

DOI: <https://doi.org/10.32782/2524-0072/2025-78-22>

УДК 005.96:004.9:342.7(477):061.1(4-672EU)

КУЛЬТУРА ІНФОРМАЦІЙНОЇ ПРИВАТНОСТІ В СИСТЕМІ УПРАВЛІННЯ ПЕРСОНАЛОМ

CULTURE OF INFORMATION PRIVACY IN THE PERSONNEL MANAGEMENT SYSTEM

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 розглянуто проблему формування культури інформаційної приватності (захисту персональних даних) в системі управління персоналом в контексті євроінтеграції України. На основі огляду академічної літератури вирізнено основні підходи у дослідженнях зв'язку культури та інформаційної приватності. Перший підхід наголошує на важливості врахування культури країни (регіону) як одного із факторів впливу на режими державного регулювання захисту даних, а також на орієнтації та практики громадян щодо приватності (що є зовнішнім оточенням для організації). Другий підхід зосереджує увагу на такому явищі, як культура приватності в організації, необхідності формування культури захисту даних в системі управління персоналом. Підкреслено важливість розробки методик оцінювання культури інформаційної приватності. Наголошено на практичній значущості досліджень культури захисту даних у системі управління персоналом в контексті євроінтеграції країни.

Ключові слова: управління персоналом, захист персональних даних, інформаційна приватність, культура приватності, організаційна культура, євроінтеграція України.

The article explores the pressing issue of cultivating a culture of information privacy (the protection of personal data) within human resource management systems in the context of Ukraine's European integration. Given the growing role of digital technologies and the increasing demand for data confidentiality, the development of a privacy-conscious culture is becoming critically important. The purpose of the article is to substantiate the importance of forming a culture of information privacy in the personnel management system of organizations, as well as to analyze the role of data protection culture in society, including its influence as an external context on the development of a privacy culture in an organization. The concepts of information privacy and personnel management systems were considered. Based on an analysis of contemporary academic literature, two key approaches to studying the relationship between culture and information privacy are identified. The first approach emphasizes the macro level – cultural characteristics of a country or region, including traditions, values, and social attitudes – which influence national data protection policies and shape citizens' behaviors and expectations regarding privacy. These factors form the external environment in which organizations operate. The second approach focuses on the organizational culture level – highlighting the need to foster a culture of information privacy within human resource management systems. This includes implementing systemic measures to raise employee awareness, develop ethical standards, and create a secure informational environment. Special attention is given to the development of methodologies for assessing the maturity of information privacy culture at various levels: organizational, sectoral, and national. The article underscores the practical significance of such research in helping Ukrainian institutions align with European standards for personal data protection, which is a vital component of the country's integration into the European Union.

Keywords: personnel management, personal data protection, information privacy, privacy culture, organizational culture, European integration of Ukraine.

Постановка проблеми. Захист персональних даних, дотримання організаціями інформаційної приватності громадян є одним

із важливих напрямків становлення стійкої до ризиків і загроз політики демократичних держав. Право на приватність, право на нерозго-

лошення особистої інформації є ключовими правами громадянина, а також важливими передумовами реалізації інших основоположних прав і свобод. Стрімка цифровізація повсякденного та економічного життя, поширення державних і комерційних послуг в онлайн-середовищах поряд із незаперечними перевагами підвищують ризики витоку персональних даних та кіберзагрози для громадян, організацій та урядів. Збирання «великих даних», просування персоналізованої реклами на основі неявного онлайн-відстеження уподобань зробило персональні дані новим джерелом прибутків для власників особливо великих онлайн-платформ, корпорацій у різних галузях цифрової, основаної на даних економіки. Виникає конфлікт між економічною вигодою та дотриманням прав людини.

В таких умовах уряди багатьох держав, а також міждержавних утворень впроваджують нові чи оновлені законодавчі норми і регуляції для захисту і управління персональними даними громадян. Значним кроком уперед стало прийняття і з 2018 року впровадження у практику Загального регламенту про захист даних (GDPR) у країнах Європейського союзу. Регламент запроваджує значні зобов'язання щодо захисту даних для всіх організацій в Європейському Союзі та тих, хто веде бізнес з громадянами ЄС [1].

