

УДК 342.7:004.056

Дуліна Оксана Василівна

*кандидат юридичних наук, доцент,
доцент кафедри публічного управління
та регіоналістики*

*Навчально-науковий інститут публічної
служби та управління*

Національний університет

«Одеська політехніка»

ORCID: 0000-0002-1009-558X

Куспляк Ігор Сергійович

*кандидат політичних наук, доцент,
доцент кафедри публічного управління
та регіоналістики,
заступник директора*

*Навчально-наукового інституту публічної
служби та управління*

Національний університет

«Одеська політехніка»

ORCID: 0000-0003-1494-5008

Сівак Володимир Михайлович

*доктор філософії в галузі права,
доцент кафедри публічного управління
та регіоналістики*

*Навчально-науковий інститут публічної
служби та управління*

Національний університет

«Одеська політехніка»

ORCID: 0009-0007-4854-1585

<https://doi.org/10.25313/3083-7774-2026-5-10>

ІНФОРМАЦІЙНО-ПРАВОВИЙ МЕХАНІЗМ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У КОРПОРАТИВНІЙ СФЕРІ

Анотація. Вступ. Цифровізація господарської діяльності істотно трансформує корпоративні процеси, пов'язані зі збиранням, зберіганням, використанням, передаванням і захистом персональних даних. Використання CRM-, ERP-, HRM-систем, хмарних сервісів, електронного документообігу, платформ електронної комерції, IoT-рішень та технологій штучного інтелекту розширює масштаби корпоративної обробки інформації про працівників, клієнтів, контрагентів і користувачів цифрових сервісів. Водночас це посилює ризики незаконного доступу, витоку, профілювання, надмірного збирання та неправомірного використання персональних даних. У зв'язку з цим актуалізується потреба у комплексному дослідженні інформаційно-правового механізму захисту персональних даних у корпоративній сфері.

Мета. Метою дослідження є комплексний аналіз інформаційно-правового механізму захисту персональних даних у корпоративній сфері, визначення його правових, організаційних і технологічних складових, а також обґрунтування напрямів удосконалення корпоративної моделі обробки персональних даних з урахуванням міжнародних і європейських стандартів.

Матеріали і методи. Матеріалами дослідження є: 1) міжнародні та європейські акти у сфері захисту персональних даних, зокрема Конвенція Ради Європи № 108 та GDPR; 2) нормативно-правові акти України, що регулюють інформаційні відносини, захист персональних даних, електронний документообіг, електронну комерцію, кібербезпеку та відповідальність за порушення у сфері обробки даних; 3) законопроект № 8153 щодо модернізації національного законодавства про захист персональних даних; 4) наукові праці вітчизняних авторів, присвячені проблематиці персональних даних, інформаційної безпеки, корпоративного compliance, HRM-систем, хмарних сервісів та IoT-рішень. У процесі дослідження використано формально-юридичний метод, порівняльно-правовий метод, системно-структурний аналіз, метод класифікації, узагальнення та логіко-правового моделювання.

Результати. У статті розкрито зміст інформаційно-правового механізму захисту персональних даних у корпоративній сфері. Проаналізовано положення Конвенції Ради Європи № 108, GDPR та перспективи модернізації національного законодавства у зв'язку із законопроектом № 8153. Охарактеризовано вітчизняне нормативне забезпечення захисту персональних даних, включаючи інформаційне, цифрове, адміністративне, кримінальне та кібербезпечове законодавство. Узагальнено наукові підходи до класифікації персональних даних, визначено їх юридично значущі ознаки та значення у корпоративній сфері. Запропоновано авторське визначення інформаційно-правового механізму захисту персональних даних у корпоративній сфері як комплексної системи нормативного регулювання, внутрішнього корпоративного управління, технічної безпеки, контролю доступу, запобігання витокам, реагування на інциденти та юридичної відповідальності, спрямованої на охорону персональних даних у межах корпоративної діяльності. Визначено правовий, організаційний і технологічний



Copyright © The Author(s).

This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (<https://creativecommons.org/licenses/by/4.0/>)

напрями захисту персональних даних та розкрито їх значення для корпоративного управління, кадрового адміністрування, договірної роботи, електронної комерції, публічних закупівель, хмарних сервісів та інформаційної безпеки.

Перспективи. Подальші наукові дослідження доцільно спрямувати на розроблення практичної моделі корпоративного data protection compliance, удосконалення внутрішніх політик обробки персональних даних, формування процедур оцінки ризиків, реагування на інциденти інформаційної безпеки та забезпечення відповідності корпоративної обробки персональних даних європейським стандартам.

Ключові слова: захист персональних даних, інформаційно-правовий механізм, цифровізація, інформаційна безпека, кібербезпека, електронна комерція, корпоративна безпека, захист інформації, інформаційні технології, суб'єкт господарювання, корпоративна сфера.

Постановка проблеми. Актуальність дослідження інформаційно-правових механізмів захисту персональних даних у корпоративній сфері зумовлена інтенсивною цифровізацією господарської діяльності, глобалізацією інформаційних процесів та істотним зростанням обсягів персональних даних, що обробляються суб'єктами господарювання. Використання CRM-, ERP-, HRM-систем, хмарних сервісів, електронного документообігу, маркетингових платформ, засобів аналітики та технологій штучного інтелекту суттєво розширює можливості компаній щодо збирання, зберігання, передавання, аналізу й використання інформації про працівників, клієнтів, контрагентів і користувачів.

Водночас така інтенсифікація обробки персональних даних породжує нові правові ризики, пов'язані з незаконним доступом до інформації, її витоком, надмірним накопиченням, неправомірним використанням, профілюванням, автоматизованим прийняттям рішень та порушенням права особи на приватність. У корпоративній сфері ці ризики набувають особливої ваги, оскільки персональні дані стають не лише об'єктом правової охорони, а й важливим економічним ресурсом, що використовується у процесах управління, маркетингу, кадрового адміністрування, договірної роботи та цифрової комунікації.

Персональні дані як особливо значуща та чутлива інформація про людину посідають центральне місце в системі сучасних інформаційних відносин. Ефективний захист персональних даних має розглядатися як елемент корпоративної комплаєнс-політики, а також як складова гарантування прав і свобод людини в умовах цифрової економіки.

Особливої актуальності зазначена проблематика набуває для України в контексті європейської правової інтеграції. Чинна модель правового регулювання захисту персональних даних потребує подальшого узгодження з міжнародно-правовими та європейськими стандартами, зокрема з підходами, закладеними в праві Європейського Союзу. Недостатня адаптованість національного законодавства до сучасних викликів цифрової економіки, включаючи використання великих даних, хмарних технологій, алгоритмічної аналітики та штучного інтелекту, створює перешкоди для міжнародного співробітництва, транскордонного обігу даних і діяльності українських компаній, орієнтованих на європейський ринок.

Розвиток цифрових технологій зумовлює необхідність уточнення категоріального апарату у сфері захисту персональних даних, а також наукового осмислення співвідношення приватного інтересу особи, публічного інтересу держави та економічного інтересу корпорацій.

Аналіз останніх досліджень і публікацій. Дослідження міжнародних і європейських стандартів захисту персональних даних у працях О. В. Різенко [1], Р. Б. Тополевського [2], К. С. Мельник [3], В. К. Антошкіної [4], та С. О. Колба [5] формують нормативну основу для аналізу української моделі правового регулювання у контексті її гармонізації з правом Європейського Союзу. У цих працях захист персональних даних розглядається не лише як сукупність юридичних процедур, а як елемент гарантування приватності, інформаційного самовизначення та належного балансу між правами особи, публічними інтересами й потребами цифрової економіки. Особливого значення набуває звернення до стандартів GDPR, які трансформували корпоративний підхід до обробки персональних даних через принципи підзвітності, мінімізації даних, цільового обмеження, безпеки обробки, ризик-орієнтованого управління та ефективного контролю.

Окремий науковий пласт становлять праці, присвячені теоретико-правовому, організаційному та техніко-прикладному вимірам захисту персональних даних. Зокрема, у дослідженнях А. Цюменко [6;7] увагу зосереджено на класифікації персональних даних і їх місці в доктрині адміністративного права, що має значення для уточнення понятійно-категоріального апарату відповідної сфери. В. М. Брижко [8] розглядає організаційно-правові засади захисту персональних даних, формуючи теоретичне підґрунтя для аналізу цього інституту як комплексного правового явища. Прикладний корпоративний вимір проблематики репрезентовано у працях В. Жуляєва [9], який досліджує захист даних у системі управління персоналом в умовах кіберзагроз для інформаційної приватності. Техніко-організаційний аспект забезпечення безпеки персональних даних розкрито у працях Л. Савицької, Т. Коробейнікової, О. Костюк, І. Колесник, О. Дудник [10], присвячених захисту Internet of Things у корпоративній комп'ютерній мережі, а також у дослідженні О. С. Борисенко та А. Г. Тимошенко [11], які аналізують методи захисту персональних даних у хмарному середовищі.

