МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Західноукраїнський національний університет
Юридичний факультет

Кафедра адміністративного права та судочинства

Міждисциплінарна курсова робота
з дисципліни: «Актуальні питання адміністративного права та процесу»
на тему:

«Захист персональних даних у сфері надання адміністративних послуг: європейські стандарти та українська практика»

Студентка групи ПРм-11
Замосьна Наталія
Керівник: д.ю.н., доц. Гречанюк Р.В.

Національна шкала_____
*Кількість балів:*_____
*Оцінка:*_____
ECTS _____
Члени комісії: _____
_____ _____
_____

Тернопіль-2026

ЗМІСТ

ВСТУП

Актуальність теми визначається стрімкою цифровою трансформацією державного сектору, яка стала важливим досягненням України на міжнародній арені. Це підняло фундаментальне питання як забезпечити право особи на приватність в умовах загальної відкритості та цифровізації. Надання адміністративних послуг зараз практично неможливе без масштабної обробки персональних даних у державних реєстрах, що створює безпрецедентні виклики для захисту прав і свобод громадян.

Перша причина актуальності пов'язана з інтенсивним процесом європейської інтеграції. Україна, отримавши статус кандидата на вступ до Європейського Союзу, взяла на себе зобов’язання імплементувати положення Загального регламенту захисту даних - GDPR. На 2026 рік національне законодавство досягло нового рівня, де персональні дані розглядаються не просто як інформація, а як об’єкт суворого контролю з боку осіб, яким ці дані належать. Друга причина стосується впровадження концепції “*держави в телефоні*”, що призвело до створення єдиних цифрових екосистем, таких як портал та застосунок “*Дія*”, де консолідується величезна кількість даних. Це створює конфлікт між швидкістю та зручністю надання послуг і принципом мінімізації обробки даних. Третя причина пов’язана з поширенням технологій штучного інтелекту для автоматизації адміністративних рішень.

Об’єктом дослідження є суспільні відносини, які виникають у процесі обробки та захисту персональних даних під час надання адміністративних послуг державними органами та органами місцевого самоврядування. Предмет дослідження охоплює правові норми України та Європейського Союзу, які регулюють захист персональних даних, а також практичні аспекти їх застосування у сфері адміністративних послуг.

Метою курсової роботи є дослідження теоретичних підвалин та практичної реалізації європейських стандартів захисту персональних даних у системі надання адміністративних послуг України. Для досягнення вказаної мети передбачено виконання таких основних завдань як, окреслення сутності та принципів захисту персональних даних відповідно до норм GDPR, аналіз сучасного стану національного законодавства у сфері адміністративних послуг на предмет відповідності стандартам ЄС, дослідження правового статусу суб'єктів, які обробляють персональні дані на цифрових платформах, виявлення типових проблем і правових колізій, пов'язаних із збиранням та зберіганням даних користувачів, розробка пропозицій щодо гармонізації української практики із нормами європейського законодавства у сфері захисту приватності.

Методи дослідження. Серед використовуваних методів: порівняльно-правовий, системно-структурний, прогностичний формально-юридичний метод, прогностичний метод, метод аналізу та синтезу

Наукова новизна роботи полягає в комплексному аналізі впливу сучасних технологій, зокрема штучного інтелекту та хмарних рішень, на забезпечення безпеки персональних даних у сфері адміністративних послуг в Україні в умовах відповідності останнім вимогам європейських регуляторів. **Структура роботи.** Курсова робота складається зі вступу, трьох змістовних розділів, висновків і списку використаних джерел.

РОЗДІЛ 1. ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У СФЕРІ ПУБЛІЧНОГО АДМІНІСТРУВАННЯ.

1.1. Поняття та правова природа персональних даних у сфері надання адміністративних послуг.

Теоретико-правове осмислення захисту персональних даних у системі публічного адміністрування вимагає насамперед аналізу понять та змістового наповнення категорії таких як "*персональні дані*".

Зараз вже не розглядають персональні дані як суто технічну категорію, так як вони перетворилися на фундаментальний об'єкт правового захисту, що безпосередньо пов'язаний із правом на повагу до приватного та сімейного життя, гарантія якого закріплена у статті 8 Конвенції про захист прав людини і основоположних свобод.