Прийнятий Україною курс на євроінтеграцію передбачає гармонізацію важливих законодавчих норм, зокрема й тих, що стосуються захисту даних, а також відповідального впровадження їх в практику організацій. У нинішній ситуації повномасштабної війни з РФ, яка несе щоденні людські жертви, руйнації матеріальної, в тому числі інформаційно-комунікативної інфраструктури, постійні загрози інформаційній безпеці, а також труднощі з управлінням людськими ресурсами, ці завдання є складним викликом.

Одним із напрямів дослідження механізмів впровадження правового регулювання захисту персональних даних на державному і організаційному рівнях є врахування пов'язань культури та приватності. Ці зв'язки не є прямими, а радше множинними і взаємозалежними. Культура на будь-якому рівні – індивідуальному, груповому, організаційному, національному, міжнаціональному – є складним, усталеним і водночас динамічним явищем, яке видозмінюється у часі під впливом значущих подій і обставин. Прийняття нових законодавчих норм, їх впровадження, медій-

ний супровід ініціатив можуть створювати нове середовище для культурних настанов і практик. Разом із тим традиційні цінності і настанови, усталені культурні преференції і практики в суспільствах можуть сприяти чи ні появі нових законів, впливати на темпи їх впровадження, зокрема, у системи управління персоналом.

Аналіз останніх досліджень і публікацій.

У вітчизняних дослідженнях приділено увагу проблемам формування інформаційної культури особи, зокрема, у працях О. Прудникової [2], К. Белякова [3], інформаційної безпеки людини – у роботі О. Золотар [4], інформаційного права та законодавства – у працях В. Брижка, В. Фурашева [5], правового регулювання захисту персональних даних – у працях О. Горпинюк, М. Бема, І. Городиського [6, 7], протидії кібератакам на рівні підприємства, в тому числі як загрози конфіденційній інформації, зокрема у працях І. Каліної та ін. [8]. Питання захисту даних працівника є одним із ключових в системі управління персоналом і особливо актуальним в часи кризи, війни, трансформацій, що розкрито, зокрема, у працях С. Гусарова, К. Мельника [9], К. Кошеленка [10].

В англомовній академічній літературі останнім десятиліттям багато уваги приділено питанням ролі культури у становленні політик і практик інформаційної приватності, захисту персональних даних. Для нас важливими є оглядові праці P. Pavlou [11] та E. Engström et al [21], порівняльний аналіз політик захисту даних R. Guay & K. Birch [16], культурно-антропологічний підхід Y. Li [20], досвід емпіричних досліджень зв'язків культури суспільства та настанов щодо захисту персональних даних, зокрема S. Cockcroft, S. Rekker [22], S. Negash et al [24]. Значна частина емпіричних розвідок базується на концепції типів культури, запропонованої Г. Гофстеде, та її модифікацій [17; 18; 23]. Для аналізу проблеми формування культури приватності в організації джерелами слугували праці M. Qureshi [26], A. Da Veiga [27], L. Iwaya et al [25].

Виділення невирішених раніше частин загальної проблеми. Попри значний внесок вітчизняних і зарубіжних дослідників у вивчення різних аспектів проблеми захисту персональних даних, питань інформаційної культури, організаційної культури, управління персональними даними працівника в організації тощо, проблема дослідження ролі культури у регулюванні інформаційної приватності та формування культури захисту даних

в системі управління персоналом потребує окремої уваги.

Формулювання цілей статті (постановка завдання). Метою статті є обґрунтування важливості формування культури інформаційної приватності в системі управління персоналом організацій, а також аналіз ролі культури захисту даних у суспільстві, включаючи її вплив як зовнішнього контексту на розвиток культури приватності в організації.

Виклад основного матеріалу дослідження. Щодо понять «інформаційна приватність» та «система управління персоналом». Інформаційну приватність вивчають представники різних дисциплін – права, управління, економіки, психології, соціології, маркетингу, менеджменту, інформаційних систем тощо [11]. У вітчизняних соціальних і правових дисциплінах значну увагу приділено аналізу понять, пов'язаних із правом на інформаційну приватність. Так, О. Горпинюк формулює поняття інформаційної приватності таким чином: частина життєдіяльності особи, стосовно інформації про яку особа на власний розсуд встановила межі та умови її нагромадження, зберігання, впливу і розповсюдження для будь-яких сторонніх суб'єктів. Тоді *право на інформаційну приватність* стосується контролю особи за збиранням та обігом відомостей про приватне життя, встановлення режиму конфіденційності приватної інформації та право на збереження приватної інформації в таємниці [6, с. 26, 28, 29].