Водночас у науковій літературі недостатньо розробленим залишається комплексне розуміння захисту персональних даних саме у корпоративній сфері як інтегрованої системи правових, організаційних і технологічних засобів.

Мета статті — здійснити аналіз інформаційно-правового механізму захисту персональних даних у корпоративній сфері та обґрунтувати напрями його вдосконалення з урахуванням цифровізації корпоративних процесів, європейських стандартів захисту даних і потреб забезпечення прав суб'єктів персональних даних.

Матеріали і методи. Матеріалами дослідження є міжнародні, європейські та національні нормативно-правові акти, що регулюють захист персональних даних, інформаційну безпеку, електронний документообіг, електронну комерцію, кібербезпеку та відповідальність за порушення у сфері обробки персональних даних. Особливу увагу приділено положенням Конвенції Ради Європи № 108, GDPR, Закону України «Про захист персональних даних», Закону України «Про інформацію», Закону України «Про захист інформації в інформаційно-комунікаційних системах», а також законопроекту № 8153, спрямованому на модернізацію національної моделі захисту персональних даних. Теоретичну основу дослідження становлять наукові праці, присвячені проблемам класифікації персональних даних, корпоративного compliance, цифровізації бізнес-процесів, HRM-систем, хмарних сервісів, IoT-рішень та кібербезпеки.

У процесі дослідження використано формально-юридичний метод — для аналізу змісту нормативно-правових актів у сфері захисту персональних даних; порівняльно-правовий метод — для зіставлення української моделі правового регулювання з міжнародними та європейськими стандартами; системно-структурний метод — для визначення правових, організаційних і технологічних складових інформаційно-правового механізму захисту персональних даних у корпоративній сфері; метод класифікації — для узагальнення видів персональних даних і корпоративних процесів, у межах яких вони обробляються; метод аналізу та синтезу — для встановлення взаємозв'язку між нормативним регулюванням, корпоративним управлінням і технічними засобами захисту інформації; метод логічного узагальнення — для формулювання висновків щодо необхідності впровадження ризик-орієнтованої моделі corporate data protection compliance.

Виклад основного матеріалу. Згідно з міжнародними стандартами, зокрема, Загальною декларацією прав людини, Конвенцією про захист прав людини та основоположних свобод, Міжнародним пактом про громадянські і політичні права право на захист персональних даних є невід'ємною складовою права на повагу до приватного і сімейного життя. У цих актах закріплено основоположні принципи, які мають бути враховані при розробці національного законодавства, як то законність, пропорційність, цільове призначення, мінімізація даних, обмеження строків зберігання, конфіденційність та відповідальність за порушення.

У міжнародно-правовому вимірі захист персональних даних ґрунтується насамперед на стандартах Ради Європи та Європейського Союзу. Базовим міжнародним договором у цій сфері є Конвенція Ради Європи № 108 «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» від 28 січня 1981 року [12], яка закріпила розуміння персональних даних як будь-якої інформації, що стосується ідентифікованої або такої, що може бути ідентифікована, особи. Україна ратифікувала Конвенцію № 108 та Додатковий протокол до неї Законом України від 06.07.2010 № 2438-VI.

Подальшим розвитком цього стандарту стала модернізована Конвенція 108+, затверджена у 2018 році Протоколом CETS № 223. Її мета адаптація захисту персональних даних до викликів цифрових технологій, посилення механізмів реалізації права на захист даних, закріплення принципів прозорості, пропорційності, підзвітності, мінімізації даних і privacy by design. Рада Європи прямо вказує, що модернізація Конвенції 108 спрямована на реагування на виклики нових інформаційно-комунікаційних технологій і посилення ефективності її імплементації [13].

У межах права Європейського Союзу ключовим актом є Регламент ЄС 2016/679 — GDPR, прийнятий Європейським Парламентом і Радою ЄС 27 квітня 2016 року. Для України значення GDPR полягає в необхідності гармонізації національного законодавства з європейською моделлю захисту персональних даних у контексті євроінтеграції. Практичне значення такої гармонізації полягає, зокрема, у наближенні України до механізмів ЄС щодо адекватності рівня захисту даних, що потенційно може спростити транскордонну передачу персональних даних між Україною та державами-членами ЄС [1].

У корпоративній сфері ці міжнародні стандарти мають прикладне значення, оскільки формують модель data protection compliance для суб'єктів господарювання. Вона передбачає законну, прозору, цільову, мінімізовану, точну, безпечну та підзвітну обробку персональних даних працівників, клієнтів, контрагентів і користувачів цифрових сервісів. Для бізнесу це означає необхідність внутрішніх політик обробки даних, контролю доступу, строків зберігання, процедур реалізації прав суб'єктів даних, оцінки ризиків, належного договірної оформлення відносин із підрядниками та забезпечення безпеки корпоративних інформаційних систем.

Отже, Конвенція і GDPR утворюють міжнародно-європейський стандарт захисту персональних даних, який має значення не лише для державного регулювання, а й для корпоративної практики. Для українських суб'єктів господарювання він задає орієнтир переходу від формального дотримання вимог закону

до системного управління персональними даними як елементом корпоративної безпеки, комплаєнсу та правової відповідальності [2].

Нормативне забезпечення захисту персональних даних у корпоративній сфері в Україні має комплексний характер і формується на перетині інформаційного, цивільного, господарського, трудового, адміністративного та цифрового законодавства. Його основу становлять акти, що визначають загальний правовий режим інформації, спеціальні правила обробки персональних даних, вимоги до захисту інформації в інформаційно-комунікаційних системах, електронного документообігу, електронної комерції, електронної ідентифікації та кібербезпеки.

Базове значення має Закон України «Про інформацію» [14], який закріплює загальні правові засади інформаційних відносин, визначає інформацію як відомості та/або дані, що можуть бути збережені на матеріальних носіях або відображені в електронній формі, а також формує загальне розуміння захисту інформації як системи правових, адміністративних, організаційних, технічних та інших заходів. Для корпоративної сфери цей закон має методологічне значення, оскільки персональні дані розглядаються як різновид інформації, що потребує спеціального правового режиму, належного доступу, збереження, цілісності та захисту від неправомірного поширення.

Спеціальним актом у цій сфері є Закон України «Про захист персональних даних» [15], який визначає персональні дані як відомості або сукупність відомостей про фізичну особу, що ідентифікована або може бути конкретно ідентифікована. Цей закон установлює основні принципи обробки персональних даних, права суб'єкта персональних даних, обов'язки володільців і розпорядників, а також загальні вимоги до збирання, зберігання, використання, поширення, знеособлення та знищення таких даних. У корпоративній сфері його положення безпосередньо поширюються на обробку даних працівників, кандидатів на посади, клієнтів, контрагентів, представників юридичних осіб, користувачів цифрових сервісів і споживачів електронної комерції [16].

Важливу роль у забезпеченні технічної складової захисту відіграє Закон України «Про захист інформації в інформаційно-комунікаційних системах» [17]. Він має значення для корпоративних CRM-, ERP-, HRM-систем, хмарних сервісів, електронного документообігу, баз клієнтів, кадрових платформ і систем внутрішнього контролю, оскільки встановлює вимоги до захисту інформації, що обробляється в інформаційних системах, а також до програмно-технічних засобів, за допомогою яких така обробка здійснюється. У цьому аспекті захист персональних даних не може обмежуватися лише юридичним оформленням згоди чи політики конфіденційності, а має включати технічні й організаційні заходи запобігання витоку, знищенню, блокуванню, несанкціонованому доступу та порушенню цілісності даних.

Окремий блок нормативного регулювання становлять акти, пов'язані з цифровізацією корпоративного документообігу та електронною взаємодією. Закон України «Про електронні документи та електронний документообіг» [18] визначає правовий режим електронного документа, що має істотне значення для кадрових, договірних, фінансових і внутрішньо-корпоративних процесів, у межах яких персональні дані створюються, передаються, зберігаються й архівуються в електронній формі. Закон України «Про електронну ідентифікацію та електронні довірчі послуги» [19] забезпечує правові засади електронної ідентифікації, електронного підпису, електронної печатки та інших довірчих послуг, що мають значення для автентифікації учасників корпоративних правовідносин і підтвердження юридичної сили електронних дій із даними.