Стаття 2 Закону України "Про захист персональних даних" - "це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована" [17]. Проте в умовах сучасного надання адміністративних послуг, які активно використовують інформаційно-комунікаційні технології, це визначення потребує розширеного тлумачення з урахуванням Загального регламенту ЄС з захисту даних GDPR. Згідно зі статтею 4 GDPR, "персональні дані охоплюють будь-яку інформацію про ідентифіковану або ідентифіковану особу, включаючи ім'я, ідентифікаційний номер, інформацію про місцезнаходження, онлайн-ідентифікатори чи будь-які інші дані, що описують фізичну, генетичну, культурну, соціальну або економічну ідентичність особи" [21].

У доктрині адміністративного права важливим є погляд на правову природу персональних даних у контексті публічних послуг. Один підхід трактує персональні дані як об'єкт інформаційних правовідносин із

акцентом на режим їх доступу та правовий статус володільця реєстру. Другий, більш поширений у європейській практиці, спирається на концепцію "*інформаційного самовизначення*". Ця концепція ґрунтується на праві особи самостійно вирішувати, коли і в яких межах інформація про її приватне життя може бути передана іншим.

Особливістю обробки персональних даних у сфері адміністративних послуг є їх імперативний характер. Відмінно від цивільно-правових відносин, де обробка переважно базується на добровільній згоді суб'єкта даних, у публічному управлінні вона часто зумовлена необхідністю виконання владою своїх законних обов'язків або завдань у суспільних інтересах. Відтак правова природа таких даних визначається балансом між суспільним інтересом і захистом приватності.

Зазначають, що "персональні дані у публічному адмініструванні є своєрідним юридичним еквівалентом особистості у цифровій площині" [23, с. 112]. Надання адміністративної послуги, наприклад реєстрації нерухомості чи оформлення соціальної субсидії, неможливе без ідентифікації громадянина. Тому дані виступають засобом індивідуалізації особи у публічно-правових взаєминах.

Актуальним також є класифікація персональних даних, які обробляються при отриманні публічних послуг. У період повної цифровізації реєстрів доцільно виділяти такі категорії інформації як: Загальні ідентифікатори ПІБ, спеціальні дані з високим ризиком для прав осіб, технічні метадані, які генеруються під час взаємодії з державними платформами.

Юридичний статус таких даних є об'єктом активних наукових дискусій. У практиці Європейського суду з прав людини, зокрема у справі Breyer v Germany, було встановлено, що "навіть динамічні IP-адреси можуть класифікуватися як персональні дані, якщо контролер володіє

правовими механізмами для ідентифікації особи за допомогою додаткової інформації, отриманої від провайдера” [26]. У контексті української практики надання адміністративних послуг це означає, що захисту підлягає не лише зміст анкети заявника, а й сам цифровий слід його звернення.

1.2. Європейські стандарти захисту персональних даних

Європейська система захисту персональних даних є передовою правовою моделлю, яка визнає інформаційну приватність одним із фундаментальних прав людини. Її сучасні стандарти формувалися в межах двох основних інституційних напрямів - Ради Європи та Європейського Союзу.

Ключовим документом Ради Європи стала Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних, прийнята 28 січня 1981 року. Вона стала першим обов’язковим міжнародним документом, що зобов’язав держави “забезпечувати в національних правових системах захист прав і свобод людини під час обробки її персональних даних” [9]. Подією стало прийняття Модернізованої Конвенції 108, яка врахувала сучасні виклики, зокрема у сфері великих даних і штучного інтелекту, а також запровадила посилені вимоги щодо підзвітності осіб, які керують обробкою даних.

Щодо Європейського Союзу, ключовим нормативним актом став Загальний регламент про захист даних GDPR 2016/679, який має пряму дію в державах-членах. Регламент встановлює суворі принципи обробки персональних даних, серед яких, законність, справедливість, прозорість, обмеження мети обробки та мінімізація даних. “Особливу роль у сфері адміністративних послуг відіграє принцип цілісності та конфіденційності” [21], що вимагає від державних установ впровадження ефективних технічних рішень для захисту даних від несанкціонованого доступу.

