DOI: https://doi.org/10.32782/2524-0072/2025-82-65

УДК 005.95/.96:004.738.5:004.056(4+477)

ЗАХИСТ ДАНИХ У СИСТЕМІ УПРАВЛІННЯ ПЕРСОНАЛОМ В УМОВАХ ВИКЛИКІВ ТА КІБЕРЗАГРОЗ ДЛЯ ІНФОРМАЦІЙНОЇ ПРИВАТНОСТІ

DATA PROTECTION IN THE PERSONNEL MANAGEMENT SYSTEM IN THE CONTEXT OF CHALLENGES AND CYBER THREATS TO INFORMATION PRIVACY

Жуляєв Владислав Валерійович
аспірант,
Міжрегіональна академія управління персоналом
ORCID: https://orcid.org/0000-0001-6855-856X

Zhuliaiev Vladyslav
Interregional Academy of Personnel Management

У статті проаналізовано виклики і загрози, пов'язані із захистом персональних даних працівників у системах управління персоналом. Показано міждисциплінарний характер проблеми інформаційної приватності, що охоплює соціотехнічні, правові, організаційні, етичні, соціокультурні аспекти. Обґрунтовано необхідність багаторівневого аналізу, із увагою до внутрішніх процесів організації та впливів зовнішнього середовища. Розглянуто новітні регуляторні норми ЄС щодо захисту даних, штучного інтелекту та кіберстійкості, важливі для організацій країн ЄС та України, яка перебуває в умовах повномасштабної війни та євроінтеграції. Підкреслено, що цифровізація HR-систем одночасно спрощує управління персоналом і посилює ризики витоків даних працівника. Підкреслено глобальний характер ризиків, пов'язаних з приватністю, та наголошено на необхідності скоординованих зусиль регуляторних органів, бізнесу та громадянського суспільства для забезпечення надійного захисту персональних даних та зміцнення інформаційної приватності в цифровому середовищі, що розвивається.

Ключові слова: захист персональних даних, інформаційна приватність, ціфрові HR-системи, управління персоналом, кіберзагрози, регулювання ЄС, GDPR, штучний інтелект, євроінтеграція України.

The article presents a comprehensive analysis of the key challenges and threats related to the protection of employees' personal data within contemporary human resource management systems. It emphasizes that information privacy constitutes an inherently interdisciplinary problem requiring an integrated approach that combines socio technical, legal, organizational and sociocultural perspectives. Information privacy based on the principles of personal information control, transparency, consent and trust. The study highlights the need for a multilayered analytical framework that considers both internal organizational processes and external environmental influences, including regulatory initiatives, international standards, political and economic dynamics, and technological risks associated with digital transformation. Special attention is given to the latest EU regulatory frameworks on data protection, artificial intelligence and cyber resilience, which introduce new obligations for organizations, including compliance with employee data protection requirements. The article underscores the specific context of Ukraine, which simultaneously faces the demands of European integration and the intensified cyber threats caused by the ongoing full-scale war, creating additional risks of confidential data leakage. It is demonstrated that the digitalization of HR processes and the adoption of HR information systems generate significant managerial advantages while also amplifying vulnerabilities to cyberattacks that pose threats of data leakage, including personal data of employees. An analysis of leading experts' perspectives confirms that information privacy has evolved beyond a purely technical concern into a multidimensional challenge encompassing technological, social, economic, and political dimensions. The global scope of privacy-related risks was underscored, along with the imperative for coordinated action among regulators, businesses, and civil society to ensure strong safeguards for personal data and to enhance information privacy within the rapidly changing digital landscape.

Keywords: personal data protection; information privacy; digital HR systems; human resource management; cyber threats; EU regulation; GDPR, artificial intelligence; European integration of Ukraine.

Постановка проблеми. Рух України до європейського простору продовжується навіть в той час, коли українська держава майже чотири роки знаходиться у стані повномасштабної війни. Одним із напрямів суспільних трансформацій має стати оновлена політика у сфері захисту даних, на яку в країнах ЄС суттєво вплинуло впровадження у дію Загального регламенту захисту даних (GDPR) у 2018 році [14]. В Україні діє Закон про захист даних, прийнятий у 2010 році [6]; також підготовано проєкт оновленого Закону, в якому мають бути враховані сучасні нормативно-правові засади поводження з персональними даними. Прийняття GDPR стало стимулом для багатьох країн світу оновити чи прийняти закони про захист даних (інформаційну приватність). Це стає відповіддю на стрімкі зміни, пов'язані із цифровізацією економічного, громадського і повсякденного життя, коли велика частина інформації, в тому числі персонального, конфіденційного характеру знаходиться в цифровому просторі. Фінансові трансакції, комерційні, державні послуги змістилися в онлайн-середовище. Соціальні мережі стали простором, в якому розгортається велика частина комунікацій, одночасно доступ до глобальних платформ часто потребує надання персональних даних. Ці та інші новації (наприклад, технології штучного інтелекту) розширюють можливості отримання швидких і зручних послуг для індивідів, але одночасно створюють значні ризики і загрози для обробки персональних даних осіб великими компаніями у своїх цілях, ризики посилення технологій спостереження, в тому числі в публічному середовищі, на робочому місці, ризики шахрайства і крадіжок цифрових даних тощо. Саме для протидії таким викликам і загрозам відбувається оновлення нормативно-правової бази захисту персональних даних у всьому світі.