Для корпоративної сфери особливе значення має Закон України «Про електронну комерцію» [20], оскільки саме в електронному середовищі суб'єкти господарювання масово обробляють ідентифікаційні, контактні, платіжні, поведінкові та технічні дані споживачів і користувачів цифрових сервісів. У межах електронної комерції персональні дані використовуються для укладення й виконання електронних договорів, реєстрації користувачів, доставки товарів, здійснення платежів, комунікації з клієнтами, маркетингової аналітики та персоналізованої реклами. Тому цей закон функціонально доповнює законодавство про захист персональних даних, визначаючи правове середовище, у якому корпоративна обробка даних набуває найбільш інтенсивного характеру.

Кібербезпековий вимір захисту персональних даних у корпоративній сфері пов'язаний із Законом України «Про основні засади забезпечення кібербезпеки України» [21]. Його значення полягає в тому, що сучасні персональні дані обробляються переважно в цифрових системах, які є потенційними об'єктами кібератак, несанкціонованого доступу, шкідливого програмного втручання, фішингу, витоку або блокування інформації. Для суб'єктів господарювання це означає необхідність інтегрувати захист персональних даних у систему корпоративної кібербезпеки, управління ризиками, контролю доступу, реагування на інциденти та забезпечення безперервності бізнес-процесів.

Додаткове значення має Закон України «Про публічні електронні реєстри» [22], оскільки корпоративна діяльність пов'язана з використанням даних з реєстрів про юридичних осіб, кінцевих бенефіціарних власників, посадових осіб, підписантів, підприємців та інших фізичних осіб. Цей акт важливий для розуміння правового режиму даних у цифрових реєстрах, їх доступності, достовірності, захисту та використання у господарському обороті.

Стратегічний вимір нормативного забезпечення формують акти державної політики у сфері цифрової трансформації. Зокрема, Національна економічна стратегія на період до 2030 року [23] та Стратегія цифрового розвитку інноваційної діяльності України на період до 2030 року [24] визначають цифровізацію, розвиток інноваційної інфраструктури, електронних сервісів і технологічного підприємництва як пріоритети державної політики. Для досліджуваної проблематики ці документи мають значення тому, що розширення цифрової економіки об'єктивно збільшує масштаби корпоративної обробки персональних даних і, відповідно, потребує ефективних механізмів їх правового, організаційного та технічного захисту.

Адміністративно-правовий механізм захисту персональних даних у корпоративній сфері охоплює відповідальність за порушення встановленого порядку їх обробки та контролю. Його основу становлять ст. 188–39 і 188–40 КУпАП. Стаття 188–39 КУпАП передбачає відповідальність за порушення законодавства про захист персональних даних, зокрема недодержання порядку їх захисту, незаконний доступ до даних або порушення прав суб'єкта персональних даних. Стаття 188–40 КУпАП спрямована на забезпечення виконання законних вимог Уповноваженого Верховної Ради України з прав людини щодо усунення таких порушень. У корпоративній сфері суб'єктами відповідальності можуть бути посадові особи підприємств, фізичні особи-підприємці та інші особи, відповідальні за обробку персональних даних.

Кримінальна відповідальність передбачена у разі суспільно небезпечного посягання на приватність особи. Його нормативною основою є ст. 182 Кримінального кодексу України, яка встановлює відповідальність за незаконне збирання, зберігання, використання, знищення, поширення або зміну конфіденційної інформації про особу. У корпоративній сфері такі порушення можуть проявлятися у незаконному копіюванні клієнтських баз, розголошенні кадрових, фінансових чи біометричних даних, а також передачі персональних даних третім особам без правової підстави.

Стаття 2 Закону України «Про захист персональних даних» [15] визначає поняття персональних даних як відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Законодавство не встановлює вичерпного переліку відомостей про фізичну особу, які можуть бути віднесені до персональних даних. Це зумовлено різноманітністю цілей їх збирання та обробки, а також використанням різних технічних і організаційних способів роботи з такими даними. Зокрема, у науковій літературі персональні дані громадян визначаються як будь-яка інформація в об'єктивній формі, що дає можливість встановити її інформаційне джерело та стосується суб'єкта даних, тобто ідентифікованої або такої, що може бути ідентифікована, фізичної особи та відносно якої уповноважені суб'єкти наділені обов'язком забезпечити належний рівень її організаційно-правової охорони [6].

Як правило, дослідниками персональні дані розглядаються як особливий вид інформації, об'єкт адміністративних та/або інформаційних правовідносин, об'єкт захисту тощо [25]. Суб'єктів персональних даних варто розглядати, як конкретну фізичну особу, персональні дані якої обробляються, а саме підлягають збиранню, зміні, зберігання та захисту з метою ідентифікації такої особи, у тому числі з використанням інформаційних технологій та штучного інтелекту [7]. Визначення правового статусу суб'єкта персональних даних дає змогу перейти до характеристики самих персональних даних як об'єкта правової охорони, зокрема через виокремлення їх основних ознак.

З урахуванням наведених підходів персональні дані як об'єкт інформаційно-правової охорони характеризуються такими юридично значущими ознаками:

- персональні дані становлять відомості або сукупність відомостей про фізичну особу, тобто охоплюють будь-яку інформацію, яка стосується конкретної людини;
- визначальною ознакою персональних даних є їх ідентифікаційна властивість, оскільки такі відомості дають змогу прямо або опосередковано встановити особу;
- персональні дані мають об'єктивовану форму вираження, оскільки фіксуються у певному джерелі або на відповідному носії — паперовому, електронному, цифровому чи іншому;
- персональні дані характеризуються змістовою невичерпністю, адже закон не встановлює закритого переліку таких відомостей, а їх склад залежить від мети, сфери та способу обробки;
- відомості про особу набувають спеціального правового режиму персональних даних із моменту їх обробки, тобто вчинення будь-яких дій щодо них: збирання, реєстрації, накопичення, зберігання, зміни, оновлення, використання, поширення, передачі, знеособлення або знищення, зокрема із застосуванням інформаційних чи автоматизованих систем [6].

У науковій літературі найбільш поширеними є підходи, за якими:

- персональні дані поділяються на загальні, вразливі та спеціальні: загальні персональні дані — прізвище, ім'я та по батькові, дата народження, а також інші персональні дані, які за згодою суб'єкта цих даних розміщені в загальнодоступних базах персональних даних; вразливі персональні дані — відомості про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях та професійних спілках, звинувачення у скоєнні злочину або засудження до кримінального покарання, а також дані, що стосуються здоров'я чи статевого життя; спеціальні

персональні дані — персональні дані, що не входять до вразливих чи загальних персональних даних, межі обігу яких визначаються суб'єктом цих даних [26];

- персональні дані класифікують на загальнодоступні персональні дані, конфіденційні персональні дані та спеціальні персональні дані, статус, вимоги до обробки та захисту яких визначаються національним законодавством на основі вимог міжнародного права [3];
- персональні дані громадян поділяють використовуючи критерії їх змістового наповнення та рівня встановленої «доступності» на такі групи: загальні (або загальнодоступні), спеціальні та біометричні; різновидами біометричних персональних даних громадян виступають генетичні дані про особу та дані, що стосуються здоров'я або медичні персональні дані громадян [6].

Класифікація персональних даних має не лише теоретико-доктринальне, а й прикладне правове значення, оскільки саме від виду персональних даних залежить обсяг правових, організаційних і технічних засобів їх охорони. У цьому контексті захист персональних даних слід розглядати як систему заходів, спрямованих на охорону відомостей про ідентифіковану або таку, що може бути ідентифікована, фізичну особу. Ідентифікованою вважається особа, чия особистість визначається прямо чи опосередковано, зокрема, через ідентифікаційний номер або один чи декілька елементів фізичної, фізіологічної, психічної, економічної, культурної або соціальної totoжності [8].

У зв'язку з цифровізацією корпоративного управління обсяг персональних даних, що обробляються суб'єктами господарювання, постійно зростає. Компанії використовують електронні бази даних, CRM-, ERP- та HRM-системи, хмарні сервіси, аналітичні платформи й інші цифрові інструменти, які забезпечують накопичення, систематизацію, аналіз і подальше використання даних про працівників, клієнтів, контрагентів та інших фізичних осіб. Саме тому у корпоративній сфері персональні дані мають розглядатися як об'єкт підвищеного правового, організаційного й технічного захисту.

