УДК 342.721
DOI https://doi.org/10.32782/1813-338X-2023.4.56

О. С. Дяковський
кандидат юридичних наук, старший викладач кафедри інформаційного,
господарського та адміністративного права
Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського»
докторант кафедри публічного права
Державний податковий університет
ORCID ID: 0000-0003-3412-9278

С. С. Чернецький
доктор філософії з публічного управління та адміністрування
ORCID ID: 0000-0002-7368-4509

ІНСТИТУЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ: ДОСВІД УКРАЇНИ І ЄС

У статті розглядається інституційне забезпечення захисту персональних даних в контексті України та ЄС, а також порівнюється досвід цих двох регіонів. Україна, рухаючись до вступу до ЄС, активно працює над адаптацією свого законодавства щодо захисту персональних даних до стандартів ЄС. В сучасному цифровому світі, де персональні дані стають найціннішим активом, їх захист стає важливим аспектом для забезпечення приватності та безпеки громадян. Зокрема, в 2010 році був прийнятий Закон України «Про захист персональних даних», що визначає правові основи захисту цих даних та встановлює відповідальність за їх порушення. Проте, існують певні виклики в реалізації цього закону, такі як недостатня ефективність контролю за дотриманням правил захисту даних.

З'ясовано, що у порівнянні з Україною, ЄС має більш розвинуту систему інституційного захисту персональних даних. Однією з ключових інституцій у цьому контексті є Європейський орган з захисту даних, який має на меті забезпечення дотримання правил щодо захисту даних в усіх країнах-членах ЄС. Додатково, ЄС прийняв загальний регламент щодо захисту даних, який надає громадянам більші права контролю над їх персональними даними та встановлює високі стандарти захисту цих даних. Встановлено, що хоча Україна активно працює над покращенням свого законодавства в частині захисту персональних даних, їй ще потрібно зробити значні зусилля, щоб досягти такого ж рівня інституційного забезпечення, як у ЄС. Йдеться про вдосконалення контрольних механізмів, підвищення рівня поінформованості громадян про їх права та зобов'язання щодо захисту даних, а також зміцнення співпраці з міжнародними партнерами у цій сфері. Хоча обидва регіони знаходяться на різних етапах розвитку у цій сфері, подальше співробітництво та обмін досвідом можуть сприяти покращенню стандартів захисту персональних даних на всій території.

Ключові слова: *інформаційні технології, персональні дані, стандарти, механізми правового захисту, обіг даних, інформація, суб'єкти захисту, правове регулювання, відповідальність, згода на обробку, цифрове середовище.*

Постановка проблеми. Розвиток інформаційних технологій та поширення відповідної продукції фактично у всі сфери людської діяльності несуть в собі не тільки очевидні переваги, але й низку загроз та проблем. Одна з таких пов'язана із захистом персональних даних. Згідно статистичних даних, у 2023 році в ЄС було накладено близько 2,1 млрд. € штрафів через порушення законодавства про захист персональних даних. Сумарна кількість перевищує сукупну вартість аналогічного штрафу за 2019, 2020 та 2021 роки в цілому. Основною причиною цього став новий рекордний штраф у розмірі 1,2 млрд. € для материнської компанії Facebook – Meta, пов'язаний з незаконною передачею даних до США в рамках стандартних договірних положень платформи [1].

Аналіз останніх досліджень і публікацій. Проблематика захисту персональних даних та стрімкого росту кількості порушень в даному напрямку притаманна і для України. Зазначене обумовлено низьким рівнем інституційного забезпечення, що формується на засадах реактивності, а не проактивності, що власне суперечить динамічній природі технологій та їх впливу на захист персональних даних. Про недосконалість нормативно-правового регулювання ведуть мову у своїх дослідженнях такі вчені як Бєлова Ю. Д., який піддає ґрунтовному аналізу базову директиву щодо захисту персональних даних в ЄС [2], Кебус А. В., що в рамках теоретичних наукових розвідок проводить порівняльно-правовий аналіз особливостей інституційного забезпечення захисту персональних даних [3]. Із зарубіжних розвідок цікавими були статистичні дослідження, оприлюднені в рамках статті Амстронга М. [1].