У вітчизняній традиції право на інформаційну приватність є компонентом права на приватність. Законодавство України включає норми щодо захисту персональних даних [12], а також передбачає кримінально-правову охорону інформаційної приватності. Персональні дані – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована (абзац 10 статті 2 Закону України «Про захист персональних даних»).

Розвиток інформаційного суспільства актуалізував потребу в спеціальних правилах збору та використання особистої інформації, що сприяло становленню концепції «інформаційної приватності». Ця концепція призвела до появи спеціальних правових норм для захисту персональних даних [13, с. 22]. В європейській традиції право на повагу до приватного життя та право на захист персональних даних є різними правами, хоча й тісно пов'язаними. В Преамбулі GDPR право на інформаційну приватність визнається осно-

воположним правом людини. Новий законопроект «Про захист персональних даних», що досить повно відповідає вимогам GDPR, був ухвалений у першому читанні Верховною Радою у листопаді 2024 року [14], що свідчить про рух до гармонізації засад захисту персональних даних в українському та європейському праві.

Серед акторів, які можуть порушувати / втручатися у приватність, виділяють наступні: інші особи, організації, держави. Організації можуть мати справу із обробкою персональних даних їхніх клієнтів, користувачів послуг (покупці, пацієнти, тощо), а отже мають дотримуватися правових регламентів управління такими даними. Окрім цього, кожна організація має юридичні зобов'язання щодо захисту персональних даних працівників у робочому середовищі та має впроваджувати належні заходи приватності для пом'якшення ризиків у таких сферах, як моніторинг робочого місця, обробка чутливих особистих даних тощо. Захист персональних даних стосується всіх основних функціональних сфер системи управління персоналом: рекрутинг та відбір, навчання та розвиток, управління ефективністю, дизайн робочих місць та роботи, управління талантами, компенсації та пільги тощо [15].

Культура країни (регіону) як фактор впливу на політики та настанови щодо інформаційної приватності. Дослідники виходять із припущення, що у різних культурах (за одиницю аналізу можуть слугувати країни, наддержавні союзи, наприклад, ЄС, регіони тощо) люди по-різному сприймають такі явища, як фізична, інформаційна, комунікаційна приватність, конфіденційність персональних даних тощо. Ці відмінності різних культур можуть обумовлювати настанови і поведінку індивідів в онлайн-середовищі, управління даними в організаціях, більше того – можуть впливати на формування державних політик щодо захисту даних. Так, у розвідці «Порівняльний аналіз управління даними: соціотехнічні уявлення про цифрові персональні дані в США і ЄС у 2008–2016 роки» [16] автори показують відмінності науково-технічного (наприклад, збір даних), політико-економічного (зокрема, комерціалізація даних) і правового (захист персональних даних) контексту, у якому розвивалося управління даними в США та ЄС. Для США характерний компроміс між соціально-економічними перевагами економіки даних і ризиками для приватності, тоді як в ЄС акцент зроблено на цінності дотри-

мання демократичних прав. Автори дослідження обрали культурно-аналітичний підхід і доводять, що соціотехнічні уявлення (тобто інституційне домінування специфічних ціннісно-нормативних дискурсів) є впливовим фактором для розробки практичних кроків щодо регулювання та управління інформаційною приватністю у різних юрисдикціях.

Поширеним способом для емпіричної перевірки гіпотез щодо впливу типу культури країни на різні аспекти інформаційної приватності є методологія Г. Гофстеде у різних її модифікаціях [17; 18]. На сьогодні функціонує авторський сайт, де можна порівняти виміри «культурного індексу» за допомогою співставлення кількості балів за шкалою від 0 до 100 для різних країн [19]. Цей підхід широко використовують у крос-культурній психології [20], дослідженнях менеджменту організацій (особливо транснаціональних компаній), тощо. Найчастіше для емпіричних досліджень обирають індекси «колективізм проти індивідуалізму» та «уникання невизначеності» [21]. Для «колективістських» культур є характерним, що групи (тобто, родина, родичі, колеги, країна) пов'язують і зобов'язують індивідів діяти певним чином, тоді як в «індивідуалістських» культурах поширені настанови, що індивіди є незалежними один від одного.