Основним відповідальним актором, на якого закони про захист даних покладають відповідальність за дотримання регламентів поводження із даними, є організації різного типу – у державному і приватному секторах, комерційні і неприбуткові тощо. Саме на мезорівні організацій відбувається розробка внутрішніх політик поводження із даними, дотримання цих протоколів у реальній організаційній практиці, відповідальність у разі недотримання правових вимог і норм. Мова йде в першу чергу про належну обробку даних працівників організації (підприємства, навчального закладу, міністерства чи відомства тощо), а також у разі наявності – обробку клієнтських баз даних, даних постачальників, обробку даних у ході міжнародних трансакцій тощо. У всіх випадках в організації велику роль відіграє підрозділ з управління персоналом, який є сполучною ланкою між керівництвом організації та всіма іншими підрозділами (в першу чергу інформаційної безпеки / кібербезпеки, юридичним відділом, які опікуються захистом баз даних). Працівники відділів управління персоналом мають дбати про власну обізнаність та обізнаність колективу організації у царині захисту даних.

Аналіз останніх досліджень і публікацій. Вітчизняні дослідники приділяють увагу проблемі захисту даних працівників в Україні, в тому числі в контексті євроінтеграції, цифровізації, умов війни, кібератак. На основі аналізу теоретичних підходів, судової практики та міжнародних стандартів Л. Малюга і К. Шкрібляк роблять висновок, що в умовах цифрової трансформації трудових відносин правове регулювання захисту персональних даних працівників в Україні є концептуально застарілим [8]. У роботі С. Гусарова і К. Мельника розглянуто питання захисту персональних даних працівника, в тому числі в умовах війни і супутніх небезпек [4]. На важливість підвищення рівня цифрової компетентності державних службовців (уміння відповідати викликам кібер-ризиків, зберігати конфіденційні дані) звертають увагу І. Матвєєнко і Г. Панченко [9]. Розглядаючи процеси цифровізації економіки, Т.Збрицька і О. Сорока вказують, що HR-менеджери мають оволодівати сучасними технологіями і одночасно трансформувати базові HR-процеси [7]. Аналіз теоретичних і практичних аспектів цифровізації у ракурсі впливу на процеси менеджменту персоналу та поширення HRM-систем на вітчизняному ринку провели І. Варіс, О. Кравчук, І. Бацман [1]. На виклики структурних розривів між технологічним оновленням організацій та нестачею компетентностей персоналу до ефективного застосування цифрових інструментів, платформ та інновацій вказують В. Руденко, О. Другова, М. Бріль [10].

Важливими є розвідки, де звертається увага на роль зовнішніх (навколишнє середовище) і внутрішніх (рівень організації) чинників для захисту даних громадян. Так, у статті Gstrein&Beaulieu (2022) досліджується перспектива аналізу взаємозв'язку технологічної, етичної та регуляторної динаміки приватності [18]. У розвідці Ahmadon et al (2025) проаналізовано роль зовнішньої інфраструктури цифрової приватності [11]; у праці Bhave et al

(2019) звертається увага на необхідність врахування численних інтерфейсів приватності на робочому місці [13]. Дослідження Tang (2023) висвітлює юридичні зобов'язання щодо захисту особистих даних працівників у робочому середовищі та впровадження належних заходів для пом'якшення ризиків [22]. Детальний огляд проблем і загроз конфіденційності даних в цифровій екосистемі HR надано у статті Jain et al [20].

Виділення невирішених раніше частин загальної проблеми. Попри увагу цих та інших дослідників до окремих аспектів досліджуваної проблеми, нагальною зостається необхідність розгляду трансформації систем управління і захисту даних в організаціях під впливом змін зовнішнього середовища, а також глобальних і внутрішніх викликів і загроз цим процесам.