Мета статті – розкриття специфіки інституційного забезпечення в частині захисту персональних даних із урахуванням досвіду передових країн світу.

Виклад основного матеріалу. Інституційне забезпечення захисту персональних даних являє собою систему правових, організаційних, технічних та інших заходів, спрямованих на забезпечення конфіденційності, цілісності та доступності персональних даних, які зберігаються, обробляються та передаються різними суб'єктами, у тому числі організаціями, компаніями, органами публічного управління. Мова йде про створення ефективних правових рамок, розробку політик та процедур, впровадження технічних засобів захисту, формування цифрової свідомості та навчання персоналу, а також надання прав й контролю громадянам над їхніми персональними даними. Інституційне забезпечення захисту персональних даних може включати створення спеціалізованих органів, що надають консультації та здійснюють нагляд за виконанням правил захисту даних, провадять регулярну оцінку ризиків й аудит систем безпеки даних.

Інституційне забезпечення захисту персональних даних є важливою складовою сучасного цифрового середовища, оскільки воно сприяє підвищенню довіри користувачів до обробки їхніх персональних даних, а також забезпечує відповідність нормам чинного законодавства. Так, основним правовим інструментом ЄС у сфері захисту персональних даних була Директива 95/46/ЄС Європейського парламенту та Ради Європи від 24.10.1995 р. «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» (Директива про захист персональних даних) [3]. Ключова ціль документу – захист основоположних прав і свобод, що зводяться до уникнення та мінімізації ризиків неправомірного втручання у персональні дані третіми особами в процесі їх обробки. В розрізі аналізу розвитку законодавства ЄС про захист персональних даних вказана Директива має суттєве значення, адже фактично вона сформувала підґрунтя для подальшого нормативно-правового і організаційного розвитку інституту в рамках ЄС (було закріплено цілі, окреслено термінологію, принципи обробки даних, сформовано ключові засади у співвідношенні із застосуванням національного законодавства, розкрито зміст особливих категорій обробки і т.і.). Проте, 27.04.2016 прийнято Регламент (Євросоюз) 2016/679 Європейського Парламенту та Ради про захист фізичних осіб стосовно обробки персональних даних та про вільне переміщення таких даних [4], яким власне скасовано дію вищевказаного документу. Порівняно з Директивою до регламенту внесено багато нових вимог, які здебільшого ускладнюють процес роботи організацій, які працюють з персональними даними. Однією з таких змін є, наприклад, обов'язок повідомляти уповноважені органи про витік персональних даних протягом 72 годин.

Його прийняття – логічний і не менш важливий крок в удосконаленні інституційного забезпечення захисту персональних даних, адже норми багато в чому резонують із попередньою Директивою [2, с. 137]. Зокрема, саме в Регламенті суттєво розширено вже існуючі права фізичної особи як суб'єкта захисту персональних даних, а також інтегровано нові (право бути забутим, право на мобільність, посилення права доступу до персональних даних, бути поінформованим про випадки незаконного доступу).

З юридичної точки зору цікаво звернути увагу на один організаційний аспект. Так, ст. 203 Договору про Європейський Союз та Договору про функціонування Європейського Союзу встановлено, що умови норм, прийнятих у ЄС, мають бути затверджені державами-учасницями [5], у зв'язку з чим вимоги Регламенту мають були імплементовані в національне законодавство держав-членів до травня 2018 року. Деякими країнами не було дотримано вказаної вимоги, через що Європейська Комісія закликала Суд ЄС накласти на них фінансові санкції (Греція

виплатила 5 287,50 € / день з дати порушення терміну, з мінімальною одноразовою виплатою в розмірі 1 310 000 € з дня винесення першого судового рішення до повного виконання зобов'язань). Після такого кейсу, в Греції оперативно ухвалили новий закон про персональні дані. Аналогічна ситуація сталася і в Іспанії.

