управлінських рішень, спрямованих на мінімізацію інформаційних ризиків.

Для ТОВ «МК БЕТОН», яке функціонує у сфері виробництва бетонної продукції, логістики та супутніх послуг, інформаційна безпека персоналу має особливе значення у зв'язку з поєднанням виробничих і адміністративних процесів. Підприємство обробляє широкий спектр персональних даних: від стандартних кадрових відомостей до інформації про кваліфікацію працівників, режим роботи, оплату праці, участь у виробничих процесах, транспортних операціях і зовнішніх господарських відносинах. У таких умовах впровадження сучасних рішень у сфері інформаційної безпеки є необхідною передумовою підвищення ефективності управління персоналом і забезпечення стабільності діяльності підприємства.

Одним із базових напрямів удосконалення інформаційної безпеки є цифровізація кадрових процесів. Перехід від паперових форм ведення кадрового діловодства до електронних систем управління персоналом дозволяє забезпечити централізоване зберігання даних, підвищити їх доступність і контрольованість, а також мінімізувати ризики втрати або пошкодження інформації. Для ТОВ «МК БЕТОН» доцільним є впровадження HRM-систем, які забезпечують автоматизацію основних кадрових процесів: облік персоналу, ведення особових справ, табелювання робочого часу,

нарахування заробітної плати, управління відпустками, оцінювання персоналу та планування його розвитку.

Важливим аспектом впровадження цифрових рішень є інтеграція HRM-систем із бухгалтерськими та управлінськими програмами. Це дозволяє забезпечити єдність інформаційного простору підприємства, уникнути дублювання даних і підвищити точність управлінських рішень. Для підприємства середнього масштабу, яким є ТОВ «МК БЕТОН», така інтеграція має особливе значення, оскільки дозволяє оптимізувати використання ресурсів і підвищити ефективність управління.

Таблиця 3.3

Сучасні цифрові рішення у сфері інформаційної безпеки персоналу

[32, с. 45]

Рішення	Характеристика	Переваги для підприємства
HRM-системи	Автоматизація кадрових процесів	Централізація даних, зниження помилок
ERP-системи	Інтеграція бізнес-процесів	Єдиний інформаційний простір
Системи контролю доступу	Розмежування прав користувачів	Захист від несанкціонованого доступу
Хмарні технології	Зберігання даних на віддалених серверах	Безпека та резервування
Антивірусні програми	Захист від шкідливого ПЗ	Зниження кіберризиків
Системи резервного копіювання	Збереження даних	Захист від втрати інформації

Важливим елементом забезпечення інформаційної безпеки є впровадження систем управління доступом до інформації. Для ТОВ «МК БЕТОН» це означає використання багаторівневих механізмів автентифікації, впровадження ролей користувачів, обмеження доступу до персональних даних відповідно до посадових обов'язків. Використання таких інструментів дозволяє знизити ризики витоку інформації та забезпечити контроль за її використанням.

Суттєвим напрямом є також використання сучасних засобів кіберзахисту. До них належать антивірусні програми, системи виявлення вторгнень, захист електронної пошти, шифрування даних, багатофакторна автентифікація. Для підприємства важливо не лише впровадити ці

інструменти, а й забезпечити їх регулярне оновлення та адаптацію до нових загроз.

Не менш важливим є впровадження управлінських рішень, спрямованих на підвищення рівня інформаційної безпеки. До таких рішень належать розроблення стратегій інформаційної безпеки, формування політик захисту персональних даних, визначення відповідальних осіб, створення системи внутрішнього контролю та аудиту.

Для ТОВ «МК БЕТОН» доцільно сформувати комплексну стратегію інформаційної безпеки, яка передбачає визначення цілей, завдань, ресурсів і механізмів реалізації заходів захисту. Така стратегія повинна бути інтегрована в загальну стратегію розвитку підприємства та враховувати специфіку його діяльності.

Важливим напрямом є формування культури інформаційної безпеки серед працівників. Це передбачає проведення регулярних навчань, інструктажів, тренінгів, спрямованих на підвищення обізнаності працівників щодо правил роботи з персональними даними, кіберзагроз і способів їх уникнення. Для підприємства з невеликою чисельністю персоналу це є одним із найбільш ефективних інструментів забезпечення безпеки.