У корпоративній сфері законодавство не встановлює вичерпного переліку відомостей про фізичну особу, які можуть визнаватися персональними даними. Це пояснюється різноманітністю корпоративних процесів, у межах яких здійснюється їх збирання та обробка: трудові відносини, кадрове адміністрування, договірні роботи, клієнтське обслуговування, маркетинг, фінансовий облік, комплаєнс, відеоспостереження та забезпечення інформаційної безпеки.

У контексті захисту персональних даних у корпоративній сфері цифровізація HRM є водночас інструментом підвищення ефективності управління персоналом і джерелом підвищених інформаційно-правових ризиків. Сучасні HR-екосистеми охоплюють цифрові платформи для рекрутингу, адаптації працівників, навчання, оцінювання результативності, управління компенсаціями, пільгами та кадровою аналітикою. Такі системи, зокрема HRIS, LMS, talent management platforms, BAS HRM, PeopleForce, Hurma, Kadro, Workday, SAP SuccessFactors, Oracle HCM Cloud, функціонують переважно на основі хмарних сервісів, мобільних застосунків, SaaS-рішень та інструментів штучного інтелекту. Унаслідок цього персональні дані працівників і кандидатів концентруються в єдиних цифрових середовищах, де обробляються ідентифікаційні, контактні, професійні, фінансові, освітні, поведінкові, оціночні, а іноді й чутливі дані. Це створює складні потоки персональної інформації всередині корпорації та між зовнішніми постачальниками HR-сервісів, що актуалізує потребу в контролі доступу, договірному врегулюванні обробки даних, шифруванні, аудиті, обмеженні строків зберігання, мінімізації даних і реагуванні на кіберінциденти. Отже, цифрові HRM-системи в корпоративному секторі мають розглядатися не лише як управлінський інструмент, а як об'єкт підвищеного організаційного та технічного захисту персональних даних [9].

Поряд із кадровим адмініструванням, істотний масив персональних даних у корпоративній сфері формується в межах договірної роботи та електронної комерції. Якщо HRM-системи забезпечують обробку даних кандидатів і працівників, то договірні та комерційні цифрові процеси охоплюють персональні дані контрагентів, їх представників, підписантів, фізичних осіб-підприємців, споживачів і користувачів електронних сервісів. Електронну комерцію доцільно розглядати як форму підприємницької діяльності, що здійснюється із використанням електронних комунікацій, цифрових платформ, інформаційних систем і технологій обробки даних. Її зміст полягає у встановленні та реалізації господарських зв'язків між суб'єктами підприємництва, а також між бізнесом і споживачами у цифровому середовищі [27]. У межах таких процесів персональні дані використовуються для ідентифікації сторін, укладення електронних договорів, підтвердження волевиявлення, виконання замовлень, здійснення платежів, доставки товарів, комунікації з клієнтами та забезпечення належного обліку господарських операцій.

Отже, договірні роботи та електронна комерція є самостійними корпоративними процесами, у межах яких персональні дані обробляються інтенсивно й системно. Це зумовлює необхідність поєднання правового регулювання електронних правочинів із вимогами законодавства про захист персональних даних, зокрема щодо законності, цільового характеру, мінімізації, безпеки та пропорційності їх обробки [28].

Взаємозв'язок електронного договору та персональних даних відображає одну з ключових тенденцій цифровізації приватноправових відносин, за якої правове регулювання має адаптуватися до технологіч-

них способів укладення, виконання та зберігання договорів. Електронні договори сприяють оперативності господарського обороту й підвищують зручність взаємодії зі споживачами, однак водночас зумовлюють необхідність належного захисту персональних даних учасників таких правовідносин. У цьому контексті стандарти GDPR мають орієнтирне значення для України, оскільки формують підходи до законної, прозорої, безпечної та пропорційної обробки персональних даних у цифровому договірному середовищі [4].

У контексті захисту персональних даних у корпоративній сфері окремої уваги потребує використання технологій Інтернету речей, оскільки підключені пристрої здатні безперервно генерувати, накопичувати й передавати значні масиви інформації про фізичних осіб. У корпоративному середовищі це стосується смарт-офісів, систем контролю доступу, відеоспостереження, логістичних датчиків, переносних пристроїв, корпоративного транспорту, виробничого обладнання та клієнтських IoT-сервісів. За наявності ідентифікаційного чи профілюючого зв'язку з конкретною особою такі відомості набувають правового режиму персональних даних і потребують належного правового, організаційного та технічного захисту. Отже, застосування IoT-рішень у корпоративній сфері посилює ризики прихованого моніторингу, надмірного збирання даних, профілювання, несанкціонованого доступу та витоку інформації. Це зумовлює необхідність чіткого визначення мети й правових підстав обробки таких даних, мінімізації їх обсягу, обмеження строків зберігання, контролю доступу, шифрування, аудиту пристроїв і впровадження процедур реагування на інциденти інформаційної безпеки [10].

У корпоративній сфері суб'єкт господарювання виступає не лише особою, яка самостійно обробляє персональні дані працівників, клієнтів, контрагентів та уповноважених представників, а й особою, чиї дані та дані її посадових осіб потребують захисту під час участі в господарських процедурах, зокрема у публічних закупівлях. У складі тендерної пропозиції компанія часто подає документи, що містять персональні дані директора, підписанта, працівників або залучених фахівців: копії паспортів, РНОКПП, накази про призначення, довіреності, документи про освіту, кваліфікацію чи досвід [29]. Підприємство одночасно є і володільцем персональних даних, і учасником правовідносин, у межах яких персональні дані його представників можуть розкриватися третім особам або потрапляти до електронної системи закупівель. Захист персональних даних на рівні господарюючого суб'єкта має охоплювати не тільки внутрішню обробку даних, а й контроль за їх передачею назовні: перевірку необхідності документів, мінімізацію обсягу відомостей, уникнення дублювання інформації з відкритих реєстрів та оскарження надмірних вимог замовника. У сфері публічних закупівель захист персональних даних є не лише обов'язком суб'єкта господарювання, а й інструментом захисту його власних корпоративних інтересів та прав фізичних осіб, які діють від його імені.

Технічна складова інформаційно-правового механізму захисту персональних даних у корпоративній сфері спрямована на забезпечення конфіденційності, цілісності, доступності та стійкості цифрової інфраструктури, у межах якої здійснюється обробка персональних даних. Її зміст становлять програмні, апаратні, криптографічні та мережеві заходи, що мінімізують ризики несанкціонованого доступу, втрати, модифікації, блокування або витоку інформації.

У цьому контексті особливого значення набувають захищене проектування інформаційних систем, безпека API, автентифікація та розмежування прав доступу, шифрування даних під час передавання й зберігання, використання захищених протоколів зв'язку, резервне копіювання, журналювання дій користувачів, моніторинг інцидентів і регулярний аудит безпеки. Такі інструменти забезпечують не лише технічний захист даних, а й виконують регуляторну функцію, оскільки дають змогу підтвердити належний рівень корпоративної обробки персональних даних відповідно до вимог законодавства та стандартів data protection compliance. Технічний захист персональних даних у корпоративній сфері є необхідною умовою функціонування всієї системи інформаційно-правової охорони, оскільки саме він забезпечує практичну реалізацію правових і організаційних вимог у цифровому середовищі [11].

Організаційна складова інформаційно-правового механізму захисту персональних даних у корпоративній сфері охоплює внутрішні управлінські, процедурні та контрольні заходи, спрямовані на забезпечення законної й безпечної обробки персональних даних. Її зміст становлять: призначення відповідальної особи за організацію роботи із захисту персональних даних; затвердження локальних актів щодо порядку їх обробки й захисту; визначення правових підстав, мети, обсягу та строків обробки даних; розмежування доступу працівників до інформаційних систем і баз даних; повідомлення Секретаріату Уповноваженого Верховної Ради України з прав людини про обробку чутливих персональних даних, що становить особливий ризик для прав і свобод суб'єктів персональних даних; організація внутрішнього контролю, аудиту й реагування на порушення.

У табл. 1 узагальнено правовий, організаційний і технологічний напрями захисту персональних даних у корпоративній сфері, визначено відповідні корпоративні процеси та розкрито зміст обробки інформації в межах кожного з них.