Автори розвідки «Зв'язки між культурою та політикою інформаційної приватності» [22] у дослідженні розвитку законодавства про захист даних у 35 країнах використовували культурні індекси за методологією GLOBE «Глобальне лідерство та ефективність організаційної поведінки» (модифікований варіант моделі Г. Гофстеде) [23]. Одним із висновків аналізу є те, що зв'язок між культурою країни і регулюванням даних є значуще негативним, коли рівень показника «колективізм» високий. На думку авторів, показники культурних індексів країн, на кшталт «дистанція влади» чи «уникання невизначеності» здатні пояснити високий чи низький рівень захищеності інформаційної приватності в законодавстві країни [22].

Дослідження «Взаємодія між культурою, регуляторною структурою та інформаційною приватністю в різних країнах» [24] направлене на з'ясування впливу країни (США, Великобританія, Індія, Гонконг) та її регуляторної структури на ставлення до проблем інформаційної приватності. Ці країни уособлювали різні типи культур за типологією Г. Гофстеде: індивідуалістична (США, Великобританія), колективістична (Індія), змішана (Гонконг).

Однією із гіпотез було припущення, що культурні настанови та нормативні системи впливають на ставлення до приватності. Було опитано 1086 фахівців, які працюють у сфері ІКТ, управління даними, кібербезпеки, аналітики даних, управління транскордонними потоками даних користувачів. Дійсно, фахівці з США і Великобританії (індивідуалістичний тип культури) продемонстрували високу чутливість щодо втрати контролю над особистими даними, активно використовуючи інструменти контролю (зокрема, VPN). Респонденти з Індії (колективістичний тип) виявляли менше стурбованості щодо приватності, частіше покладалися на державний контроль та соціальні норми взаємодії, ніж на технології. На думку дослідників, проведений аналіз підтвердив, що культура країни є важливим фактором в управлінні інформаційною приватністю, саме культурний фактор пояснює відмінності у ставленні до можливого розкриття особистої, конфіденційної інформації. Культурна належність пояснює відмінності у занепокоєнні опитуваних фахівців щодо повторного використання даних, помилок в даних, несанкціонованого використання даних, контролю за збором даних та усвідомлення проблеми приватності даних.

Результати досліджень про вплив культури країни на політики, настанови і практики захисту даних є надзвичайно корисними для розробки стратегій і тактик управління приватністю в організаціях, а також для розуміння ролі зовнішнього культурного середовища у формуванні організаційної культури.

Культура інформаційної приватності в системі управління персоналом організації. Іншим ракурсом досліджень зв'язків культури та управління приватністю є аналіз такого явища, як культура (інформаційної) приватності / культура захисту персональних даних в організації. Термінологія не є усталеною, можна зустріти й інші дотичні поняття, наприклад, культура та атмосфера приватності в організації (Organisational Privacy Culture and Climate) [25]. Мова йде про специфічні цінності, норми, знання, настанови, навички, практики, які стосуються захисту персональних даних в організації і надзвичайно актуалізуються в умовах цифрового суспільства та стрімкого розповсюдження нових інформаційних технологій, комерціалізації даних, кіберзагроз.

Культура інформаційної приватності є компонентом організаційної культури. У розвідці «Розбудова культури приватності» [26]

автор пропонує практичне керівництво для організацій у впровадженні культури приватності, щоб забезпечити не лише відповідність нормативно-правовим актам, але й досягти довіри персоналу. Він наголошує, що саме організаційна культура допомагає підприємствам виживати у конкурентному середовищі. Культура приватності повинна відповідати ціннісній системі підприємства, компанії. У моделях факторів, що впливають на організаційну культуру, зазвичай виділяють: а) фактори середовища (національні та релігійні цінності, освіта, галузь тощо); б) фактори самої організації (розмір, стиль керівництва, управління аспектами організаційної культури); в) практики управління персоналом, такі як тренінги, залучення співробітників, ефективна комунікація, системи заохочень тощо. На прикладі корпоративної культури можна бачити напрями інтеграції бізнес-процесів і політик приватності, від гармонізації яких залежить формування культури приватності (табл. 1).

Культуру приватності в організації характеризують спільні цінності, переконання, норми щодо захисту персональних даних. Ця культура формується з часом і вимагає значних зусиль, тому що пов'язана із різними напрямками, процесами в організації, впливає на політики, стратегії, поведінку. Культура приватності демонструє, як організація дотримується регулятивних правил і цінує проблему захисту даних [25]. В ефективній культурі приватності захист персональних даних є пріоритетом. Важливо розробляти стратегії, що перетворюють знання про приватність на постійні практики [26].