Важливим елементом є створення системи моніторингу та реагування на інциденти інформаційної безпеки. Для ТОВ «МК БЕТОН» це означає впровадження процедур виявлення, аналізу та усунення інцидентів, а також розроблення планів відновлення діяльності у разі порушення безпеки.

Окрему увагу слід приділити використанню хмарних технологій. Вони дозволяють забезпечити надійне зберігання даних, доступ до них з різних пристроїв, автоматичне резервне копіювання та високий рівень захисту. Однак використання хмарних сервісів потребує ретельного вибору постачальників і дотримання вимог безпеки.

Впровадження сучасних цифрових та управлінських рішень у сфері інформаційної безпеки персоналу дозволяє ТОВ «МК БЕТОН» досягти таких результатів: підвищення рівня захищеності персональних даних, зниження

ризиків витоку інформації, підвищення ефективності управління персоналом, забезпечення відповідності законодавчим вимогам, створення умов для сталого розвитку підприємства.

Узагальнюючи, слід зазначити, що ефективна система інформаційної безпеки персоналу має будуватися на поєднанні сучасних цифрових технологій і управлінських підходів. Для ТОВ «МК БЕТОН» це означає необхідність комплексного підходу, що включає автоматизацію кадрових процесів, впровадження систем захисту інформації, розвиток організаційної структури управління, підвищення кваліфікації персоналу та постійне вдосконалення системи безпеки.

Разом із тим, процес впровадження сучасних цифрових та управлінських рішень у сфері інформаційної безпеки персоналу не може бути одномоментним. Для ТОВ «МК БЕТОН» він має здійснюватися поетапно, із врахуванням масштабів підприємства, наявних фінансових ресурсів, рівня технічного забезпечення та готовності персоналу до організаційних змін. Практика свідчить, що навіть найбільш досконалі програмні засоби не забезпечують належного результату без відповідного управлінського супроводу, належної організації внутрішніх процесів та підтримки з боку керівництва. Саме тому цифрові рішення у сфері безпеки персональних даних повинні впроваджуватися у взаємозв'язку із загальною політикою розвитку підприємства та системою управління персоналом.

На першому етапі доцільним є проведення внутрішньої діагностики стану інформаційної безпеки персоналу на підприємстві. Така діагностика має включати аналіз наявних каналів обробки персональних даних, виявлення слабких місць у кадровому діловодстві, оцінювання технічного стану інформаційної інфраструктури, а також визначення рівня готовності працівників до роботи в цифровому середовищі. Для ТОВ «МК БЕТОН» така діагностика є особливо важливою, оскільки підприємство поєднує виробничі, логістичні, бухгалтерські та кадрові процеси, а отже, інформаційні потоки є багатоканальними та потребують узгодженого контролю.

Результати діагностики мають стати основою для формування дорожньої карти цифрової трансформації у сфері інформаційної безпеки персоналу. У межах цієї дорожньої карти необхідно визначити першочергові заходи, строки їх реалізації, відповідальних осіб, необхідні ресурси та критерії оцінки результативності. Такий підхід дозволить уникнути фрагментарності у впровадженні змін та забезпечить системність управлінських дій. Для ТОВ «МК БЕТОН» це означає, що цифровізація кадрових процесів має бути підпорядкована чітко визначеним управлінським цілям: підвищенню рівня захисту персональних даних, зменшенню кількості помилок у кадровій документації, прискоренню доступу до інформації та посиленню контролю за використанням даних.

Важливим напрямом є впровадження принципу безперервності захисту інформації. На практиці це означає, що безпека персональних даних повинна забезпечуватися на всіх етапах їх життєвого циклу — від моменту збору інформації про працівника до її архівування або знищення після завершення строків зберігання. У діяльності ТОВ «МК БЕТОН» це стосується документів про прийняття на роботу, трудових договорів, наказів, табелів обліку робочого часу, даних щодо оплати праці, відпусток, лікарняних, інформації про кваліфікацію, навчання та внутрішні переміщення працівників. На кожному з цих етапів мають діяти чіткі регламенти обробки інформації, які виключають несанкціонований доступ або втрату даних.