Отже, систематизація правового, організаційного та технологічного напрямів захисту персональних даних у корпоративній сфері має не лише прикладне, а й прогностичне значення, оскільки така діяльність

Таблиця 1

Напрями захисту персональних даних у корпоративній сфері

На- прям	Корпоративні процеси	Зміст обробки інформації
Правовий	корпоративне управління	обробка персональних даних директорів, членів органів управління, учасників, акціонерів, кінцевих бенефіціарних власників, підписантів та уповноважених представників юридичної особи з метою підтвердження повноважень, реалізації корпоративних прав, ведення установчих, реєстраційних і внутрішньо-корпоративних документів
	договірна робота	обробка даних фізичних осіб-підприємців, представників контрагентів, підписантів, довірених осіб, контактних і платіжних відомостей для укладення, виконання, зміни, припинення та архівування договорів
	клієнтські відносини та електронна комерція	обробка ідентифікаційних, контактних, платіжних, технічних і поведінкових даних клієнтів, споживачів і користувачів цифрових сервісів для реєстрації акаунтів, укладення електронних договорів, здійснення платежів і комунікації з клієнтами
	публічні закупівлі та тендерна участь	обробка персональних даних директорів, підписантів, уповноважених осіб, працівників і залучених фахівців у складі тендерної документації для підтвердження повноважень, кваліфікації, досвіду та відповідності учасника вимогам закупівлі
	передача персональних даних третім особам і транскордонна передача	обробка та передавання персональних даних IT-підрядникам, хмарним провайдером, бухгалтерам, аудиторам, маркетинговим сервісам, логістичним операторам та іншим контрагентам із визначенням правових підстав, мети, обсягу, строків і гарантій захисту таких даних
Організаційний	трудові відносини, рекрутинг і HR-адміністрування	обробка даних кандидатів, працівників і колишніх працівників: резюме, контактних даних, документів про освіту, кваліфікацію, досвід роботи, особових справ, відомостей про оплату праці, відпустки, лікарняні, дисциплінарні процедури, оцінювання та звільнення
	комплаєнс і внутрішній контроль	обробка даних керівників, працівників, бенефіціарів, контрагентів і представників третіх осіб у межах перевірки доброчесності, конфлікту інтересів, антикорупційного контролю, санкційного скринінгу, внутрішнього аудиту та службових розслідувань
	управління доступом до персональних даних	обробка інформації про користувачів корпоративних систем, їхні ролі, рівні доступу, службові повноваження, журнали входу, запити на доступ, зміну або відкликання доступу до баз персональних даних, документів і цифрових платформ
	реалізація прав суб'єктів персональних даних	обробка звернень фізичних осіб щодо доступу до власних персональних даних, їх виправлення, оновлення, видалення, обмеження обробки, відкликання згоди, заперечення проти обробки або отримання інформації про порядок використання даних
	зберігання, архівування та знищення персональних даних	обробка інформації на всіх етапах життєвого циклу даних: створення, накопичення, систематизація, зберігання, архівування, обмеження доступу, знеособлення, видалення або знищення після досягнення мети обробки чи завершення встановлених строків зберігання
Технологічний	CRM-, ERP-, HRM-системи та корпоративні цифрові платформи	автоматизована обробка персональних даних працівників, клієнтів, контрагентів і користувачів у корпоративних інформаційних системах, включаючи збирання, структурування, аналітику, оновлення, передавання, інтеграцію та контроль доступу до даних
	хмарні сервіси та SaaS-рішення	зберігання, передавання й обробка персональних даних у хмарному середовищі, включаючи використання корпоративної пошти, електронного документообігу, баз клієнтів, HRM-платформ, бухгалтерських сервісів, резервного копіювання та віддаленого доступу
	інформаційна безпека та IT-адміністрування	обробка технічних ідентифікаторів, логінів, IP-адрес, device ID, журналів доступу, корпоративної пошти, даних про інциденти, технічну активність користувачів, спроби несанкціонованого доступу, блокування, витоку або пошкодження інформації
	корпоративна безпека, відеоспостереження і контроль доступу	обробка відеозображень, фото, даних пропускних систем, біометричних ідентифікаторів, журналів входу/виходу, інформації про переміщення працівників, відвідувачів і контрагентів у межах забезпечення фізичної та інформаційної безпеки
	IoT-рішення та мережеві пристрої	обробка даних, що генеруються підключеними пристроями, датчиками, смарт-офісами, системами моніторингу, корпоративним транспортом, виробничим обладнанням або переносними пристроями, зокрема даних про місцезнаходження, поведінку, активність, маршрути чи технічні параметри

Джерело: узагальнено авторами

повинна бути орієнтована на підготовку суб'єктів господарювання до майбутньої імплементації оновленої моделі правового регулювання, закладеної у проєкті Закону України «Про захист персональних даних» № 8153, що перебуває на розгляді Верховної Ради України та спрямований на адаптацію національного законодавства до сучасних міжнародних і європейських стандартів, зокрема GDPR і модернізованої Конвенції Ради Європи 108+ [5].

У контексті корпоративної сфери законопроект № 8153 «Про захист персональних даних» [30] має системоутворююче значення, оскільки пропонує перехід до комплексної моделі корпоративного data protection compliance. Його положення передбачають для корпоративної сфери низку новацій, спрямованих на посилення законності, прозорості, безпечності та підзвітності обробки персональних даних суб'єктами господарювання, зокрема, законопроект:

- деталізує правовий статус контролера та оператора персональних даних, що є важливим для компаній, які самостійно обробляють дані працівників, клієнтів і контрагентів або передають їх IT-підрядникам, хмарним сервісам, бухгалтерам, CRM- чи HRM-провайдерам;
- посилює вимоги до корпоративного комплаєнсу, оскільки передбачає необхідність внутрішніх політик, процедур, інструкцій, аудиту даних, визначення правових підстав обробки, строків зберігання, порядку доступу, передачі, видалення та знищення персональних даних;
- уточнює правові підстави обробки персональних даних, що має значення для трудових, договірних, маркетингових, фінансових і комплаєнс-процесів компанії, де дані можуть оброблятися не лише на підставі згоди, а й для виконання договору, закону або законного інтересу;
- орієнтує бізнес на впровадження принципів privacy by design і privacy by default, тобто захисту персональних даних уже на етапі проєктування корпоративних інформаційних систем, цифрових сервісів, CRM-, ERP-, HRM-платформ і систем відеоспостереження;
- актуалізує захист персональних даних працівників, кандидатів і колишніх працівників, оскільки вимагає законної, цільової та пропорційної обробки кадрових даних, обмеження доступу до них, визначення строків зберігання й порядку знищення після припинення трудових відносин;
- посилює регулювання автоматизованої обробки, профілювання та використання штучного інтелекту, що має значення для HR-аналітики, автоматизованого відбору кандидатів, оцінки працівників, скорингу, таргетованої реклами й персоналізованого клієнтського сервісу;
- деталізує вимоги до передачі персональних даних третім особам і за кордон, що є важливим для компаній, які використовують міжнародні хмарні сервіси, глобальні CRM-системи, зовнішніх консультантів, маркетингових операторів або IT-підрядників;
- передбачає посилення відповідальності за порушення правил обробки персональних даних, що підвищує для бізнесу фінансові, репутаційні, договірні та комплаєнс-ризики у разі витоку, незаконного доступу, неправомірної передачі або неналежного захисту даних

У корпоративному вимірі положення законопроекту № 8153 формують передумови переходу від фрагментарного захисту персональних даних до системної ризик-орієнтованої моделі їх обробки, що, у свою чергу, сприятиме гармонізації національного законодавства з європейськими стандартами, підвищенню довіри до українських компаній на ринку ЄС, спрощенню транскордонного обігу даних та посиленню правових і технологічних засобів протидії кіберзлочинності.

Висновки. Інститут персональних даних має комплексний міжгалузевий характер, оскільки поєднує конституційно-правові гарантії приватності, цивільно-правові засоби охорони немайнових прав, адміністративно-правовий порядок контролю, інформаційно-правовий режим обробки даних та господарсько-правовий вимір корпоративної діяльності.

Інформаційно-правовий механізм захисту персональних даних у корпоративній сфері доцільно визначити як інтегровану систему правових, організаційних і технологічних засобів, спрямованих на забезпечення законної, цільової, пропорційної, безпечної та підзвітної обробки персональних даних працівників, клієнтів, контрагентів, посадових осіб, учасників, акціонерів, бенефіціарів і користувачів цифрових сервісів у межах корпоративної діяльності.

Установлено, що зазначений механізм реалізується через три взаємопов'язані напрями: правовий, який охоплює нормативні підстави, принципи обробки персональних даних і юридичну відповідальність; організаційний, що передбачає внутрішні політики, локальні акти, розподіл повноважень, контроль доступу, аудит, реагування на інциденти та реалізацію прав суб'єктів персональних даних; технологічний, спрямований на забезпечення конфіденційності, цілісності, доступності й стійкості корпоративних інформаційних систем.