Роль у встановленні європейських стандартів відіграє судова практика Європейського суду з прав людини. Завдяки тлумаченню статті 8 Конвенції про захист прав людини і основоположних свобод, яка гарантує право на повагу до приватного життя, формуються принципи та межі допустимого втручання держави у сферу захисту персональних даних.

У справі “S. and Marper v. the United Kingdom” (2008) Європейський суд з прав людини визнав, що “зберігання державними органами відбитків пальців та зразків ДНК осіб, які не були засуджені, порушує право на приватність, оскільки таке втручання не відповідає критерію необхідності в демократичному суспільстві” [27]. Це рішення встановило принцип пропорційності щодо зберігання персональних даних у державних реєстрах.

В національній правовій доктрині зазначені стандарти розглядаються крізь призму євроінтеграційних процесів. Так підкреслюють, “гармонізація українського законодавства є зобов’язанням, передбаченим Угодою про асоціацію, але й ключовою умовою забезпечення безпеки інформаційного простору” [24, с. 168]. Також європейські стандарти вимагають існування незалежного наглядового органу, який має реальні інструменти для здійснення контролю над державними реєстрами. Однак це залишається об’єктом дискусій у контексті функціонування української моделі інституту Омбудсмена.

1.3 Нормативно-правове забезпечення захисту персональних даних в Україні.

Система нормативно-правового регулювання захисту персональних даних в Україні має багаторівневу структуру, яка нині перебуває у процесі активних змін. Ця трансформація обумовлена необхідністю виконання зобов’язань в межах Угоди про асоціацію між Україною та ЄС, а також

прагненням досягти адекватного рівня захисту даних, потрібного для інтеграції у Єдиний цифровий ринок Європи.

Основою цієї системи виступає Конституція України, стаття 32, передбачає, що “збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди не допускається, якщо це не передбачено законом та не відповідає інтересам національної безпеки, економічного добробуту або захисту прав людини” [8]. У рішенні обґрунтовано, що конфіденційна інформація включає дані про національність, освіту, сімейний стан, релігійні переконання, стан здоров’я, а також адресу, дату і місце народження [22].

Ключовим документом спеціалізованого законодавства є Закон України “Про захист персональних даних” № 2297-VI, який визначає термінологію, права суб’єктів даних і обов’язки володільців. Водночас зазначають, що чинна редакція Закону, хоча і базується на положеннях Директиви 95/46/ЄС, “вже недостатньо відповідає сучасним вимогам цифрового середовища та стандартам ” [5, с. 546]. Тому в перспективі на 2025-2026 роки обговорюється впровадження нового проєкту Закону “Про захист персональних даних” , який покликаний замінити застарілі положення та створити інститут незалежного наглядового органу [17].

У сфері адміністративних послуг важливу роль відіграють Закон України “Про адміністративні послуги” і Закон України “Про особливості надання публічних послуг”. Ці нормативні акти встановлюють правила обробки даних у державних реєстрах і впроваджують принцип “*єдиного вікна*”, забезпечуючи автоматичний обмін інформацією через систему “*Трембіта*” із дотриманням протоколів безпеки, визначених Законом України “Про захист інформації в інформаційно-комунікаційних системах”.

Особливим є регулювання питань цифровізації. Закон України “Про Єдиний державний демографічний реєстр” встановлює порядок роботи з біометричними даними. Часто акцентують увагу на тому, що інтеграція біометричних даних у додаток “*Дія*” “потребує не тільки технічного захисту, але й процесуального регулювання” [5, с. 550]. Це питання врегульовується низкою постанов Кабінету Міністрів України, серед яких Постанова № 911 щодо використання електронних відображень паспортів у рамках експериментального проєкту

У контексті публічного адміністрування існує Закон України “Про доступ до публічної інформації”, який регулює взаємодію між відкритістю даних і захистом приватності. Стаття 6 цього закону встановлює трискладовий тест, відповідно до якого інформація з обмеженим доступом може бути оприлюднена лише за умови, що суспільний інтерес переважає можливу шкоду від її розкриття [15].