Окремої уваги заслуговує питання інтеграції інформаційної безпеки з кадровою політикою підприємства. На ТОВ «МК БЕТОН» кадрова політика повинна враховувати не лише потребу у забезпеченні підприємства трудовими ресурсами, а й вимоги до конфіденційності та безпечної обробки персональних даних. Це означає, що ще на етапі відбору та прийняття працівників доцільно приділяти увагу їх цифровим компетентностям, здатності дотримуватися внутрішніх процедур безпеки, відповідальності при роботі з документами та електронними системами. Таким чином,

інформаційна безпека персоналу має інтегруватися в загальну систему формування трудової дисципліни та корпоративної культури.

Не менш важливим є впровадження системи періодичного оновлення програмного забезпечення та технічної інфраструктури. Для багатьох підприємств основною проблемою є не відсутність цифрових інструментів як таких, а використання застарілих програмних продуктів, що не відповідають сучасним вимогам захисту інформації. Для ТОВ «МК БЕТОН» це означає необхідність регулярного оновлення облікових систем, антивірусних програм, операційних середовищ, засобів резервного копіювання та захисту електронної пошти. Такий підхід дозволяє мінімізувати ризики використання вразливостей, які можуть бути використані зловмисниками для доступу до персональних даних працівників.

Важливо також забезпечити резервування інформаційних ресурсів, які використовуються у кадровому діловодстві. Резервне копіювання даних є одним із базових, але водночас найбільш ефективних інструментів інформаційної безпеки. Для ТОВ «МК БЕТОН» доцільно організувати регулярне створення резервних копій кадрових документів, баз даних, електронних реєстрів та інших важливих масивів інформації. При цьому важливо, щоб резервні копії зберігалися окремо від основних робочих середовищ та були захищені від несанкціонованого доступу. Це дозволить підприємству забезпечити відновлення даних у випадку технічного збою, вірусного зараження, випадкового видалення інформації або інших позаштатних ситуацій.

Суттєвим напрямом удосконалення є також запровадження практики внутрішнього тестування безпеки. Йдеться про періодичну перевірку того, наскільки ефективно діють політики захисту персональних даних, чи правильно працівники реагують на потенційно небезпечні електронні листи, чи дотримуються встановлених правил доступу до інформації, наскільки швидко виявляються і усуваються помилки у роботі з персональними даними. Для ТОВ «МК БЕТОН» така практика може здійснюватися у формі внутрішніх

аудитів, контрольних перевірок, тестувань знань працівників або моделювання типових інцидентів інформаційної безпеки.

Значну роль у забезпеченні безпеки персоналу відіграє побудова ефективної системи внутрішніх комунікацій. У цифровому HR-середовищі працівники мають чітко розуміти, до кого звертатися у разі виявлення проблеми, як повідомляти про підозрілі дії, куди передавати інформацію про технічні збої чи інциденти безпеки. Для ТОВ «МК БЕТОН» важливо створити такі канали комунікації, які будуть простими, швидкими та зрозумілими для всіх категорій персоналу — як адміністративно-управлінських працівників, так і працівників виробничої та транспортної сфери. Це сприятиме формуванню атмосфери відповідальності та залученості працівників до забезпечення інформаційної безпеки.

Ще одним важливим напрямом є впровадження сучасних методів аналітики у сфері управління ризиками інформаційної безпеки. Використання цифрових інструментів дозволяє не лише фіксувати події, пов'язані з доступом до даних, а й аналізувати закономірності використання інформації, виявляти аномальні дії, формувати прогнози щодо потенційних загроз. Для ТОВ «МК БЕТОН» впровадження таких аналітичних інструментів може стати важливим елементом превентивного управління ризиками, оскільки дає змогу своєчасно реагувати на небезпечні тенденції ще до того, як вони призведуть до реальних втрат.

Перспективним для підприємства є і впровадження принципу персоніфікованої відповідальності за роботу з персональними даними. Практика показує, що колективна відповідальність часто призводить до розмитості повноважень, коли жоден працівник не відчуває себе безпосередньо відповідальним за порушення. Натомість чітке визначення зон відповідальності, фіксація прав доступу, закріплення конкретних функцій за окремими посадовими особами сприяють посиленню дисципліни та підвищують рівень контролю за обробкою персональних даних. Для ТОВ «МК БЕТОН» такий підхід є доцільним у зв'язку з необхідністю чіткого

розмежування повноважень між службою персоналу, бухгалтерією, керівниками підрозділів та працівниками, які мають доступ до електронних систем.