Достатньо складним і суворим з позиції наслідків за недотримання вимог у сфері захисту персональних даних видається законодавства Ісландії. Станом на 2023 рік в державі успішно функціонує спеціальний наглядовий орган – Persónuvernd. Профільним законом Ісландії [6] встановлено зобов'язання проконсультуватися та отримати попередній дозвіл на обробку персональних даних, якщо цілі зачіпають суспільні інтереси. Не менш важливим стало створення Національного реєстру Ісландії із переліком суб'єктів, котрі заперечують проти спаму та використання їхніх даних для маркетингових цілей. Контролери, які займаються маркетингом і продажами перед використанням контактних даних повинні перевірити наявність особи в цьому списку. З-поміж прогресивних аспектів вбачаємо:

− введення в дію норми, котра визначає строки чинності законодавства про обробку персональних відносно даних померлих фізичних осіб – щонайменше 5 років з моменту їхньої смерті;

− персональні дані, зібрані за допомогою відстежувальних технологій, у т.ч. Cookie, не можуть зберігатися понад 90 днів;

− рекламні листи мають чітко містити: найменування особи, яка звертається до суб'єкта, контакт для заперечення проти отримання листів і телефонних дзвінків, відомості щодо джерела надходження контакту, якщо суб'єкт не являється клієнтом;

− знижено поріг надання згоди на обробку персональних даних до 13 років.

Так, якщо в Ісландії на державному рівні передбачено жорсткі штрафи та систему контролю за захистом персональних даних, то до прикладу Іспанія обрала за основу модель часткового саморегулювання. Національне законодавство країни встановлює, що у випадку надходження до наглядового органу скарги відносно порушень у сфері захисту персональних даних, розпоряднику надається два місяці для самостійного вирішення питання. Разом з тим, сильної критики зазнало положення закону про те, що політичні партії мають право використовувати персональні дані, отримані з веб-сторінок та інших публічних джерел, для здійснення політичної діяльності в період виборів. Після оскарження в Конституційному суді Іспанії цього положення було внесено правки і наразі дозволяється обробка лише у тому випадку, якщо вони були вільно оприлюднені людьми під час здійснення свого права на вираження поглядів та ідеологічну свободу. Присутній також цілий розділ про гарантії цифрових прав. У кількох статтях ідеться про захист приватного життя на робочому місці (закріплено право на недоторканність приватного життя та право використання цифрових пристроїв на робочому місці, право на недоторканність приватного життя від використання пристроїв відеоспостереження/звукозапису на робочому місці та використання систем геолокації при виконанні трудових зобов'язань). Згода на використання файлів Cookie може вважатися отриманою на законних підставах, якщо на сайті хоча б мінімум інформації про використання надається за допомогою банера. Регламентовано, що згодою також слід вважати конклюдентну дію, до прикладу, у формі використання смуги прокрутки або переходу за посиланнями на відвіданому сайті.

Законодавство про захист персональних даних у Франції має тривалу історію, адже профільний Закон про обробку даних, файлів та свобод прийнято ще в 1978 році [7]. Окремі аналогії можна проводити у відношенні із Законом Ісландії. Французьке право також передбачає положення стосовно обробки персональних даних померлих, здійснення якої може провадитися виключно в тому випадку, якщо за життя особа не заперечила проти цього. Подібно до Національного реєстру Ісландії, у Франції існує Bloctel. Будь-яка особа в праві пройти реєстрацію, тим самим виразивши свою відмову від надходження рекламних дзвінків та повідомлень. Чинність такої відмови – 3 роки із можливістю продовження. Порівняно із практикою Іспанії, в ході використання на сайті файлів Cookie згода суб'єкта має бути однозначною: прокручування вниз, гортання або перегляду сайту чи додатка недостатньо, щоб це вважалося згодою. Французька правова комуніта наполягає на тому, що підтвердження особи має в першу чергу відображати її волю: суб'єкт інформується у зрозумілій, повній та видимій формі, лише одних посилань на загальні умови використання сайту недостатньо. При цьому, тут дозволено купувати маркетингові списки з даними у третіх осіб, якщо має місце відповідний дозвіл на перечу персональних даних

від суб'єктів, що містяться у списках та забезпечено належний захист даних.