Формулювання цілей статті (постановка завдання). Метою статті є розгляд проблеми захисту даних працівників організацій в системах управління персоналом в умовах поширення нових нормативно-правових вимог, впровадження цифрових інформаційних систем менеджменту людських ресурсів та супутніх цим процесам викликам і загрозам, розглянутих на рівні зовнішнього середовища. Це пов'язано також із питанням необхідності розробки багаторівнего підходу до аналізу управління захистом даних в організації.

Виклад основного матеріалу дослідження. Сучасні дослідники проблем захисту даних, приватності, інформаційної безпеки, кібербезпеки, які працюють у різних дисциплінах, все частіше говорять про необхідність опрацювання комплексних, міждисциплінарних підходів, які б включали і переосмислювали здобуті результати і співставляли їх для пошуку нових моделей. Захист даних працівників у фізичних та цифрових середовищах відбувається на рівні організацій [17], разом із тим організації діють в економічному, правовому, ринковому, технічному середовищах, процеси в яких треба враховувати для розбудови стратегії управління даними та реалізації відповідних практик. Для кращого розуміння проблеми захисту даних в цифровому суспільстві може стати в нагоді, зокрема, розроблена фахівцями галузі модель, яка визначає сім основних факторів, що впливають на впровадження надійної інфраструктури цифрової приватності. Це технічні, регуляторні, економічні, законодавчі, правові, індивідуальні, а також суспільні та культурні фактори. Кожен з цих факторів вливає на очікування людей щодо приватності і захисту персональних даних в будь-якій цифровій екосистемі [11]. Про необхідність розробки програми досліджень, яка б окреслювала численні інтерфейси – як мінімум юридичний, етичний, технологічний, міжнародний та кадровий – говорять дослідники приватності на робочому місці [13]. Науковці наголошують на необхідності розрізняти інформаційну приватність та приватність робочого середовища (просторову, акустичну тощо). До стейкхолдерів захисту даних аналітики включають різних учасників, пов'язаних з трудовими відносинами: працівників, роботодавців, державу та суспільство в цілому [12]. Отже, після розгляду нових регуляторних вимог до відділів управління персоналом щодо захисту даних в ЄС і огляду тренду цифровізації систем управління персоналом, які несуть в собі як переваги, так і виклики, ми також розглянемо експертні оцінки стану викликів і загроз для інформаційної приватності в глобальному світі.

Нормативно-правовий вимір захисту даних в організації включає конкретні регуляторні акти, такі як GDPR, національні закони про захист даних, трудове законодавство та галузеві стандарти. Як вже вказувалося, прийняття GDPR посилило рух до оновлення законодавства про захист даних у всьому світі. У межах заданих юридичних рамок організації мають діяти, виконуючи обов'язки щодо прозорості, підзвітності, оцінки ризиків та реагування на інциденти. Це ключовий вимір для формування відповідальної практики обробки даних, яка зосереджена в основному у відділах кадрів, HRM та суміжних підрозділах. Для кращого розуміння сучасних вимог захисту даних, яких мають дотримуватися системи управління персоналом в організаціях країн ЄС (а також тих, які обробляють дані громадян ЄС), назвемо ключові нормативно-правові вимоги захисту даних (рамка GDPR) [14].

Визначення дійсної правової основи для обробки даних працівників: ст. 6 GDPR визначає перелік законних підстав, ст. 7 уточнює вимоги до згоди. У трудових відносинах також застосовується ст. 88, яка дозволяє державам встановлювати додаткові правила щодо обробки даних працівників. Захист даних за проєктом і за замовчуванням: ст. 25 вимагає, щоб компанії впроваджували технічні та організаційні заходи, які забезпечать мінімізацію даних та захист приватності ще на етапі

проєктування систем. Прозорість та розкриття інформації: статті 12-14 зобов'язують роботодавця надавати зрозумілу, доступну та повну інформацію про обробку даних: що збирається, навіщо, як довго зберігається і які права має працівник. Право на доступ та перенесення: ст. 15 гарантує право отримати копію своїх даних та інформацію про їх обробку; ст. 20 встановлює право на перенесення даних у структурованому вигляді. Право бути забутим: ст. 17 визначає випадки, коли суб'єкт даних може вимагати видалення, наприклад, якщо дані більше не потрібні, або обробка була незаконною.

Стаття 83 дозволяє Наглядовому органу накладати адміністративні штрафи за порушення Регламенту. Ці штрафи є відчутними для організації: до 4% від глобального обороту або 20 мільйонів євро. Зобов'язання, накладені GDPR, у поєднанні із загрозою високих штрафів у випадках невідповідності, стали викликом і спонукали організації країн ЄС запроваджувати нові керівні принципи, процедури та практики. Ці заходи направлені на здійснення захисту даних за замовчуванням і дизайном, впровадження нових ефективних процедур для швидкого розгляду та звітності про порушення приватності, проведення оцінок дотримання вимог (DPIA), управління згодою та ефективну (автоматизовану) обробку запитів щодо прав суб'єктів даних, тощо. Дослідники Labadie & Legner (2023) наголошують, що багато організацій стикаються з труднощами при дотриманні вимог EU-GDPR: ці нові типи правил захисту даних не можуть бути вирішені шляхом адаптації існуючих рамок, а вимагають фундаментального переосмислення того, як компанії зберігають і обробляють персональні дані на рівні всього підприємства [21].