У контексті цифрової економіки важливо також враховувати репутаційний аспект інформаційної безпеки. Захист персональних даних працівників є не лише внутрішньою функцією підприємства, а й фактором його ділової репутації. Для ТОВ «МК БЕТОН» забезпечення належного рівня інформаційної безпеки сприятиме зміцненню довіри з боку працівників, партнерів, клієнтів і контролюючих органів. У сучасному бізнес-середовищі здатність підприємства гарантувати безпечне поводження з даними дедалі частіше сприймається як показник його управлінської зрілості та надійності.

Отже, подальше впровадження сучасних цифрових та управлінських рішень у сфері інформаційної безпеки персоналу на ТОВ «МК БЕТОН» має здійснюватися комплексно та послідовно. Йдеться не лише про технічне оновлення програмного середовища, а й про глибшу трансформацію управлінських підходів, організаційної культури та кадрової політики підприємства. Лише за умов поєднання цифрових інструментів, чітких управлінських регламентів, системи контролю, безперервного навчання персоналу та орієнтації на превентивне управління ризиками можна забезпечити високий рівень захисту персональних даних і створити надійне цифрове HR-середовище. Це, у свою чергу, стане важливим чинником підвищення ефективності управління персоналом, зміцнення конкурентних позицій підприємства та забезпечення його стійкого розвитку в умовах зростаючих інформаційних викликів.

ВИСНОВКИ

У результаті проведеного дослідження встановлено, що проблема забезпечення безпеки персональних даних у процесі цифровізації кадрового діловодства є надзвичайно актуальною в умовах сучасних трансформацій управління персоналом. Цифровізація HR-процесів, з одного боку, сприяє підвищенню ефективності діяльності організацій, автоматизації кадрових процедур та покращенню якості управлінських рішень, а з іншого — супроводжується зростанням ризиків, пов'язаних із захистом інформації, що потребує формування комплексних підходів до забезпечення інформаційної безпеки. Підсумовуючи дослідження можемо зробити наступні висновки:

1. В умовах подальшого розвитку цифрової економіки питання захисту персональних даних набуватиме ще більшої ваги, оскільки обсяги інформації постійно зростають, а способи її обробки стають дедалі складнішими. Це зумовлює необхідність переходу від реактивної моделі забезпечення безпеки до проактивної, яка передбачає попередження загроз ще на етапі їх виникнення. Для підприємств, зокрема ТОВ «МК БЕТОН», це означає необхідність постійного моніторингу інформаційного середовища, впровадження сучасних систем аналізу ризиків, а також формування культури безпечної поведінки працівників у цифровому просторі. Важливим є також посилення ролі управлінського персоналу у питаннях інформаційної безпеки, оскільки саме від стратегічних рішень керівництва залежить ефективність функціонування всієї системи захисту даних.

2. Забезпечення безпеки персональних даних має розглядатися не лише як обов'язок підприємства відповідно до законодавчих вимог, а як важливий елемент його конкурентної стратегії. У сучасних умовах рівень захисту інформації дедалі частіше стає критерієм оцінки надійності підприємства з боку партнерів, інвесторів і працівників. Саме тому інтеграція механізмів інформаційної безпеки у всі управлінські процеси дозволяє не лише мінімізувати ризики, а й створює додаткові переваги для розвитку підприємства. Таким чином, подальше вдосконалення системи захисту

персональних даних у цифровому кадровому діловодстві є стратегічним завданням, реалізація якого сприятиме забезпеченню стабільності, ефективності та довгострокової конкурентоспроможності організації.

3. У роботі розкрито сутність персональних даних як важливого інформаційного ресурсу в системі управління персоналом. Встановлено, що персональні дані працівників охоплюють широкий спектр відомостей — від ідентифікаційних до професійних і соціально-економічних характеристик — і відіграють ключову роль у забезпеченні ефективності HR-процесів. Їх правильна обробка та захист є необхідною умовою функціонування сучасної системи управління персоналом.