Практичне вдосконалення захисту персональних даних у корпоративній сфері має здійснюватися шляхом запровадження ризик-орієнтованої моделі обробки даних, інвентаризації корпоративних процесів, визначення правових підстав обробки, мінімізації обсягу даних, регламентації строків їх зберігання, договірної врегулювання передачі даних третім особам, посилення контролю доступу, шифрування, аудиту інформаційних систем і впровадження процедур реагування на кіберінциденти.

Особливе значення має законопроект № 8153 «Про захист персональних даних», який формує передумови переходу від фрагментарного захисту даних до системної моделі корпоративного data protection compliance, орієнтованої на гармонізацію національного законодавства з європейськими стандартами, посилення підзвітності суб'єктів господарювання, захист прав суб'єктів персональних даних, спрощення транскордонного обігу даних і підвищення стійкості бізнесу до кіберзагроз.

ДОДАТКОВА ІНФОРМАЦІЯ

ВНЕСОК АВТОРІВ: Усі автори зробили внесок порівну.

ФІНАНСУВАННЯ: Автори не отримували фінансування для цього дослідження.

ЗАЯВА ПРО ДОСТУПНІСТЬ ДАНИХ: Не застосовується.

КОНФЛІКТ ІНТЕРЕСІВ: Автори заявляють про відсутність конфлікту інтересів.

Література

1. Різенко О. В. Європейські правові стандарти захисту персональних даних. *Аналітично-порівняльне правознавство*. 2024. № 6. С. 643–648. DOI: <https://doi.org/10.24144/2788-6018.2024.06.105>
2. Тополевський Р. Б. Особливості правового регулювання персональних даних в Україні у контексті стандартів Європейського Союзу. *Науковий вісник Міжнародного гуманітарного університету*. 2024. Вип. 71. С. 18–21. DOI: <https://doi.org/10.32782/2307-1745.2024.71.4>
3. Мельник К. С. Правові та організаційні засади захисту персональних даних в умовах євроінтеграції України : автореф. дис. ... канд. юрид. наук. Київ, 2016. 20 с.
4. Антошкіна В. К., Кузьменко О. В. Електронний договір і персональні дані: взаємодія між GDPR та Законом України «Про захист персональних даних». *Європейський правничий часопис*. 2025. Вип. 10. С. 71–78. DOI: [https://doi.org/10.36919/3041-1149\(print\).10.2025.71-78](https://doi.org/10.36919/3041-1149(print).10.2025.71-78)
5. Колб С. О. Правове регулювання захисту персональних даних працівників: міжнародні стандарти та перспективи вдосконалення в Україні. *Актуальні проблеми вітчизняної юриспруденції*. 2024. Вип. 6. С. 56–64. DOI: <https://doi.org/10.32782/2408-9257-2024-6-9>
6. Цюменко А. Персональні дані громадян та їхня класифікація в сучасній доктрині адміністративного права. *Вісник Київського національного університету імені Тараса Шевченка. Військово-спеціальні науки*. 2023. Вип. 1. С. 41–45. DOI: <https://doi.org/10.17721/1728-2217.2023.53.41-45>
7. Цюменко А. В. Суб'єкти персональних даних громадян та їхня класифікація в сучасній доктрині адміністративного права. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2025. Вип. 87(3). С. 202–207. DOI: <https://doi.org/10.24144/2307-3322.2025.87.3.29>
8. Брижко В. М. Організаційно-правові питання захисту персональних даних: дис. ... канд. юрид. наук. Ірпінь, 2004. 185 с.
9. Жуляєв В. Захист даних у системі управління персоналом в умовах викликів та кіберзагроз для інформаційної приватності. *Економіка та суспільство*. 2025. № 82. DOI: <https://doi.org/10.32782/2524-0072/2025-82-65>
10. Савицька Л., Коробейнікова Т., Костюк О., Колесник І., Дудник О. Засоби захисту internet of things в корпоративній комп'ютерній мережі. *Інформаційні технології та комп'ютерна інженерія*. 2024. Том. 59, № 1. С. 83–93. DOI: <https://doi.org/10.31649/1999-9941-2024-59-1-83-93>
11. Борисенко О. С., Тимошенко А. Г. Огляд методів захисту персональних даних у хмарному середовищі. *Інфокомунікаційні та комп'ютерні технології*. 2024. № 1(07). С. 31–34. DOI: <https://doi.org/10.36994/2788-5518-2024-01-07-04>
12. Про ратифікацію Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додаткового протоколу до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних стосовно органів нагляду та транскордонних потоків даних : Закон України від 6 липня 2010 року N 2438-VI. URL: <https://zakon.rada.gov.ua/laws/main/2438-17?#Text> (дата звернення: 11.04.2026)
13. Федосенко Н. А., Спіцина Г. О. Актуальні питання міжнародно-правового регулювання захисту персональних даних працівників. *Аналітично-порівняльне правознавство*. 2023. № 2. С. 204–208. DOI: <https://doi.org/10.24144/2788-6018.2023.02.34>
14. Про інформацію : Закон України № 2657-XII від 2 жовтня 1992 р. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text> (дата звернення: 14.04.2026).
15. Про захист персональних даних : Закон України від № 2297-VI від 1 червня 2010 року URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text> (дата звернення: 13.04.2026).
16. Повалена М., Левчук Н. Правове забезпечення інформаційної безпеки в сфері захисту персональних даних. *Вісник Національного університету «Львівська політехніка». Серія: «Юридичні науки»*. 2025. № 4 (48). С. 350–357. DOI: <http://doi.org/10.23939/law2025.48.350>

17. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 5 липня 1994 року № 80/94-VR. URL: <https://zakon.rada.gov.ua/laws/show/80/94-vr#Text> (дата звернення: 14.04.2026).
18. Про електронні документи та електронний документообіг : Закон України від 22 травня 2003 року № 851-IV. URL: <https://zakon.rada.gov.ua/laws/show/851-15#Text> (дата звернення: 13.04.2026).
19. Про електронну ідентифікацію та електронні довірчі послуги : Закон України від 5 жовтня 2017 року № 2155-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2155-19#Text> (дата звернення: 14.04.2026).
20. Про електронну комерцію : Закон України від 3 вересня 2015 року № 675-VIII. URL: <https://zakon.rada.gov.ua/laws/show/675-19#Text> (дата звернення: 13.04.2026).
21. Про основні засади забезпечення кібербезпеки України : Закон України 5 жовтня 2017 року № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text> (дата звернення: 14.04.2026).
22. Про публічні електронні реєстри : Закон України 18 листопада 2021 року № 1907-IX. URL: <https://zakon.rada.gov.ua/laws/show/1907-20#Text> (дата звернення: 14.04.2026).
23. Про затвердження Національної економічної стратегії на період до 2030 року : Постанова Кабінету міністрів України від 3 березня 2021 р. № 179. URL: <https://zakon.rada.gov.ua/laws/show/179-2021-%D0%BF#Text> (дата звернення: 14.04.2026).
24. Про схвалення Стратегії цифрового розвитку інноваційної діяльності України на період до 2030 року та затвердження операційного плану заходів з її реалізації у 2025–2027 роках : Постанова Кабінету міністрів України від 31 грудня 2024 р. № 1351-р. URL: <https://zakon.rada.gov.ua/laws/show/1351-2024-%D1%80#Text> (дата звернення: 13.04.2026).
25. Лютіков П. С. Персональні дані: доктринальне тлумачення категорії у науках адміністративного та інформаційного права. *Аналітично-порівняльне правознавство*. 2023. № 6. С. 472–477. DOI: <https://doi.org/10.24144/2788-6018.2023.06.81>
26. Різак М. В. Класифікація персональних даних як необхідний елемент введення ефективної комунікації в суспільстві. *Наук. вісн. Міжнар. гуманітарного ун-ту*. 2013. Вип. 6–3(1). С. 90–94. URL: <https://www.vestnik-pravo.mgu.od.ua/archive/juspradenc6-3-1/23.pdf> (дата звернення: 11.04.2026).
27. Кройтор В. А. Електронний договір. *Аналітично-порівняльне правознавство*. 2024. № 6. С. 254–258. DOI: <https://doi.org/10.24144/2788-6018.2024.06.40>
28. Виноградова О. В., Євтушенко Н. О., Крючок І. С. Електронна комерція в епоху диджиталізації. *Причорноморські економічні студії*. 2020. Вип. 53. С. 55–61. DOI: <https://doi.org/10.32843/bses.53-8>
29. Овчаренко А. С., Товкун Л. В. Захист персональних даних при здійсненні публічних закупівель: виклики та правові орієнтири. *Ампаро*. 2025. № 3. С. 74–80. DOI: <https://doi.org/10.26661/2786-5649-2025-3-10>
30. Про захист персональних даних : проект Закону України № 8153 від 25.10.2022 року. URL: <https://itd.rada.gov.ua/billinfo/Bills/Card/40707> (дата звернення: 13.04.2026).