В свою чергу, основу національної моделі правового захисту персональних даних складає Конституція України [8], а саме в розрізі комплексу положень розділу 2. Власне регулювання правових відносин в частині обробки і захисту персональних даних як таких покладено на Закон України «Про захист персональних даних» [9]. До законодавства у сфері захисту персональних даних слід також віднести Кримінальний кодекс України (наприклад, статті 163, 182 та ін.), у яких передбачено кримінальну відповідальність за правопорушення [10]. Адміністративна відповідальність за порушення у сфері обробки та захисту персональних даних встановлена ст. 188-39 Кодексу України про адміністративні правопорушення [11]. Захист персональних даних передбачається ст. 270, 286 Цивільного кодексу України [12], ст. 6 Закону України «Про оперативно-розшукову діяльність» [13], Основами законодавства про охорону здоров'я від 19.11.1992 (ст. 40) [14]; Законами України «Про нотаріат» (ст. 8) [15], «Про адвокатуру та адвокатську діяльність» [16] тощо. Майже всі галузеві нормативно-правові акти також містять положення, що регламентують обробку персональних даних у відповідній сфері [17, с. 204].

Для реалізації політики у сфері захисту персональних даних ще у 2011 році було створено перший профільний центральний орган виконавчої влади – Державну службу України з питань захисту персональних даних. За три роки свого функціонування служба була ліквідована, а її повноваження передано до Департаменту з питань захисту персональних даних Секретаріату Уповноваженого Верховної Ради України з прав людини. Одна із ключових функцій (контролю) реалізується шляхом проведення перевірок фізичних осіб, фізичних осіб-підприємців, підприємств, установ і організацій усіх форм власності, органів державної влади та місцевого самоврядування, що є володільцями та/або розпорядниками персональних даних. Специфіка проведення планових і позапланових, виїзних і невиїзних перевірок регламентована спеціальним Порядком [18]. Слід наголосити, що відповідно до ч. 2 ст. 4 Закону України «Про Уповноваженого Верховної Ради України з прав людини», Уповноважений здійснює свою діяльність незалежно від інших державних органів та посадових осіб [19]. На практиці, досить часто можна зустріти випадки, коли помилково діяльність із проведення перевірок щодо додержання вимог законодавства про захист персональних даних розглядають в розрізі Закону України «Про основні засади державного нагляду (контролю) у сфері господарської діяльності» [20]. Разом з тим, доцільно зауважити, що вимоги вказаного закону поширюються виключно на діяльність центральних органів виконавчої влади та підпорядкованих їм територіальних управлінь, органів місцевого самоврядування, державних колегіальних органів і т.і. Вказане також підтверджується, зважаючи на гарантії незалежності та безсторонності омбудсмена. Відповідно, двома ключовими документами, дія яких поширюється на перевірки зі сторони Уповноваженого Верховної Ради України з прав людини є Закон [9] та Порядок [18].

При цьому, що не менш важливо, в ході реалізації своїх повноважень органи публічної влади в праві витребовувати виключно ту інформацію, котра необхідна їм для виконання управлінських функцій. В розрізі зазначеного, показовою є постанова Харківського окружного адміністративного суду № 820/10192/15, де зазначено, що в процесі перевірки державною податковою інспекцією було витребувано не лише первинні документи про об'єкт перевірки (книжковий клуб), але й дані щодо його клієнтів, для яких роблять знижку (зокрема, ПІБ, номер картки, перелік придбаної продукції, розмір знижки та її обґрунтування і т.і.). Суд визнав такий перелік відомостей затребуваним необґрунтовано, початково посилаючись на легальне трактування концепту «захист персональних даних» через призму чинного законодавства, а за тим на ст. 10 Закону України «Про захист персональних даних» [21]. В рамках судового засідання було наголошено, що розголошення подібного роду даних є допустимим виключно у випадку згоди самих суб'єктів персональних даних, а також за умови, коли це необхідно для забезпечення прав людини, економічного добробуту, а також інтересів національної безпеки. Відповідно, зважаючи на зазначене, відмову суб'єкта господарювання у наданні податковій службі вказаних відомостей слід сприймати як правомірну та обґрунтовану. Ідентичної думки були також судді вищих інстанцій.