На нормативному рівні значно виділяється типовий порядок обробки персональних даних, який затверджено Наказом Уповноваженого Верховної Ради України з прав людини. Цей документ виконує функцію практичного керівництва для центрів надання адміністративних послуг та інших органів влади, регулюючи детальні аспекти, такі як ведення журналів доступу, призначення відповідальних осіб та процедури повідомлення про порушення, пов’язані із витоком даних.

Висновок до РОЗДІЛУ 1.

Результати теоретико-правового аналізу, виконаного в першому розділі, свідчать, що захист персональних даних у сфері публічного адміністрування набув статусу фундаментального правового інституту. Цей аспект реалізує межі взаємодії між людиною і державою в умовах глобальної цифровізації. Персональні дані, з огляду на їхню правову природу, є своєрідним цифровим відображенням особи, і їх обробка в

системі адміністративних послуг має імперативний характер. Обов'язковість надання інформації державі повинна супроводжуватися найвищими стандартами її захисту та повагою принципу інформаційного самовизначення.

Аналіз європейських норм, зокрема вимог GDPR та практики Європейського суду з прав людини, демонструє потребу дотримання владою принципів пропорційності та мінімізації. Накопичення даних без конкретної адміністративної мети розглядається як недопустиме посягання на приватність. Разом із цим дослідження стану нормативно-правового забезпечення в Україні показує певний дисбаланс: технічні нововведення, як-от система "*Трембіта*" чи застосунок "*Дія*", розвиваються швидше, ніж адаптується профільне законодавство. Хоча Конституція забезпечує міцне регуляторне підґрунтя, Закон України "Про захист персональних даних" більше не відповідає сучасним викликам. Це акцентує увагу на необхідності прийняття нових законодавчих актів для гармонізації практики зі стандартами ЄС і створення реально незалежного наглядового органу.

Збалансування потреб суспільства в ефективних цифрових сервісах із забезпеченням права особи на приватність дасть змогу сформувати безпечну та прозору систему публічного адміністрування, яка відповідатиме принципам правової держави.

РОЗДІЛ 2. МЕХАНІЗМ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ПРИ НАДАННІ АДМІНІСТРАТИВНИХ ПОСЛУГ УКРАЇНІ

2.1. Особливості обробки персональних даних суб'єктами надання адміністративних послуг.

Дослідження особливостей обробки персональних даних суб'єктами, які надають адміністративні послуги, обумовлює необхідність заглибленого аналізу специфіки правовідносин, що виникають у системі державного управління між органами влади та громадянами. У сучасному контексті розвитку адміністративного права України, яке характеризується активними процесами цифровізації та адаптації до європейських стандартів, роль суб'єктів із надання послуг як контролерів даних набуває якісно нового змісту.

Однією з основних характеристик обробки персональних даних у зазначеній сфері є її правова основа. У приватних правовідносинах переважає згода фізичної особи на обробку інформації, тоді як у державному адмініструванні така діяльність зазвичай базується на прийнятому законодавстві та виконанні функцій власника персональних даних. У цьому контексті слід посилатися на статтю 11 Закону України "Про захист персональних даних", яка встановлює імперативні правила, що зобов'язують заявників надавати необхідну інформацію для отримання послуги, а державні органи - гарантувати її належний захист [17]. Такі правовідносини формують специфічний обов'язок держави бути не лише зберігачем, а й надійним захисником даних. Це надзвичайно актуально, оскільки обмеження права користувача на відмову від обробки даних фактично унеможливлює ефективне використання адміністративної послуги.

Суттєвим аспектом є також розмежування функцій власників і розпорядників даних в рамках діяльності центрів надання

адміністративних послуг. У цьому розподілі ЦНАПи відіграють роль офісу, який займається збором та первинною верифікацією інформації, водночас безпосередня обробка зазвичай залишається компетенцією спеціалізованих державних органів, таких як Державна міграційна служба або Державна реєстраційна служба. “Ризики розмивання відповідальності, що можуть виникати в умовах багаторівневої взаємодії між суб’єктами” [5, с. 547]. Ці виклики вирішуються завдяки впровадженню логічно структурованих протоколів передачі даних та технологій наскрізного шифрування, які забезпечують додатковий рівень безпеки інформації в межах системи “*Трембіта*”.