References:

1. Rizenko, O. V. (2024). Yevropeiski pravovi standarty zakhystu personalnykh danykh [European legal standards for personal data protection]. *Analitychno-porivnialne pravoznavstvo — Analytical and Comparative Jurisprudence*, 6, 643–648. <https://doi.org/10.24144/2788-6018.2024.06.105> [in Ukrainian].
2. Topolevskyi, R. B. (2024). Osoblyvosti pravovoho rehuliuвання personalnykh danykh v Ukraini u konteksti standartiv Yevropeiskoho Soiuzu [Features of personal data regulation in Ukraine in the context of European Union standards]. *Naukovyi visnyk Mizhnarodnoho humanitarnoho universytetu. Seriya: Yurysprudentsiia — Scientific Bulletin of the International Humanitarian University. Series: Jurisprudence*, 71, 18–21. <https://doi.org/10.32782/2307-1745.2024.71.4> [in Ukrainian].
3. Melnyk, K. S. (2016). Pravovi ta orhanizatsiini zasady zakhystu personalnykh danykh v umovakh yevrointegratsii Ukrainy [Legal and organizational principles of personal data protection in the context of Ukraine's European integration]. *Extended abstract of candidate's thesis*. Kyiv [in Ukrainian].
4. Antoshkina, V. K., & Kuzmenko, O. V. (2025). Elektronnyi dohovir i personalni dani: vzaiemodiiia mizh GDPR ta Zakonom Ukrainy "Pro zakhyst personalnykh danykh" [Electronic contract and personal data: interaction between the GDPR and the Law of Ukraine "On Personal Data Protection"]. *Yevropeyskyi pravnychi chasopys — European Legal Journal*, 10, 71–78. [https://doi.org/10.36919/3041-1149\(Print\).10.2025.71-78](https://doi.org/10.36919/3041-1149(Print).10.2025.71-78) [in Ukrainian].
5. Kolb, S. O. (2024). Pravove rehuliuвання zakhystu personalnykh danykh pratsivnykiv: mizhnarodni standarty ta perspektivy vdoskonalennia v Ukraini [Legal regulation of employees' personal data protection: international standards and prospects for improvement in Ukraine]. *Aktualni problemy vitchyznianoï yurysprudentsii — Current Issues of Domestic Jurisprudence*, 6, 56–64. <https://doi.org/10.32782/2408-9257-2024-6-9> [in Ukrainian].
6. Tsiomenko, A. (2023). Personalni dani hromadian ta yikhnia klasyfikatsiia v suchasniï doktryni administratyvnoho prava [Citizens' personal data and their classification in the modern doctrine of administrative law]. *Visnyk Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. Viiskovo-spetsialni nauky — Bulletin of Taras Shevchenko National University of Kyiv. Military-Special Sciences*, 1, 41–45. <https://doi.org/10.17721/1728-2217.2023.53.41-45> [in Ukrainian].

7. Tsiomenko, A. V. (2025). Subiekty personalnykh danykh hromadian ta yikhnia klasyfikatsiia v suchasni doktryni administratyvnoho prava [Subjects of citizens' personal data and their classification in the modern doctrine of administrative law]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Serii: Pravo — Scientific Bulletin of Uzhhorod National University. Series: Law*, 87(3), 202–207. <https://doi.org/10.24144/2307-3322.2025.87.3.29> [in Ukrainian].

8. Bryzhko, V. M. (2004). Orhanizatsiino-pravovi pytannia zakhystu personalnykh danykh [Organizational and legal issues of personal data protection]. *Candidate's thesis*. Irpin [in Ukrainian].

9. Zhuliaiev, V. (2025). Zakhyst danykh u systemi upravlinnia personalom v umovakh vyklykiv ta kiberzahroz dlia informatsiinoi pryvatnosti [Data protection in the personnel management system under the conditions of challenges and cyber threats to information privacy]. *Ekonomika ta suspilstvo — Economy and Society*, 82. <https://doi.org/10.32782/2524-0072/2025-82-65> [in Ukrainian].

10. Savytska, L., Korobeinikova, T., Kostyuk, O., Kolesnyk, I., & Dudnyk, O. (2024). Zasoby zakhystu Internet of Things v korporativnii kompiuternii merezhi [Means of protecting the Internet of Things in a corporate computer network]. *Informatsiini tekhnolohii ta kompiuterna inzheneriia — Information Technologies and Computer Engineering*, 59(1), 83–93. <https://doi.org/10.31649/1999-9941-2024-59-1-83-93> [in Ukrainian].

11. Borysenko, O. S., & Tymoshenko, A. H. (2024). Ohliad metodiv zakhystu personalnykh danykh u khmarnomu seredovyschi [Overview of methods for protecting personal data in a cloud environment]. *Infokomunikatsiini ta kompiuterni tekhnolohii — Infocommunication and Computer Technologies*, 1(07), 31–34. <https://doi.org/10.36994/2788-5518-2024-01-07-04> [in Ukrainian].

12. Pro ratyfikatsiiu Konventsii pro zakhyst osib u zviazku z avtomatyzovanoi obrobkoiu personalnykh danykh ta Dodatkovoho protokolu do Konventsii pro zakhyst osib u zviazku z avtomatyzovanoi obrobkoiu personalnykh danykh stosovno orhaniv nahliadu ta transkordonnykh potokiv danykh [On ratification of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows]. (2010, July 6). *Vidomosti Verkhovnoi Rady Ukrainy — Bulletin of Verkhovna Rada of Ukraine*. Kyiv: Parlam. vyd-vo. Retrieved from <https://zakon.rada.gov.ua/laws/main/2438-17#Text> [in Ukrainian].

13. Fedosenko, N. A., & Spitsyna, H. O. (2023). Aktualni pytannia mizhnarodno-pravovoho rehuliuвання zakhystu personalnykh danykh pratsivnykiv [Current issues of international legal regulation of employees' personal data protection]. *Analichno-porivnialne pravoznavstvo — Analytical and Comparative Jurisprudence*, 2, 204–208. <https://doi.org/10.24144/2788-6018.2023.02.34> [in Ukrainian].

14. Pro informatsiiu [On Information]. (1992, October 2). *Vidomosti Verkhovnoi Rady Ukrainy — Bulletin of Verkhovna Rada of Ukraine*. Kyiv: Parlam. vyd-vo. Retrieved from <https://zakon.rada.gov.ua/laws/show/2657-12#Text>

15. Pro zakhyst personalnykh danykh [On Personal Data Protection]. (2010, June 1). *Vidomosti Verkhovnoi Rady Ukrainy — Bulletin of Verkhovna Rada of Ukraine*. Kyiv: Parlam. vyd-vo. Retrieved from <https://zakon.rada.gov.ua/laws/show/2297-17#Text> [in Ukrainian].

16. Povalena, M., & Levchuk, N. (2025). Pravove zabezpechennia informatsiinoi bezpeky v sferi zakhystu personalnykh danykh [Legal support of information security in the field of personal data protection]. *Visnyk Natsionalnoho universytetu «Lvivska politehnika». Serii: «Yurydychni nauky» — Bulletin of Lviv Polytechnic National University. Series: Legal Sciences*, 4(48), 350–357. <http://doi.org/10.23939/law2025.48.350> [in Ukrainian].

17. Pro zakhyst informatsii v informatsiino-telekomunikatsiinykh systemakh [On Information Protection in Information and Telecommunication Systems]. (1994, July 5). *Vidomosti Verkhovnoi Rady Ukrainy — Bulletin of Verkhovna Rada of Ukraine*. Kyiv: Parlam. vyd-vo. Retrieved from <https://zakon.rada.gov.ua/laws/show/80/94-vr#Text> [in Ukrainian].

18. Pro elektronni dokumenty ta elektronnyi dokumentobih [On Electronic Documents and Electronic Document Management]. (2003, May 22). *Vidomosti Verkhovnoi Rady Ukrainy — Bulletin of Verkhovna Rada of Ukraine*. Kyiv: Parlam. vyd-vo. Retrieved from <https://zakon.rada.gov.ua/laws/show/851-15#Text> [in Ukrainian].