Важливим елементом формування культури інформаційної приватності є постійний моніторинг її стану – як на перших етапах оцінки слабких місць і прогалин та планування реальних кроків для її впровадження, так і для регулярного аудиту дотримання цінностей та норм приватності. В зв'язку з цим важливою є пропозиція дослідницького інструменту опитування для оцінки стану культури інформаційної приватності [27]. У праці A. Da Veiga представлено набір питань для емпіричного опитування, який має назву «Інструмент Індексу культури інформаційної приватності», розроблений і апробований для вимірювання очікувань і настанов респондентів щодо захисту персональних даних. Індекс базується на трьох компонентах: очікування щодо приватності; реальний досвід взаємодії з організаціями; загальний рівень занепокоєння щодо приватності. Аналіз отримуваних через опитування емпіричних даних направлений на виявлення розриву між очікуваннями і реальним станом речей. Як наголошує авторка, індекс дозволяє кількісно оцінити культуру приватності в організації, галузі або в цілому у країні / між країнами [27]. Практичне значення таких замірів полягає у можливості самооцінки організації і вдосконалення політик і культури приватності, що може бути корисним і в українському контексті.

Висновки. Міждисциплінарна зацікавленість проблемами захисту персональних даних, політик інформаційної приватності як права громадян та складних зв'язків практик дотримання цього права із культурними цінностями, нормами, дискурсами призвела до

Таблиця 1

Інтеграція бізнес-процесів і політик приватності

Стратегія	Управління персоналом	Ланцюги поставок	Право	Проект-менеджмент	Технологія	Фінанси	Інциденти та кризис-менеджмент
Стратегічний напрям та інтеграція приватності	Захист персональних даних працівників на всіх етапах кар'єри	Приватність у проведенні тендерів та заключенні контрактів	Приватність у заключенні контрактів	Приватність за дизайном	Системи і контроль мережі	Інтеграція приватності до фінансових систем	Реагування на інциденти із приватності
Зобов'язання та підтримка керівництва	Тренінги та усвідомленість	Захист інформації поставальників	Визначення дотичних законів щодо приватності	Вдосконалення існуючих систем для покращення захисту приватності	Захист баз даних	Фінансові ресурси для забезпечення приватності	Кризис-менеджмент та медіа-менеджмент

Джерело: [26]

появи значного корпусу академічних розвідок, більша частина яких базується на результатах емпіричних досліджень. Ці напрацювання потребують глибшого осмислення і структурування, як показують результати представленого аналізу. Було вирішено два узагальнені напрями досліджень: вплив типу культури країни чи регіону на державні режими регулювання інформаційної приватності, а також на орієнтації і практики громадян / фахівців у сфері захисту даних щодо дотримання безпечних режимів поведінки із даними. Другий напрям стосується актуальності культури приватності в організації, активну роль у формуванні якої відіграє система управління персоналом.

Ці дослідження мають практичне значення для захисту даних в організації. Результати напрацювань в рамках першого із напрямів підкреслюють необхідність врахування культурної складової під час впровадження регуляторних заходів із захисту даних. Ці заходи не можуть бути універсальними, вони мають враховувати специфічні, локальні контексти обміну інформацією, наприклад, суспільні

орієнтації на індивідуальні досягнення чи дотримання соціальних норм. Результати досліджень в рамках другого підходу актуалізують проблеми цінності персональних даних, інформаційної грамотності, (не)поширеності орієнтацій щодо важливості дотримання інформаційної приватності, цифрової гігієни, кібербезпеки – в організаціях та ширше – у суспільному житті. Важливим є підхід, направлений на розробку методик оцінювання стану культури приватності в організаціях.