Роль в архітектурі обробки даних відіграють принципи єдиного вікна і Only Once, які спрощують взаємодію між громадянами та державними органами. Відповідно до принципу Only Once, суб’єкти не мають права повторно запитувати відомості, вже доступні в національних реєстрах. Це призводить до трансформації правового характеру обробки даних, замість виключного збирання інформації від фізичної особи установи стають активними учасниками інтегрованої системи даних.

“Таке злиття інформації сприяє ефективності процедур, але водночас потенційно створює ризики невиправданого профілювання громадян у разі нечіткої регламентації мети обробки” [1, с. 87].

Уваги заслуговує процес обробки біометричних даних та інших категорій чутливої інформації. У сфері надання послуг, пов’язаних із оформленням документів, що засвідчують особу, спеціалізовані суб’єкти обробляють цифрові зображення відбитків пальців та обличчя. Відповідно до норм GDPR, імплементованих у правову систему України, така діяльність потребує проведення оцінки впливу на захист даних. “Застосування біометричної ідентифікації у публічних сервісах має бути виключним заходом” [24, с. 170]. У цьому разі суб’єкт послуг зобов’язаний

обґрунтувати неможливість досягнення цілей ідентифікації за допомогою альтернативних, менш інвазивних способів.

2.2. Захист персональних даних в умовах цифровізації, портал та застосунок “Дія”

Аналіз функціонування порталу та мобільного застосунку “*Дія*” у 2026 році демонструє значну еволюцію механізмів захисту персональних даних у публічному секторі. Архітектурна структура екосистеми *“Дія”* побудована на основі принципу децентралізації. Зокрема, застосунок виконує роль технічного шлюзу, який не зберігає інформацію в локальній базі даних, а замість цього забезпечує її відображення у реальному часі з первинних державних реєстрів. Такий підхід значно мінімізує ймовірність “масової компрометації даних і узгоджується з принципом обмеження мети, закріпленим у статті 5 Загального регламенту про захист даних” [21].

Правовий режим функціонування цифрових документів в Україні регулюється Законом України № 1689-IX “Про особливості надання публічних (електронних публічних) послуг”, що прирівнює електронні версії документів до їхніх паперових аналогів [18]. Разом з тим значення у перспективний період 2025-2026 років набуває впровадження Дорожньої карти з питань верховенства права, яка була затверджена Кабінетом Міністрів України 14 травня 2025 року. Цей документ визначає необхідність повної адаптації національної практики до вимог модернізованої Конвенції 108+ [9], а також до положень Регламенту (ЄС) 2016/679 [3]. Одним із ключових етапів у процесі гармонізації є доопрацювання законопроєкту № 8153 “Про захист персональних даних”. У листопаді 2024 року зазначений законопроєкт пройшов перше читання та передбачає завершальне впровадження інституту незалежного наглядового органу, що стане важливим кроком у забезпеченні відповідності міжнародним стандартам [19].

Ключовим елементом безпеки застосунку "*Дія*" є використання технологій штучного інтелекту для біометричної верифікації . У цьому контексті набуває важливості думка судді Верховного Суду Я. Берназюка, який підкреслює необхідність збереження балансу між "технологічними інноваціями та забезпеченням права на приватність" [2]. Відповідно до вимог регламенту EU AI Act (Регламент ЄС 2024/1689), який почав діяти в повному обсязі у 2025–2026 роках, системи ідентифікації, що використовуються в державному управлінні, повинні відповідати суворим стандартам прозорості та проходити оцінку впливу на основоположні права [20].

Процес цифровізації за допомогою платформи "*Дія*" формує новий стандарт цифрової ідентичності, у цьому випадку захист персональних даних забезпечується не лише нормами законодавства, але й апріорно закладеними принципами архітектури системи, зокрема концепцією "*Privacy by Design*". Інструмент застосування динамічних QR-кодів для обміну документами дозволяє реалізувати правові гарантії суб'єкта щодо контролю за поширенням інформації про себе. Додатково, "впровадження механізму автоматичного логування доступів до реєстрів надає громадянам можливість у додатку відслідковувати, які саме посадові особи здійснювали перегляд його персональних даних, що забезпечує дотримання основоположного європейського принципу підзвітності" [5, с. 547].