19. Pro elektronnu identyfikatsiiu ta elektronni dovirchi posluhy [On Electronic Identification and Electronic Trust Services]. (2017, October 5). *Vidomosti Verkhovnoi Rady Ukrainy — Bulletin of Verkhovna Rada of Ukraine*. Kyiv: Parlam. vyd-vo. Retrieved from <https://zakon.rada.gov.ua/laws/show/2155-19#Text> [in Ukrainian].

20. Pro elektronnu komertsiiu [On Electronic Commerce]. (2015, September 3). *Vidomosti Verkhovnoi Rady Ukrainy — Bulletin of Verkhovna Rada of Ukraine*. Kyiv: Parlam. vyd-vo. Retrieved from <https://zakon.rada.gov.ua/laws/show/675-19#Text> [in Ukrainian].

21. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy [On the Basic Principles of Cybersecurity of Ukraine]. (2017, October 5). *Vidomosti Verkhovnoi Rady Ukrainy — Bulletin of Verkhovna Rada of Ukraine*. Kyiv: Parlam. vyd-vo. Retrieved from <https://zakon.rada.gov.ua/laws/show/2163-19#Text> [in Ukrainian].

22. Pro publichni elektronni reiestry [On Public Electronic Registers]. (2021, November 18). *Vidomosti Verkhovnoi Rady Ukrainy — Bulletin of Verkhovna Rada of Ukraine*. Kyiv: Parlam. vyd-vo. Retrieved from <https://zakon.rada.gov.ua/laws/show/1907-20#Text> [in Ukrainian].

23. Pro zatverdzhennia Natsionalnoi ekonomichnoi stratehii na period do 2030 roku [On Approval of the National Economic Strategy for the Period up to 2030]. (2021, March 3). *Uriadovyi kurier — Government Courier*. Kyiv: Kabinet Ministriv Ukrainy. Retrieved from <https://zakon.rada.gov.ua/laws/show/179-2021-%D0%BF#Text> [in Ukrainian].

24. Pro skhvalennia Stratehii tsyfrovoho rozvytku innovatsiinoi diialnosti Ukrainy na period do 2030 roku ta zatverdzhennia operatsiinoho planu zakhodiv z yii realizatsii u 2025–2027 rokakh [On Approval of the Strategy for Digital Development of Innovation Activity of Ukraine for the Period up to 2030 and Approval of the Operational Action Plan for Its Implementation in 2025–2027]. (2024, December 31). *Uriadovyi kurier — Government Courier*. Kyiv: Kabinet Ministriv Ukrainy. Retrieved from <https://zakon.rada.gov.ua/laws/show/1351-2024-%D1%80#Text> [in Ukrainian].
25. Liutikov, P. S. (2023). Personalni dani: doktrynalne tлумachennia katehorii u naukakh administratyvnoho ta informatsiinoho prava [Personal data: doctrinal interpretation of the category in the sciences of administrative and information law]. *Analychno-porivnialne pravoznavstvo — Analytical and Comparative Jurisprudence*, 6, 472–477. <https://doi.org/10.24144/2788-6018.2023.06.81> [in Ukrainian].
26. Rizak, M. V. (2013). Kласyfikatsiia personalnykh danykh yak neobkhidnyi element vvedennia efektyvnoi komunikatsii v suspilstvi [Classification of personal data as a necessary element of introducing effective communication in society]. *Naukovyi visnyk Mizhnarodnoho humanitarnoho universytetu. Serii: Yurysprudentsiia — Scientific Bulletin of the International Humanitarian University. Series: Jurisprudence*, 6–3(1), 90–94. Retrieved from <https://www.vestnik-pravo.mgu.od.ua/archive/juspradenc6-3-1/23.pdf> [in Ukrainian].
27. Kroitor, V. A. (2024). Elektronnyi dohovir [Electronic contract]. *Analychno-porivnialne pravoznavstvo — Analytical and Comparative Jurisprudence*, 6, 254–258. <https://doi.org/10.24144/2788-6018.2024.06.40> [in Ukrainian].
28. Vynohradova, O. V., Yevtushenko, N. O., & Kriuchok, I. S. (2020). Elektronna komertsiiia v epokhu dydzhytalizatsii [E-commerce in the era of digitalization]. *Prychornomorski ekonomichni studii — Black Sea Economic Studies*, 53, 55–61. <https://doi.org/10.32843/bses.53-8> [in Ukrainian].
29. Ovcharenko, A. S., & Tovkun, L. V. (2025). Zakhyst personalnykh danykh pry zdiisnenni publichnykh zakupivel: vyklyky ta pravovi oriientyry [Personal data protection in public procurement: challenges and legal guidelines]. *Amparo*, 3, 74–80. <https://doi.org/10.26661/2786-5649-2025-3-10> [in Ukrainian].
30. Verkhovna Rada of Ukraine. (2022). Pro zakhyst personalnykh danykh [On Personal Data Protection]: Draft Law of Ukraine No. 8153. Retrieved from <https://itd.rada.gov.ua/billinfo/Bills/Card/40707> [in Ukrainian].

Дата першого надходження статті до видання: 25.04.2026

Дата прийняття статті до друку після рецензування: 21.05.2026

Дата публікації: 29.05.2026

Dulina Oksana

*PhD in Law, Associate Professor,
Associate Professor of the Department of
Public Administration and Regionalism
Educational and Scientific Institute of Public
Service and Administration
Odesa Polytechnic National University*

Kuspliak Ihor

*Candidate of Political Sciences,
Associate Professor,
Associate Professor of the Department of
Public Administration and Regionalism
Deputy Director of the
Educational and Scientific Institute of Public
Service and Administration
Odesa Polytechnic National University*

Sivak Volodymyr

*PhD in Law, Associate Professor of the
Department of Public Administration and
Regional Studies
Educational and Scientific Institute of Public
Service and Administration
Odesa Polytechnic National University*

INFORMATION AND LEGAL MECHANISM FOR PERSONAL DATA PROTECTION IN THE CORPORATE SECTOR

Summary. Introduction. Digitalization of business activities significantly transforms corporate processes related to the collection, storage, use, transfer and protection of personal data. The use of CRM, ERP, HRM systems, cloud services, electronic document management, e-commerce platforms, IoT solutions and artificial intelligence technologies expands the scope of corporate processing of information about employees, customers, contractors and users of digital services. At the same time, this increases the risks of illegal access, leakage, profiling, excessive collection and misuse of personal data. In this regard, the need for a comprehensive study of the information and legal mechanism for protecting personal data in the corporate sphere is becoming more urgent.

Purpose. The purpose of the study is a comprehensive analysis of the information and legal mechanism for protecting personal data in the corporate sphere, determining its legal, organizational and technological components, as well as substantiating the directions for improving the corporate model of personal data processing, taking into account international and European standards.

Materials and methods. The materials of the study are: 1) international and European acts in the field of personal data protection, in particular the Council of Europe Convention No. 108 and GDPR; 2) regulatory legal acts of Ukraine regulating information relations, personal data protection, electronic document flow, e-commerce, cybersecurity and liability for violations in the field of data processing; 3) draft law No. 8153 on the modernization of national legislation on personal data protection; 4) scientific works of domestic authors devoted to the issues of personal data, information security, corporate compliance, HRM systems, cloud services and IoT solutions. The research used the formal legal method, comparative legal method, system-structural analysis, classification, generalization and logical-legal modeling methods.

Results. The article reveals the content of the information and legal mechanism for the protection of personal data in the corporate sphere. The provisions of the Council of Europe Convention No. 108, GDPR and the prospects for the modernization of national legislation in connection with draft law No. 8153 are analyzed. The domestic regulatory framework for the protection of personal data is characterized, including information, digital, administrative, criminal and cybersecurity legislation. Scientific approaches to the classification of personal data are summarized, their legally significant features and significance in the corporate sphere are determined. The author's definition of the information and legal mechanism for the protection of personal data in the corporate sphere is proposed as a comprehensive system of regulatory regulation, internal corporate management, technical security, access control, leak prevention, incident response and legal liability aimed at the protection of personal data within the framework of corporate activities. The legal, organizational, and technological directions of personal data protection are identified and

their significance for corporate governance, personnel administration, contractual work, e-commerce, public procurement, cloud services, and information security is revealed.

Discussion. Further scientific research should be directed towards developing a practical model of corporate data protection compliance, improving internal personal data processing policies, developing risk assessment procedures, responding to information security incidents, and ensuring compliance of corporate personal data processing with European standards.

Key words: *personal data protection, information and legal mechanism, digitalization, information security, cybersecurity, e-commerce, corporate security, information protection, information technology, business entity, corporate sphere.*