Правове, регуляторне середовище щодо впровадження нових технологій весь час змінюється у різних юрисдикціях, реагуючи на нові виклики, пов'язані із розвитком технологій ШІ, кіберзагрозами тощо. Так, останніми роками в ЄС набули чинності Закон про штучний інтелект [15] та Закон про кіберстійкість (CRA) [16], дію яких мають враховувати організації. Закон про штучний інтелект впроваджується з серпня 2024 року і буде повністю застосований у квітні 2026 року. Його описують як першу у світі комплексну правову рамку, яка встановлює гармонізовані правила для сприяння надійному ШІ в ЄС. Він запроваджує правила, що ґрунтуються на врахуванні ризиків, для розробників та користувачів ШІ – стосовно конкретних застосувань технології. Закон про ШІ спрямований на захист основних прав людини, в тому числі права на інформаційну приватність, посилюючи вимоги до обробки даних в ШІ-системах, встановлюючи суворі правила для високоризикованих ШІ-рішень, включно з HR-технологіями, і працюючи у зв'язці з GDPR.

Закон про кіберстійкість (CRA) набув чинності 10 грудня 2024 року, повне впровадження заплановано на грудень 2027 року. CRA – це регламент ЄС, який встановлює вимоги до кібербезпеки для підключених апаратних та програмних продуктів (наприклад, пристроїв Інтернету речей, розумних приладів, маршрутизаторів). Він доповнює чинні закони, такі як Директива NIS2, спрямована на зниження кіберризиків у всьому ланцюжку цифрових поставок ЄС. Основними цілями CRA є: зобов'язати виробників інтегрувати надійні заходи кібербезпеки від початкової розробки продукту протягом усього його життєвого циклу; створити єдину систему кібербезпеки для спрощення дотримання нормативних вимог як для виробників апаратного, так і для програмного забезпечення; вимагати чіткого розкриття функцій кібербезпеки та захисту для всіх цифрових продуктів; надання бізнесу та споживачам можливості безпечно використовувати цифрові продукти.

Вітчизняні експерти наголошують, що в Україні потрібними є подальші зусилля у сфері євроінтеграції. Станом на кінець 2024 року Україна виконала 71% вимог у рамках Угоди про асоціацію між Україною та ЄС щодо пунктів «Наука, технологія та інновації, космос, цифрова інтеграція». Необхідно продовжувати адаптацію українського цифрового законодавства до норм ЄС, зокрема у сфері захисту даних та регулювання ШІ [2].

Одночасно перевагою і викликом для захисту і безпеки даних в організаціях стає цифровізація HRM. Сучасні HR-екосистеми [20] охоплюють платформи та інструменти, що автоматизують рекрутинг, адаптацію в трудовому колективі, навчання, оцінювання, управління пільгами, аналітику персоналу. Вони базується на хмарних сервісах, мобільних застосунках і ШІ, які забезпечують оперативні рішення та персоналізацію процесів. Ключові компоненти екології включають інформаційні системи управління персоналом (HRIS) як централізоване сховище даних, системи управління талантами, системи управління навчанням (LMS), платформи компенсацій і пільг, інструменти залучення персоналу та

аналітику на основі ШІ. Ці компоненти формують складні потоки даних в цифровому середовищі і є вразливими до кіберзагроз. Системи управління персоналом обробляють широкий спектр персональної інформації, у тому числі чутливої. SaaS-рішення (Software as a Service) стали основою сучасних цифрових HR-екосистем (прикладами рішень є Workday, SuccessFactors, Oracle HCM Cloud тощо). Вони дозволяють компаніям використовувати HR-платформи без локальної інфраструктури, забезпечуючи ефективність, швидке оновлення та доступ у режимі реального часу, разом із тим підвищуючи виклики щодо безпеки та контролю за даними.