В Україні, яка знаходиться у стані повномасштабної війни з РФ, тим не менше йде активна робота з гармонізації правових засад захисту персональних даних з європейським правом. Частина організацій, які мають міжнародні зв'язки і обробляють дані громадян ЄС, вже мають дотримуватися у своїй діяльності норм європейського права. Отже, формування культури інформаційної приватності в організації, та ширше – у всьому суспільстві, потребує подальших досліджень, направлених на опрацювання конкретних методик і взірців та впровадження їх у практику.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Strzelecki, A., Rizun, M. (2020). Consumers' security and trust for online shopping after GDPR: examples from Poland and Ukraine. *Digital Policy, Regulation and Governance*. Vol. 22 (4). 289–305.
2. Прудникова О. В. Феномен інформаційної культури: онтологічний статус та соціоантропологічні детермінанти: монографія / за заг. ред. О. П. Дзьобаня. Харків : Право, 2017. 496 с.
3. Беляков К. І., Онопрієнко С. Г., Шопіна І.М. Інформаційна культура в Україні: правовий вимір: монографія / за заг. ред. К. І. Белякова. Київ : КВІЦ, 2018. 168 с.
4. Золотар О. О. Інформаційна безпека людини: теорія і практика: монографія. Київ : ТОВ "Видавничий дім "АртЕк", 2018. 446 с.
5. Брижко В. М., Фурашев В. М. Інформаційне право та інформаційне законодавство: наукове видання. – 2-ге вид., доповнене. Харків : Право, 2021. 288 с.
6. Горпинюк О. П. Інформаційна приватність та її захист від злочинних посягань в Україні: монографія. Львів : Бона, 2014. 324 с.
7. Бем М., Городиський І. Захист персональних даних: правове регулювання та практичні аспекти: науково-практичний посібник. Київ : Рада Європи, 2021. 220 с.
8. Каліна І., Шуляр Н., Грищенко А. Економічні виклики діяльності підприємства під час кібератак в умовах жорсткої конкурентності. *Цифрова економіка та економічна безпека*. 2023. № 9 (09). С. 14–20. DOI: <https://doi.org/10.32782/dees.9-3>
9. Гусаров С. М., Мельник К. Ю. Захист персональних даних працівника. *Право і безпека*. 2023. № 2 (89). С. 133–144. DOI: <https://doi.org/10.32631/pb.2023.2.12>
10. Кошеленко К. Менеджмент у часи війни. Лідерство, ефективність та життєстійкість. Київ : Кінцевий бенефіціар, 2024. 320 с.
11. Pavlou P. A. State of the information privacy literature: Where are we now and where should we go? *MIS Quarterly: Management Information Systems*, 2011. Vol. 35(4). P. 977–988.
12. Закон України «Про захист персональних даних», №2297-VI від 01.06.2010. Відомості Верховної Ради України. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>
13. Посібник з європейського права у сфері захисту персональних даних / [Агенція Європейського Союзу з питань основоположних прав ; Рада Європи ; Європейський суд з прав людини] ; пер. з англ. В. Кастеллі. Київ : К.І.С., 2020. 432 с.

14. Проект Закону України «Про захист персональних даних», № 8153 від 25.10.2022. Верховна Рада України, 2024. URL: <https://itd.rada.gov.ua/billinfo/Bills/Card/40707>
15. Armstrong M. *Armstrong's handbook of human resource management practice*. London: Kogan Page, 2014. 792 p.
16. Guay, R., Birch, K. (). A comparative analysis of data governance: Socio-technical imaginaries of digital personal data in the USA and EU (2008–2016). *Big Data & Society*. 2022. Vol. 9(2). DOI: <https://doi.org/10.1177/20539517221112925>
17. Hofstede G., Hofstede G.J., Minkov M. *Cultures and Organizations: Software of the Mind*. 3rd ed. New York: McGraw Hill Professional, 2010. 576 p.
18. Hofstede G. Replicating and Extending Cross-National Value Studies: Rewards and Pitfalls – An Example from Middle East Studies. *AIB Insights*. 2013. Vol. 13(2). P. 3–4.
19. Hofstede Insights. *Country comparison bar charts*. URL: <https://geerthofstede.com/country-comparison-bar-charts/>
20. Li Y. Cross-Cultural Privacy Differences. In: Knijnenburg, B.P., Page, X., Wisniewski, P., Lipford, H.R., Proferes, N., Romano, J. (eds.) *Modern Socio-Technical Perspectives on Privacy*. Springer, Cham, 2022. DOI: https://doi.org/10.1007/978-3-030-82786-1_12
21. Engström E., Eriksson K., Björnstjerna M., Strimling P. Global variations in online privacy concerns across 57 countries. *Computers in Human Behavior Reports*. 2023, 9, Article 100268. DOI: <https://doi.org/10.1016/j.chbr.2023.100268>
22. Cockcroft S., Rekker S. The relationship between culture and information privacy policy. *Electron Markets*. 2016. Vol. 26, P. 55–72. DOI: <https://doi.org/10.1007/s12525-015-0195-9>
23. Culture, leadership and organizations: The GLOBE study of 62 societies. (Eds). House R.J., Hanges P. J., Javidan M., Dorfman P. W., Gupta V. Thousand Oaks, CA: Sage, 2004. 848 p.
24. Negash S., Meso P., Musa P. F. Interactions between culture, regulatory structure, and information privacy across countries. *Journal of Global Information Management*. 2021. Vol. 29(6). P. 1–14. DOI: <https://doi.org/10.4018/JGIM.20211101.0a23>
25. Iwaya L. H., Iwaya G. H., Fischer-Hübner S., Steil A. V., Organisational Privacy Culture and Climate: A Scoping Review. *IEEE Access*. 2022. Vol. 10, P. 73907–73930. DOI: <https://doi.org/10.1109/ACCESS.2022.3190373>
26. Qureshi M.A. Building a Privacy Culture. In: *A Global Look at Privacy 2020: ISACA Research Report*. 2020. URL: <https://www.isaca.org/resources/isaca-journal/issues/2020/volume-5/building-a-privacy-culture>
27. Da Veiga A. An information privacy culture instrument to measure consumer privacy expectations and confidence. *Information & Computer Security*, 2018. Vol. 26(3). P. 338–364. DOI: <https://doi.org/10.1108/ics-03-2018-0036>