4. Досліджено особливості цифровізації кадрового діловодства, яка виступає одним із ключових напрямів розвитку сучасного менеджменту. Встановлено, що впровадження HRM-систем, електронного документообігу, хмарних технологій та інструментів штучного інтелекту забезпечує підвищення продуктивності праці, зменшення витрат часу на обробку інформації та підвищення прозорості управлінських процесів. Водночас цифровізація значно ускладнює структуру інформаційних потоків і підвищує вимоги до безпеки даних.

5. Проаналізовано нормативно-правове забезпечення захисту персональних даних, зокрема положення GDPR, національного законодавства України, а також сучасні регуляторні ініціативи у сфері кібербезпеки та штучного інтелекту. Встановлено, що сучасне правове середовище формує жорсткі вимоги до організацій щодо прозорості, підзвітності, мінімізації обробки даних та забезпечення прав суб'єктів персональних даних. Разом із тим, практична реалізація цих норм часто залишається недостатньо ефективною.

6. Здійснено оцінку організаційно-управлінських аспектів ведення кадрового діловодства на прикладі ТОВ «МК БЕТОН». Встановлено, що підприємство має сформовану систему кадрового обліку, поєднує традиційні та цифрові інструменти, однак рівень автоматизації окремих процесів

залишається обмеженим. Система захисту персональних даних має базові елементи, але потребує подальшого вдосконалення в умовах зростання обсягів інформації та ускладнення цифрового середовища.

7. Визначено основні ризики та загрози безпеці персональних даних у цифровому HR-середовищі. До ключових із них належать несанкціонований доступ до інформації, людський фактор, фрагментарна автоматизація, використання незахищених каналів передачі даних, кіберзагрози та недостатній рівень цифрових компетентностей працівників. Доведено, що більшість ризиків мають системний характер і потребують комплексного управління.

8. Обґрунтовано напрями вдосконалення системи управління безпекою персональних даних у кадровому діловодстві. Запропоновано формування організаційно-управлінського механізму захисту, що включає розробку внутрішніх політик, впровадження систем контролю доступу, автоматизацію HR-процесів, розвиток цифрових компетентностей персоналу, проведення регулярного аудиту безпеки та впровадження систем реагування на інциденти. Також обґрунтовано доцільність використання сучасних цифрових рішень, зокрема HRM- та ERP-систем, хмарних технологій і засобів кіберзахисту.

Узагальнюючи результати дослідження, можна зробити висновок, що забезпечення безпеки персональних даних у процесі цифровізації кадрового діловодства є складним багаторівневим процесом, який вимагає інтеграції технічних, організаційних і правових заходів. Ефективна система захисту даних повинна бути невід'ємною складовою загальної системи управління персоналом і стратегічного розвитку підприємства.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Авраменко А.В. Функції захисту персональних даних працівників. Науковий вісник Ужгородського національного університету. 2019. Серія ПРАВО. Випуск 55. Том 1. С. 161–164.
2. Бабчинська О. І. Цифрова трансформація HR-процесів: сучасні тренди та перспективи. Менеджмент і підприємництво в Україні: етапи становлення і проблеми розвитку. 2023. № 2. С. 95–103.
3. Балановська Т. І., Михайліченко М. В., Троян А. В. Сучасні технології управління персоналом: навчальний посібник. Київ: ФОП Ямчинський О.В., 2020. 466 с.
4. Бей Г.В., Середа Г.В. Трансформація HR-технологій під впливом цифровізації бізнес-процесів. Економіка і організація управління. 2019. № 2 (34). С. 93–101.
5. Бурлаков О. С. Інформаційні технології управління кадровим потенціалом. Modern Economics. 2019. № 14 (2019). С. 39–43. DOI: [https://doi.org/10.31521/modecon.V14\(2019\)-06](https://doi.org/10.31521/modecon.V14(2019)-06).
6. Васильченко М. І., Васишин Н. І. Сучасні кадрові технології та інструменти для розроблення автоматизованих інформаційних систем обліку персоналу підприємства. Економіка та суспільство. 2024. № 64. С. 851–857.
7. Горшков М. А. Автоматизація кадрового діловодства в умовах цифрової економіки. Економіка. Фінанси. Право. 2022. № 6. С. 52–56.
8. Гуржій Т.О. Правовий захист персональних даних: монографія. Київ: Київ. нац. торг.-екон. ун-т, 2019. 216 с.
9. Гусаров С.М., Мельник К.Ю. Захист персональних даних працівника. Право і безпека (Law and Safety). 2023. № 2 (89). С. 133–144.
10. Данилевич Н. С., Рудакова С. Г., Щетініна Л. В., Касяненко Я. А. Діджіталізація HR-процесів в сучасних реаліях. Галицький економічний вісник. 2020. № 3. С. 147–157.