В Україні впровадження цифрових рішень в системах управління персоналом прискорилося після 2020 року. Державний сектор переходить на електронний кадровий документообіг через портал «Дія» та «єКадри». Відбувається процес впровадження інтегрованої інформаційної системи управління людськими ресурсами в державних органах влади (HRMIS), яка запрацювала з 31 березня 2021 року за сприяння ЄС у межах програми підтримки управління державними фінансами в Україні (EU4PFM). Цифровізація управління державною службою та людськими ресурсами є одним із євроінтеграційних зобов'язань України в частині реформування державного управління, що здійснюється з урахуванням європейських Принципів державного управління, розроблених OECD/SIGMA, а також є однією з вимог програми Ukraine Facility, в межах якої Україна отримує фінансування від ЄС [3]. Приватні компанії активно впроваджують такі рішення, як BAS HRM, PeopleForce, Hurma, Kadro, а також міжнародні системи Workday, SAP, SuccessFactors (дет.: [3]).

Поряд із безперечними перевагами цифровізації систем управління персоналом, державні реєстри та бізнес-компанії часто стають мішенню кіберзлочинців. Так, на початок 2025 року урядова команда реагування на комп'ютерні надзвичайні події CERT-UA при Держспецзв'язку, повідомила, що в 2024 році опрацювала 4315 кіберінцидентів. Це на 69,8% більше, ніж роком раніше, коли кіберзлочинці атакували український кіберпростір 2541 раз. Найчастіше зловмисники атакують місцеві органи влади, уряд та урядові організації, сектор безпеки та оборони, енергетичний сектор, комерційні організації, телекомунікації. Найпоширенішими типами інцидентів є розповсюдження шкідливого програмного забезпечення, фішинг, шкідливе підключення, компрометація облікового запису або системи. Метою зловмисників є викрадення чутливої інформації, а також знищення даних та інформаційних систем [5].

Одним із джерел даних про сучасне бачення викликів і загроз системам захисту даних і кібербезпеці є регулярні опитування (2022, 2024, 2025) керівників організацій, фахівців та експертів з інформаційної безпеки, управління ризиками тощо під час проведення заходів Всесвітнього економічного форуму. В опитуванні «Огляд глобальної кібербезпеки-2025» брали участь представники різних секторів економіки – фінансового, енергетичного, телекомунікаційного, медичного, виробничого, державного управління із різних регіонів світу [23]. Ключовими тенденціями було визначено ускладнення глобального ландшафту кібербезпеки – через поєднання геополітичної напруги, технологічних змін, зростання кіберзлочинності, взаємозалежності інфраструктур та ланцюгів постачання, появи нових технологій і збереженні застарілих систем протидії ризикам. Геополітичні конфлікти значно змінюють сприйняття ризиків, а головними загрозами експерти назвали кібершпигунство та втрату організаціями конфіденційної, в тому числі персональної інформації. Наголошено, що війна проти України демонструє вразливість критичних секторів до комбінованих кібер- і фізичних атак. Одним із загрозливих трендів є проблема глобальної нерівності у доступі до кіберзахисту. Зафіксовано значні регіональні відмінності у відповідях: 42% представників організацій з Латинської Америки та 36% – з Африки не впевнені у готовності до кіберзагроз, тоді як у Європі та Північній Америці таких лише 15%. Поглиблюється розрив між великими та малими і середніми організаціями. Малі компанії стикаються з проблемами кіберстійкості у 7 разів частіше, ніж великі (порівняно із 2022 роком). Разом із тим велика взаємозалежність ланцюгів постачання означає, що навіть компанії з високим рівнем захисту можуть постраждати через слабкі ланки серед партнерів. У звіті підкреслено, що нові технології – штучний інтелект (AI) , Інтернет речей (IoT), хмарні сервіси – одночасно створюють нові можливості та збільшують площу атаки. Особливо небезпечним є поєднання AI-інструментів і кіберзлочинності, що підвищує точність і швидкість атак, в тому числі націлених на злами баз даних (табл. 1).

Таблиця 1

Відповіді експертів на питання: Які проблеми кібербезпеки, пов'язані з GenAI, вас найбільше хвилюють?, 2025, %

Розвиток можливостей зловмисників (наприклад, фішинг, розробка шкідливого програмного забезпечення, дипфейки)	47
Витік даних (розкриття персональних даних через GenAI)	22
Інші (ризики ланцюга постачання програмного забезпечення, безпека систем штучного інтелекту, правові проблеми інтелектуальної власності)	17
Підвищена складність управління безпекою	14

Джерело: сформовано на основі [23]