В системі інституційного забезпечення захисту прав людини наступною ланкою слід вважати судовий захист (зазвичай, цивільне провадження). Проте кількість судових справ

у порівнянні із іншими категоріями є відносно невеликою, що, на нашу думку, є наслідком низької правової обізнаності громадян. Одним із важливих інструментів, що дає змогу всім відповідним зацікавленим сторонам у складі організації оцінити вимоги до захисту даних, є оцінка впливу на захист даних. Офіційна процедура та інструмент документування широко використовується для пов'язаної з високими ризиками діяльності з обробки даних; типові форми для нього надають різні органи, що займаються захистом даних, та інші зацікавлені сторони. Офіційну процедуру захисту даних рекомендується проводити до запуску нової ІТ-системи або процесу обробки. Керувати організацією цього процесу мають фахівці із захисту даних, однак відповідальність за дотримання законів про захист даних лежить на розпорядникові даних як суб'єкті, що виконує обов'язки з обробки даних.

Вітчизняна інституційна модель має перейняти кращі зарубіжні практики захисту персональних даних, зокрема шляхом:

− створення спеціального реєстру при Департаменті з питань захисту персональних даних Секретаріату Уповноваженого Верховної Ради України з прав людини із переліком суб'єктів, котрі заперечують проти спаму та використання їхніх даних для маркетингових цілей;

− популяризації соціальної реклами в контексті механізмів захисту персональних даних, акцентуючи увагу на праві на забуття в Інтернеті;

− удосконалення вітчизняного законодавства шляхом визначення специфіки роботи із персональними даними померлих осіб, регламентації меж та способів використання персональних даних в рамках трудових відносин; не лише перелічувати права особи, а й містити більш детальні положення щодо процедури їх реалізації.

Захист даних сам по собі передбачає наявність достатніх ресурсів, постійне навчання і підтримку з боку вищого керівництва. Розпорядник даних повинен також забезпечувати наявність відповідних можливостей для аудиту захисту даних і сприяти аудиторам, які проводять перевірку від імені органів публічного управління в частині захисту даних. Під аудитом захисту даних мається на увазі систематична та незалежна перевірка відповідності діяльності, пов'язаної з обробкою персональних даних, внутрішній політиці та процедурам у сфері захисту даних, а також вимогам застосовної нормативної бази. За підсумками програми аудиту має прийматися план безперервного підвищення якості; крім того, доцільно рекомендувати проходження галузевих програм сертифікації, таких як ISO 27001 або ISO 27701.

Висновки і пропозиції. Таким чином, підсумовуючи зазначене слід вказати, що у більшості країн ЄС було створено органи, які спеціалізуються на захисті даних, а в деяких країнах нагляд за державними та приватними установами в цій сфері здійснюють два різні органи. Використовуючи встановлені законом повноваження, орган із захисту даних розглядає скарги суб'єктів даних у зв'язку з потенційними порушеннями закону про захист даних, робить запити і проводить розслідування порушень законодавства про захист даних і в разі необхідності вживає заходів щодо забезпечення його дотримання, а також сприяє підвищенню обізнаності суб'єктів даних про їхні права на захист персональної інформації відповідно до застосовних законів про захист даних. Базові правила обробки персональних даних властиві як для європейських держав, так і для України. Проте чинний Закон був прийнятий ще у 2010 році, але з того часу змінилися технології обробки даних, способи та підходи до їх захисту.