- 11.Дейнека В.Ю. Загальний огляд програмних продуктів для автоматизації кадрового діловодства. Документно–інформаційні комунікації в умовах глобалізації: стан, проблеми і перспективи: матеріали VIII Всеукраїн. наук.–практ. конф., м.Полтава, 23 листопада 2023 р. редкол.: І.Г. Передерій, О.Є. Гомотюк та ін. Полтава, 2023. С. 123–129.
- 12.Довжук І.В. Кадрове діловодство: навч.–метод. посіб. Переяслав (Київ. обл.): Домбровська Я.М., 2020. 251 с.
- 13.Дяків О.П., Островерхов В.М. Управління персоналом: навч.метод. посіб. Тернопіль: ТНЕУ, 2018. 288 с.
- 14.Кавтиш О. П., Максимішина О. В. Автоматизація управління персоналом як фактор підвищення продуктивності праці. Підприємництво та інновації. 2020. № 1. С. 30–37.
- 15.Коваль С.В., Скрипник С.В., Шепель І.В. Концептуальні засади автоматизації обліку праці та зарплати працівників аграрних підприємств. Економічний вісник університету. 2022. Вип. 55. С. 47-53.
- 16.Кодекс законів про працю України від 01.10.2023 №2573–ІХ. Верховна Рада України. Законодавство України: URL: <https://zakon.rada.gov.ua/laws/show/322-08#Text>
- 17.Куйбіда В.С., Петрос О.М., Федулова Л.І., Андрощук Г.О. Цифрові компетенції як умова формування якості людського капіталу. Збірник наукових праць Національної академії державного управління при Президентові України. 2019. Вип. 1. С. 118-133.
- 18.Мельник К.Ю. Захист персональних даних працівника: проблеми термінології. Актуальні проблеми приватного та публічного права: матеріали V Міжнародної науково-практичної конференції присвяченої 94-річчю з дня народження членкореспондента НАПрН України, академіка Міжнародної кадрової академії, Заслуженого діяча науки України, доктора юридичних наук, професора Процевського О.І. (31 березня 2023 року). Харків, 2023. 624 с. С. 33–36.

19. Миколайчук Р. А., Миколайчук А. І. Використання технологій штучного інтелекту для автоматизації процесу обробки документів. Сучасні інформаційні технології у сфері безпеки та оборони. 2024. № 2. С. 111-117.
20. Михайлик А.С. До питання нормативно-правового регулювання захисту персональних даних працівників в Україні. Науковий вісник УжНУ. Серія: Право. 2022. № 72. Ч. 2. С. 82–87.
21. Олексієнко О. Кадровий облік на підприємстві: яку користь приносять компаніям сервіси ЕДО. Вчасно.ua. 2024. URL: <https://vchasno.ua/kadrovyyi-oblik-na-pidpriyemstvi/>.
22. Офіційний сайт ТОВ «МК БЕТОН». URL: <https://mkbeton.com.ua/>.
23. Петюх В.М., Рудакова С.Г., Щетініна Л.В. Кадрове адміністрування: навчальний посібник. К.: КНЕУ, 2018. 339 с.
24. Про зайнятість населення: Закон України від 14.10.2023 №5067–ІХ. Верховна Рада України. Законодавство України: вебсайт. URL: <https://zakon.rada.gov.ua/laws/show/5067–17#Text>.
25. Рим О.М. Захист персональних даних працівників у Європейському Союзі. Актуальні проблеми держави і права: зб. наук. пр. Вип. 85 / редкол.: Г.І. Чанишева (голов. ред.) та ін. Одеса: Гельветика, 2020. С. 221–227.
26. Середа О.Г. Актуальні питання правового механізму захисту персональних даних працівника в умовах європейської інтеграції. Юридичний науковий електронний журнал. № 1. 2023. С. 207–211.
27. Спіцина Г.О., Гуцу С.Ф. Щодо питання правового захисту персональних даних працівників. Науковий вісник Ужгородського університету: серія: Право / голов. ред. Ю.М. Бисага. Ужгород, 2023. Т. 1. Вип. 76. С. 255–260.
28. Стельмах О. В. Інформаційні системи управління персоналом на підприємствах України. Економічний простір. 2023. № 184. С. 127–135.
29. Тур О., Тур О., Петренко Д. Використання діджитал-технологій в кадровому адмініструванні та в документообігу. Економіка та суспільство. 2024. № 61. DOI: 10.32782/2524-0072/2024-61-33.