Звіт «How Experts Think about Digital Privacy» [19] містить результати інтерв'ю з провідними фахівцями з кібербезпеки, права, цифрової етики, технологічного регулювання та ін. Вони оцінюють сучасний стан приватності в цифровому суспільстві та ключові виклики на майбутнє. Інформаційна приватність означає здатність людини вирішувати, хто отримає доступ до її даних і як вони будуть використані; базується на принципах контролю персональної інформації, прозорості, згоді та довірі. Експерти наголошують, що інформаційна приватність перестала бути лише технічним питанням, і перетворилася на багатовимірну проблему, де поєднані технологічні, соціальні, економічні та політичні чинники. Зростання обсягів даних, розвиток штучного інтелекту та алгоритмічних систем, а також зростання економіки даних змінюють уявлення про контроль над інформацією. Підкреслено, що традиційні моделі згоди суб'єкта даних вже не працюють у середовищах, де ці дані збирають постійно, часто без явної взаємодії з людиною. У звіті зазначено, що навіть новітні регуляторні рамки не встигають за темпами технологічних змін, що створює прогалини у захисті права на приватність. Окремий акцент зроблено на етичних аспектах: зростає потреба у прозорості процедур збирання даних, відповідальному їх використанню, та мінімізації ризиків дискримінації, що виникають через автоматизовану обробку інформації.

У звіті вирізнено два погляди експертів щодо напрямку розвитку інформаційної приватності у майбутньому. Прихильники оптимістичного бачення вважають, що суворіші закони про приватність, підвищена обізнаність в суспільствах і громадах та технології підсилення приватності можуть змістити баланс на користь громадян. Ті, хто дотримується радше песимістичного бачення, наголошують, що спостереження на основі штучного інтелекту, збір біометричних даних, апатія власників даних та / або невігластво, а також корпоративний опір регулюванню можуть ще більше підірвати основи захисту персональних даних. Отже, захист приватності знаходиться на роздоріжжі. Бізнес, політики та індивіди повинні перейти від дотримання вимог до змістовного захисту приватності. Подальший шлях залежить від того, наскільки серйозно до приватності будуть ставитися регуляторні органи, компанії та громадськість у найближчі роки [19].

Висновки. Проведений аналіз показує, що проблема захисту даних працівників в системі управління персоналом, як і ширша проблема захисту персональних, чутливих даних громадян в сучасних суспільствах, є гостро актуальною і суспільно значущою. Аналіз швидких змін у зовнішньому середовищі організацій – впровадження нових нормативно-регуляторних законів, які стосуються захисту даних, тенденції цифровізації і широкого впровадження інформаційних систем в управлінні персоналом потребують підвищення рівня відповідних компетентностей і стратегічного бачення лідерів, менеджерів та працівників організацій. Результати опитування експертів підтверджують, що захист персональних даних працівників стає частиною ширшої архітектури інформаційної безпеки та кіберстійкості, актуальність якої підсилюють геополітичні ризики, включно із війною проти України.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Варіс І.О., Кравчук О.І., Бацман І.С. Концептуальні основи цифровізації менеджменту персоналу. *Приазовський економічний вісник.* 2023. Вип. 4 (36). С. 32-41. DOI: https://doi.org/10.32782/2522-4263/2023-4-5

2. Виговська В., Шолудько В., Балицька М. Державна цифрова трансформація: аналіз за 2019-2024 роки. URL: https://voxukraine.org/derzhavna-tsyfrova-transformatsiya-analiz-za-2019-2024-roky (дата звернення: 26.12.2025).

3. ГО «Лабораторія законодавчих ініціатив». Цифрова трансформація системи управління людськими ресурсами на державній службі, 2025. URL: https://parlament.org.ua/wp-content/uploads/2025/07/ali_brief_-digitalisation_hrmis.pdf (дата звернення: 26.12.2025).

4. Гусаров С. М., Мельник К. Ю. Захист персональних даних працівника. Право і безпека. 2023. № 2 (89). С.133–144. https://doi.org/10.32631/pb.2023.2.12

5. Державна служба спеціального зв'язку та захисту інформації України (2025). CERT-UA минулого року опрацювала 4315 кіберінцидентів. URL: https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv (дата звернення: 27.12.2025).

6. Закон України «Про захист персональних даних», № 2297-VI від 01.06.2010. *Відомості Верховної Ради України.* https://zakon.rada.gov.ua/laws/show/2297-17#Text

7. Збрицька Т., Сорока О. Управління персоналом в епоху цифрової економіки. *Економіка та суспільство.* 2021. Вип. 31. https://doi.org/10.32782/2524-0072/2021-31-20

8. Малюга Л.Ю., Шкрібляк К.П. Особливості захисту персональних даних у процесі цифровізації трудових відносин: теоретико-правовий аналіз. *Науковий вісник Ужгородського Національного Університету. Серія ПРАВО.* 2025. Вип. 91: Ч. 2. С. 114-120. https://doi.org/10.24144/2307-3322.2025.91.2.14

9. Матвєєнко І., Панченко Г. Управління персоналом в системі державної служби України в умовах цифровізації. *Наукові перспективи.* 2022. № 9(27). https://doi.org/10.52058/2708-7530-2022-9(27)-157-170