Ефективний захист даних не є чимось недосяжним: він вимагає правового і технічного професіоналізму, виділення достатніх ресурсів і підготовки всіх фахівців, залучених до процесу обробки персональних даних. Захист даних являє собою не одиничний захід, а безперервну діяльність, що визначається організаційною стратегією, концепцією управління і готовністю нести відповідальність. Такого роду відповідальність, заснована на ретельній оцінці ризиків, спирається на документування всіх дій у сфері захисту даних, а також постійний внутрішній контроль і зовнішній нагляд.

Список використаних джерел:

1. Armstrong M. EU Data Protection Fines Hit Record High in 2023. Statista. 2023. URL: Chart: EU Data Protection Fines Hit Record High in 2023 | Statista (дата звернення: 01.08.2023)
2. Бєлова Ю. Д. Стандарти захисту права на персональні дані відповідно до Директиви 95/46/ЄС. *Університетські наукові записки*, 2017. Вип. № 63. С. 130 – 140.
3. Директива про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних: Директива 95/46/ЄС Європейського Парламенту і Ради від 24.10.1995 р. *Верховна Рада України. Законо-*

давство України. URL: https://goo.gl/kKAZGq (дата звернення: 01.08.2023)
4. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) / EURLex. URL: https://goo.gl/Klj2kL (дата звернення: 01.08.2023)
5. Консолідовані версії Договору про Європейський Союз та Договору про функціонування Європейського Союзу (2010/C 83/01). URL: old.minjust.gov.ua/file/23491.docx (дата звернення: 01.08.2023)
6. Lög um persónuvernd og vinnslu persónuupplýsinga. Lög nr. 90 27. júní 2018. URL: https://www.althingi.is/altext/148/s/1296.html (дата звернення: 01.08.2023)
7. Loi relative à l'informatique, aux fichiers et aux libertés: № 78-17 du 6.01.1978 URL: https://www.legifrance.gouv.fr/loda/id/LEGITEXT000006068624/ (дата звернення: 01.08.2023)
8. Конституція України від 28.06.1996 р. № 254к/96-ВР. *Відомості Верховної Ради України (ВВР)*, 1996. № 30. Ст. 141
9. Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI. *Відомості Верховної Ради України (ВВР)*, 2010. № 34. Ст. 481
10. Кримінальний кодекс України від 05.04.2001 р. № 2341-III. *Відомості Верховної Ради України (ВВР)*, 2001. № 25-26. Ст. 131
11. Кодекс України про адміністративні правопорушення від 07.12.1984 р. № 8073-X. *Відомості Верховної Ради Української РСР (ВВР)*, 1984. Додаток до № 51. Ст. 1122
12. Цивільний кодекс України: Закон України від 16.01.2003 р. № 435-IV. *Відомості Верховної Ради України*, 2003. №№ 40-44. Ст. 356
13. Про оперативно-розшукову діяльність: Закон України від 18.02.1992 р. № 2135-XII. *Відомості Верховної Ради України (ВВР)*, 1992. № 22. Ст. 303
14. Основи законодавства України про охорону здоров'я від 19.11.1992 р. № 2801-XII. *Відомості Верховної Ради України (ВВР)*, 1993. № 4. Ст. 19
15. Про нотаріат: Закон України від 02.09.1993 р. № 3425-XII. *Відомості Верховної Ради України (ВВР)*, 1993. № 39. Ст. 383
16. Про адвокатуру та адвокатську діяльність: Закон України від 05.07.2012 р. № 5076-VI. *Відомості Верховної Ради (ВВР)*, 2013. № 27. Ст. 282
17. Кебус А. В. Законодавства України та держав Європейського Союзу щодо кримінально-правового захисту персональних даних. *Часопис Київського університету права*, 2023. Вип. 1. С. 202 – 205.
18. Порядок здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних: наказ Уповноваженого Верховної Ради України з прав людини № 1/02-14 від 08.01.2014. URL: https://zakon.rada.gov.ua/laws/show/v1_02715-14#n92 (дата звернення: 01.08.2023)
19. Про Уповноваженого Верховної Ради України з прав людини: Закон України від 23.12.1997 р. № 776/97-ВР. *Відомості Верховної Ради України (ВВР)*, 1998. № 20. Ст. 99
20. Про основні засади державного нагляду (контролю) у сфері господарської діяльності: Закон України від 05.04.2007 р. № 877-V. *Відомості Верховної Ради України (ВВР)*, 2007. № 29. Ст. 389
21. Постанови Харківського окружного адміністративного суду у справі № 820/10192/15 від 29.10.2015 р. URL: https://reyestr.court.gov.ua/Review/53324994 (дата звернення: 01.08.2023)
22. Боднарчук О. В., Габрелян А. Ю. Розвиток системи страхування банківських вкладів України. Економіка. Фінанси. Право, 2023. № 6. С. 50 – 55.
23. Габрелян А. Ю. Вектор розвитку України: дилема вибору. Матеріали конференцій МЦНД, 2021. URL: https://doi.org/10.36074/mcnd-19.02.2021.lawgov.02 (дата звернення: 15.08.2023)
24. Чепель О. В., Габрелян А. Ю. Показання свідка в кримінальному процесі: поняття, зміст, вимоги. Аналітично-порівняльне правознавство, 2023. № 4. С. 451 – 458.
25. Чепель О. В., Габрелян А. Ю. Система прав свідка в кримінальному процесі: стан, проблеми та шляхи їх подолання. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*, 2023. № 4. С. 168 – 180.
26. Kreminskyi O., Omelchuk L., Habrelian A., Matsiuk A., Diakovskyi O. Legal regime of virtual currency in ukraine: current state, problems and prospects of regulation. *Revista Relações Internacionais do Mundo Atual*, 2023. Vol. 1. № 43. P. 21 – 24.
27. Melnyk O., Artemenko O., Yarosh A., Lytvyn O., Gabrielyan A. Administrative and legal culture of driving a vehicle as a factor in the social consciousness of a road user. *Revista Relações Internacionais do Mundo Atual*, 2021. № 3(32). URL: http://dx.doi.org/10.21902/Revrima.v3i32.550 (дата звернення: 01.08.2023)