REFERENCES:

1. Strzelecki, A., Rizun, M. (2020). Consumers' security and trust for online shopping after GDPR: examples from Poland and Ukraine. *Digital Policy, Regulation and Governance*, 22 (4), 289–305.
2. Prudnykova, O. V. (2017) Fenomen informatsiinoi kultury: ontologichnyi status ta sotsioantropolohichni determinanty [The phenomenon of information culture: ontological status and socio-anthropological determinants]. monohrafiya [a monograph]. Kharkiv : Pravo. 496 p. (in Ukrainian)
3. Bielakov, K. I., Onopriienko, S. H., Shopina, I. M. (2018) Informatsiina kultura v Ukraini: pravovyi vymir [Information culture in Ukraine: legal dimension]. monohrafiya [a monograph]. Kyiv : KVITS. 168 p. (in Ukrainian)
4. Zolotar, O. O. (2018) Informatsiina bezpeka liudyny: teoriia i praktyka [Information security of the individual: theory and practice]. monohrafiya [a monograph]. Kyiv : Vydavnychiy dim "Artek". 446 p. (in Ukrainian)
5. Bryzhko, V. M., Furashev, V. M. (2021) Informatsiynе pravo ta informatsiynе zakonodavstvo [Information law and information legislation]. naukove vydannia [a scientific edition]. 2-he vyd., dopovnene [2nd ed., revised]. Kharkiv : Pravo. 288 p. (in Ukrainian)
6. Gorpyniuk, O.P. (2014) Informatsiina pryvatnist ta yii zakhyst vid zlochyynykh posiahann' v Ukraini [Information privacy and its protection from criminal encroachments in Ukraine]. monohrafiya [a monograph]. Lviv: Bona. 324 p. (in Ukrainian)
7. Bem, M., Horodyskyi, I. (2021) Zakhyst personal'nykh danykh: pravove rehuliuвання ta praktychni aspekty [Protection of personal data: Legal regulation and practical aspects]. nauko-vo-praktychnyi posibnyk [a scientific-practical guide]. Kyiv : Rada Yevropy. 220 p. (in Ukrainian)
8. Kalina, I., Shuliar, N., Hryshchenko, A. (2023) Ekonomichni vyklyky diialnosti pidpriemstva pid chas kiberatak v umovakh zhorstkoї konkurentnosti [Economic challenges of enterprise activity during cyberattacks under

conditions of intense competition]. *Tsyfrova ekonomika ta ekonomichna bezpeka* [Digital Economy and Economic Security], 9 (09), 14–20. DOI: <https://doi.org/10.32782/dees.9-3> (in Ukrainian)

9. Husarov, S. M., Melnyk, K. Yu. (2023) Zakhyst personal'nykh danykh pratsivnyka [Protection of employee's personal data]. *Pravo i bezpeka* [Law and Safety], 2 (89), 133–144. DOI: <https://doi.org/10.32631/pb.2023.2.12> (in Ukrainian)

10. Koshelenko, K. (2024) Menedzhment u chasy viiny. Liderstvo, efektyvnist ta zhyttiistiikist [Management in times of war. Leadership, effectiveness and resilience]. monohrafiya [a monograph]. Kyiv : Kintsevyi benefitsiarii. 320 p. (in Ukrainian)

11. Pavlou, P.A. (2011). State of the information privacy literature: Where are we now and where should we go? *MIS Quarterly: Management Information Systems*, 35(4). 977-988.