10. Руденко В. О., Другова, О. С., Бріль, М. С. Діджитал-компетентність персоналу як фактор цифрової ефективності підприємств. *Трансформаційна економіка.* 2025. № 2 (11), С. 100-106. https://doi.org/10.32782/2786-8141/2025-11-16

11.Ahmadon M. A. et al. Digital Privacy: Trends, Challenges, and the Future. *IT Professional.* 2025. Vol. 27 (3). P. 69-77. https://ieeexplore.ieee.org/document/11029710

12. Ball K., Daniel E., Stride C. Dimensions of employee privacy: an empirical study. *Information Technology & People.* 2012. Vol. 25 (4). P. 376–394, doi: https://doi.org/10.1108/09593841211278785

13. Bhave D. P., Teo, L., Dalal. R. S. Privacy at Work: A Review and a Research Agenda for a Contested Terrain. *Journal of Management.* 2019. Vol. 46 (3). DOI:10.1177/0149206319878254

14. European Parliament and Council. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). *Official Journal of the European Union*, 2016, L 119, P. 1-88. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj

15. European Parliament and Council. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union*, L 2024/1689. URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj

16. European Parliament and Council. Regulation (EU) 2024/… on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act). *Official Journal of the European Union*, 2024. URL: https://eur-lex.europa.eu/

17. Gotsch M., Schögel M. Addressing the privacy paradox on the organizational level: review and future directions. *Management Review Quarterly.* 2021. Vol. 73, P. 263–296. https://doi.org/10.1007/S11301-021-00239-4

18. Gstrein O., Beaulieu A. How to protect privacy in a datafied society? A presentation of multiple legal and conceptual approaches. *Philos. Technol.* 2022. Vol. 35 (3). https://doi.org/10.1007/s13347-022-00497-4

19. How Experts Think about Digital Privacy. IEEE Digital Privacy. 2025. https://digitalprivacy.ieee.org/wp-content/uploads/2025/07/How-Experts Think-About-Digital-Privacy.pdf (дата звернення: 25.12.2025).

20. Jain N., Maheshwari M., Singhal S., & Vishnoi, D. Cybersecurity in HR Tech: A review of data privacy challenges in the digital HR ecosystem. *Advances in Consumer Research.* 2025. Issue 2. pp. 855-866.

21. Labadie C., Legner C. Building data management capabilities to address data protection regulations: Learnings from EU-GDPR. *Journal of Information Technology*, 2023. Vol. 38(1). P. 16-44. https://doi.org/10.1177/02683962221141456

22. Tang A. *Privacy in Practice: Establish and Operationalize a Holistic Data Privacy Program*. N.Y.: Taylor & Francis Group, 2023. 450 p.

23. World Economic Forum. Global Cybersecurity Outlook 2025. Geneva: World Economic Forum, 2025. 44 p. URL: https://www.weforum.org/reports/global-cybersecurity-outlook-2025 (дата звернення: 26.12.2025).

REFERENCES:

1. Varis, I. O., Kravchuk, O. I., & Batsman, I. S. (2023). Kontseptualni osnovy tsyfrovizatsii menedzhmentu personalu [Conceptual foundations of HR management digitalization]. *Pryazovskyi Economic Bulletin*, 4(36), 32–41. https://doi.org/10.32782/2522-4263/2023-4-5 (in Ukrainian).

2. Vyhovska, V., Sholudko, V., & Balytska, M. (2025). Derzhavna tsyfrova transformatsiia: analiz za 2019–2024 roky [State digital transformation: Analysis for 2019–2024]. https://voxukraine.org/derzhavna-tsyfrova-transformatsiya-analiz-za-2019-2024-roky (in Ukrainian).

3. Hromadska orhanizatsiia “Laboratoriia zakonodavchykh initsiatyv” (2025). Tsyfrova transformatsiia systemy upravlinnia liudskymy resursamy na derzhavnii sluzhbi [Digital transformation of the HR management system in the civil service]. https://parlament.org.ua/wp-content/uploads/2025/07/ali_brief_-digitalisation_hrmis.pdf (in Ukrainian).

4. Husarov, S. M., & Melnyk, K. Yu. (2023). Zakhyst personalnykh danykh pratsivnyka [Protection of employee personal data]. *Pravo i Bezpeka,* 2(89), 133–144. https://doi.org/10.32631/pb.2023.2.12 (in Ukrainian).

5. Derzhavna sluzhba spetsialnoho zv’iazku ta zakhystu informatsii Ukrainy. (2025). CERT-UA mynuloho roku opratsiuvav 4315 kiberintsydentiv [CERT-UA processed 4315 cyber incidents last year]. https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv (in Ukrainian).