30. Черняк І. О. Аналіз алгоритмів та математичних моделей для автоматизації електронного документообігу. Технічна інженерія. 2023. № 1. С. 178-183.
31. Швець Н.М., Балашова Д.Д. Шляхи цифровізації законодавства про працю. Науковий вісник Ужгородського національного університету. Серія: Право. 2024. Вип. 86, с. 69–75. URL: http://nbuv.gov.ua/UJRN/nvuzhpr_2024_86%283%29__12.
32. Шевчук А. В. Кадрове діловодство на підприємстві. Східна Європа: Економіка, Бізнес та Управління. 2019. № 21. С. 43–47.
33. Шепель І. В. Роль та шляхи розвитку HR-технологій у веденні кадрової документації. Ефективна економіка. 2023. № 12. URL: http://nbuv.gov.ua/UJRN/efek_2023_12_38.
34. Шкільняк М., Мельник А., Желюк Т., Васіна А., Дудкіна О. Менеджмент та публічне управління в умовах сучасних викликів. Вісник економіки. 2023. Вип. 2. С. 233-248.
35. Ящик О. Б., Твердохліб І. А., Ю. П. Франко, Ожга М. М. Використання технології блокчейн для забезпечення автоматизації управління освітніми документами. Наукові записки Тернопільського національного педагогічного університету імені Володимира Гнатюка. Серія : Педагогіка. 2022. № 2. С. 113-120.
36. Bisen Sh. K. Large Language Models (LLM): Difference between GPT-3 & BERT. Published in Bright AI. 2022. URL: <https://medium.com/bright-ai/nlp-deep-learningmodels- difference-between-bert-gpt-3-f273e67597d7>.
37. Chamorro-Premuzic T. The Future of Recruitment and HR: How AI Is Changing the Game. Harvard Business Review. 2022. URL: <https://hbr.org/2022/07/how-ai-is-changing-hr>
38. Deloitte Insights. 2023 Global Human Capital Trends. Deloitte, 2023. URL: <https://www2.deloitte.com/global/en/pages/about-deloitte/articles/global-human-capital-trends.html>.

39. McKinsey & Company. Reimagining HR: Insights for a post-pandemic future. 2023 URL: <https://www.mckinsey.com/business-functions/people-and-organizational-performance>.
40. Netpeak. Автоматизація HR-процесів: огляд платформ, які використовуються в Україні 2023. URL: <https://netpeak.net/ua/blog/hr-platforms-in-ukraine/>.
41. Pakhucha E., Sievidova I., Babko N., Romaniuk I. et al. Investigating the impact of structural changes: the socio-economic security framework. European Journal of Sustainable Development. 2023. Vol. 12. Is. 1. Pp. 180-198.
42. Sanjay P., Li W., Xiaoming Ch., Hua L. GPT was Only the Beginning: Autonomous Agents are Coming. Boston Consulting Group. 2023. URL: <https://www.bcg.com/publications/2023/gpt-was-only-thebeginning-autonomous-agents-are-coming>
43. Wyndham A. 10 Large Language Models That Matter to the Language Industry. Data & Indexes, Technology. 2024. URL: <https://slator.com/10-large-language-models-that-matter-to-the-language-industry>.
44. Zhao P., Zhang H., Yu Q., Wang Z., Geng Y., Fu F., Yang L., Zhang W., Jiang J., Cui B. Retrieval-Augmented Generation for AI-Generated Content: A Survey. arXiv: 2402.19473 (cs.CV) 2024. URL: <https://arxiv.org/abs/2402.19473>.