Diakovskyi O. S., Chernetskyi S. S. Institutional support for personal data protection: experience of Ukraine and the EU

This article examines the institutional framework for personal data protection in the context of Ukraine and the EU, and compares the experience of these two regions. As Ukraine moves towards EU accession, it is actively working to adapt its personal data protection legislation to EU standards. In today's digital world, where personal data is becoming the most valuable asset, its protection is becoming an important aspect of ensuring the privacy and security of citizens. In particular, in 2010, the Law of Ukraine «On Personal Data Protection» was adopted, which defines the legal framework for protecting this data and establishes liability for its violation. However, there are certain challenges in the implementation of this law, such as the lack of effective control over compliance with data protection rules.

It has been found that, compared to Ukraine, the EU has a more developed system of institutional protection of personal data. One of the key institutions in this context is the European Data Protection Authority, which aims to ensure compliance with data protection rules in all EU member states. Additionally, the EU has adopted a general data protection regulation that gives citizens greater control over their personal data and sets high standards for data protection.

It is established that although Ukraine is actively working to improve its legislation in the area of personal data protection, it still needs to make significant efforts to achieve the same level of institutional support as in the EU. This includes improving control mechanisms, raising awareness of citizens about their data protection rights and obligations, and strengthening cooperation with international partners in this area. Although the two regions are at different stages of development in this area, further cooperation and exchange of experience can help improve personal data protection standards throughout the territory.

Key words: *information technology, personal data, standards, legal protection mechanisms, data circulation, information, subjects of protection, legal regulation, responsibility, consent to processing, digital environment.*