6. Zakon Ukrainy “Pro zakhyst personalnykh danykh” №2297-VI vid 01.06.2010 [Law of Ukraine “On Personal Data Protection”]. (2010). https://zakon.rada.gov.ua/laws/show/2297-17#Text (in Ukrainian).

7. Zbrytska, T., & Soroka, O. (2021). Upravlinnia personalom v epokhu tsyfrovoi ekonomiky [HR management in the era of the digital economy]. *Ekonomika ta Suspilstvo*, 31. https://doi.org/10.32782/2524-0072/2021-31-20 (in Ukrainian).

8. Maliuha, L. Yu., & Shkribliak, K. P. (2025). Osoblyvosti zakhystu personalnykh danykh u protsesi tsyfrovizatsii trudovykh vidnosyn: teoretyko-pravovyi analiz [Features of personal data protection in the digitalization of labor relations: Theoretical and legal analysis]. *Scientific Bulletin of Uzhhorod National University. Law Series*, 91(2), pp. 114–120. https://doi.org/10.24144/2307-3322.2025.91.2.14 (in Ukrainian).

9. Matvieienko, I., & Panchenko, H. (2022). Upravlinnia personalom v systemi derzhavnoi sluzhby Ukrainy v umovakh tsyfrovizatsii [HR management in the Ukrainian civil service under digitalization]. *Naukovi Perspektyvy,* 9(27). https://doi.org/10.52058/2708-7530-2022-9(27)-157-170 (in Ukrainian).

10. Rudenko, V. O., Druhova, O. S., & Bril, M. S. (2025). Didzhytal-kompetentnist personalu yak faktor tsyfrovoi efektyvnosti pidpryiemstv [Digital competence of personnel as a factor of enterprises’ digital efficiency]. *Transformatsiina Ekonomika*, 2(11), pp. 100-106. https://doi.org/10.32782/2786-8141/2025-11-16 (in Ukrainian).

11. Ahmadon, M. A. et al., (2025). Digital Privacy: Trends, Challenges, and the Future. *IT Professional.* 27 (3), pp. 69-77. https://ieeexplore.ieee.org/document/11029710

12. Ball, K., Daniel, E., Stride, C. (2012). Dimensions of employee privacy: an empirical study. *Information Technology & People*, 25 (4), pp. 376-394, doi: https://doi.org/10.1108/09593841211278785

13. Bhave D. P., Teo, L., Dalal. R. S. (2019) Privacy at Work: A Review and a Research Agenda for a Contested Terrain. *Journal of Management*. 46 (3). DOI:10.1177/0149206319878254

14. European Parliament and Council. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). *Official Journal of the European Union*, L 119, 1–88. https://eur-lex.europa.eu/eli/reg/2016/679/oj

15. European Parliament and Council. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union,* L 2024/1689. https://eur-lex.europa.eu/eli/reg/2024/1689/oj

16. European Parliament and Council. (2024). Regulation (EU) 2024/… on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act). *Official Journal of the European Union.* https://eur-lex.europa.eu/

17. Gotsch, M., Schögel, M. (2021). Addressing the privacy paradox on the organizational level: review and future directions. *Management Review Quarterly*. 73, pp. 263–296. https://doi.org/10.1007/S11301-021-00239-4

18. Gstrein, O., Beaulieu, A. (2022). How to protect privacy in a datafied society? A presentation of multiple legal and conceptual approaches*. Philos. Technol*. 35(3). https://doi.org/10.1007/s13347-022-00497-4

19. How Experts Think about Digital Privacy (2025). IEEE Digital Privacy. https://digitalprivacy.ieee.org/wp-content/uploads/2025/07/How-Experts Think-About-Digital-Privacy.pdf

20. Jain, N., Maheshwari, M., Singhal, S., & Vishnoi, D. (2025). Cybersecurity in HR Tech: A review of data privacy challenges in the digital HR ecosystem. *Advances in Consumer Research*. Issue 2, pp. 855-866.

21. Labadie, C., & Legner, C. (2023). Building data management capabilities to address data protection regulations: Learnings from EU-GDPR. *Journal of Information Technology.* 38(1), pp. 16-44. https://doi.org/10.1177/02683962221141456

22. Tang, A. *Privacy in Practice: Establish and Operationalize a Holistic Data Privacy Program.* Taylor & Francis Group. 2023, 450 p.

23. World Economic Forum. Global Cybersecurity Outlook 2025. Geneva: World Economic Forum, 2025. 44 p. URL: https://www.weforum.org/reports/global-cybersecurity-outlook-2025

Дата надходження статті: 06.12.2025
Дата прийняття статті: 16.12.2025
Дата публікації статті: 29.12.2025