12. Zakon Ukrainy "Pro zakhyst personal'nykh danykh", No. 2297-VI vid 01.06.2010 [Law of Ukraine "On Personal Data Protection", No. 2297-VI of June 1, 2010]. Vidomosti Verkhovnoi Rady Ukrainy [Official Bulletin of the Verkhovna Rada of Ukraine]. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text> (in Ukrainian)

13. Handbook on European data protection law / [Ahentsiia Yevropeiskoho Soiuzu z pytan' osnovopolozhnykh prav ; Rada Yevropy ; Yevropeyskyi sud z prav liudyny] ; transl. from English by V. Kastelli. Kyiv : K.I.S., 2020. 432 p. (in Ukrainian)

14. Proekt Zakonu Ukrainy "Pro zakhyst personal'nykh danykh", No. 8153 vid 25.10.2022 [Draft Law of Ukraine "On Personal Data Protection", No. 8153 of October 25, 2022]. Verkhovna Rada Ukrainy [Parliament of Ukraine], 2024. URL: <https://itd.rada.gov.ua/billinfo/Bills/Card/40707> (in Ukrainian)

15. Armstrong, M. (2014). *Armstrong's handbook of human resource management practice* (13th ed.). Kogan Page.

16. Guay, R., Birch, K. (2022). A comparative analysis of data governance: Socio-technical imaginaries of digital personal data in the USA and EU (2008–2016). *Big Data & Society*, 9(2). DOI: <https://doi.org/10.1177/20539517221112925>

17. Hofstede, G., Hofstede, G.J., Minkov, M. (2010). *Cultures and Organizations: Software of the Mind*. 3rd ed. New York: McGraw Hill Professional.

18. Hofstede, G. (2013). Replicating and Extending Cross-National Value Studies: Rewards and Pitfalls – An Example from Middle East Studies. *AIB Insights*. 13(2), 3–4.

19. Hofstede Insights. (2025.). *Country comparison bar charts*. URL: <https://geerthofstede.com/country-comparison-bar-charts/>

20. Li, Y. (2022). Cross-Cultural Privacy Differences. In: Knijnenburg, B.P., Page, X., Wisniewski, P., Lipford, H.R., Proferes, N., Romano, J. (eds) *Modern Socio-Technical Perspectives on Privacy*. Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-82786-1_12

21. Engström, E., Eriksson, K., Björnstjerna, M., Strimling, P. (2023). Global variations in online privacy concerns across 57 countries. *Computers in Human Behavior Reports*, 9, Article 100268. DOI: <https://doi.org/10.1016/j.chbr.2023.100268>

22. Cockcroft, S., Rekker, S. (2016). The relationship between culture and information privacy policy. *Electron Markets*. 26, 55–72. DOI: <https://doi.org/10.1007/s12525-015-0195-9>

23. House, R.J., Hanges, P. J., Javidan, M., Dorfman, P. W., & Gupta, V. (Eds) 2004. Culture, leadership and organizations: The GLOBE study of 62 societies. Thousand Oaks, CA: Sage.

24. Negash, S., Meso, P., & Musa, P. F. (2021). Interactions between culture, regulatory structure, and information privacy across countries. *Journal of Global Information Management*, 29(6), 1–14. DOI: <https://doi.org/10.4018/JGIM.20211101.0a23>

25. Iwaya, L. H., Iwaya, G. H., Fischer-Hübner, S., Steil, A. V. (2022) Organisational Privacy Culture and Climate: A Scoping Review. *IEEE Access*. 10, 73907–73930. DOI: <https://doi.org/10.1109/ACCESS.2022.3190373>

26. Qureshi, M.A. (2020). Building a Privacy Culture. In: A Global Look at Privacy 2020: ISACA Research Report. URL: <https://www.isaca.org/resourses/isaca-journal/issues/2020/volume-5/building-a-privacy-culture>

27. Da Veiga, A. (2018). An information privacy culture instrument to measure consumer privacy expectations and confidence. *Information & Computer Security*, 26(3), 338–364. DOI: <https://doi.org/10.1108/ics-03-2018-0036>