2.3. Права суб'єкта персональних даних та порядок їх реалізації.

Забезпечення прав суб'єктів персональних даних у сфері публічного адміністрування виступає фундаментом цифрового суверенітету особи, визначаючи межі допустимого втручання держави у приватне життя. У практиці 2026 року ці права набули форми комплексного інструменту контролю, де пріоритетне місце належить праву на доступ до даних і

прозорість їх обробки. Відповідно до положень статті 8 Закону України “Про захист персональних даних”, це право реалізується в цифровій площині завдяки механізму автоматичного логування [17]. Зокрема, будь-яка взаємодія посадових осіб з даними про громадянина, що містяться у державних реєстрах, супроводжується миттєвими сповіщеннями через застосунок “*Дія*”. Такий підхід дозволяє суб’єктам персональних даних здійснювати контроль над доступом до своєї інформації в режимі реального часу, одночасно посилюючи підзвітність держави перед суспільством [12].

Особливого значення набуло право на виправлення та актуалізацію даних, що є критично важливим у контексті функціонування системи електронної взаємодії “*Трембіта*”. Недостовірні відомості в одному базовому реєстрі можуть спричинити ланцюгові помилки, які впливають на надання адміністративних послуг у мережі. Реалізація цього права ґрунтується на обов’язку держави забезпечувати точність інформації, що відповідає принципам статті 5 Загального регламенту про захист даних [21]. Одночасно право на забуття, тобто видалення даних у публічній сфері має обмежений характер і застосовується лише за умови незаконної обробки або завершення мети збору даних, як це визначено нормами європейського законодавства та положеннями перспективного законопроєкту № 8153. На додаток, впровадження технологій штучного інтелекту у державний сектор актуалізувало право осіб на оскарження рішень, прийнятих виключно автоматизованими системами . Відповідно до положень Регламенту Європейського Союзу 2024/1689 (EU AI Act), будь-яке юридично значуще рішення алгоритмічного походження має підлягати перегляду на вимогу людського втручання [20]. Що гарантує участь живої посадової особи для запобігання дискримінації, спричиненої алгоритмами.

Зазначені права можна реалізувати через адміністративний або судовий порядок захисту. Адміністративний механізм передбачає звернення до Уповноваженого Верховної Ради України з прав людини, на спеціальному порталі якого діє електронний сервіс для подання скарг щодо порушення правил обробки персональних даних [4]. У випадку неефективності адміністративного вирішення, громадяни можуть скористатися судовим захистом, що включає можливість компенсації моральної шкоди через витік або несанкціонований доступ до особистих даних.

Висновок до РОЗДІЛУ 2

Аналіз специфіки захисту персональних даних у контексті надання адміністративних послуг засвідчує, що цифрова трансформація державного сектору докорінно змінила правову природу приватності, перевівши її у площину цифрового суверенітету особи. У реаліях 2026 року обробка персональних даних державними органами набула імперативного характеру, обов'язок громадянина надати інформацію для отримання послуг супроводжується зобов'язанням держави виступати абсолютним гарантом захисту його цифрового представлення у вигляді так званого "*цифрового двійника*". Впровадження концепцій "*єдиного вікна*" та "*Тільки один раз*" через інтегровану систему обміну даними підвищило ефективність державних послуг, проте одночасно зумовило нові вимоги до точності та надійності державних реєстрів, адже будь-яка помилка в цифровій екосистемі чинить ланцюговий ефект, впливаючи на суміжні процеси.

Одним із важливих технічних і правових рішень у цьому контексті є децентралізована архітектура використання застосунку "*Дія*", що функціонує як шлюз без зберігання даних у власній базі. Це стало реальним прикладом реалізації принципу "*Privacy by Design*" . Водночас

активний розвиток технологій штучного інтелекту у процесах верифікації та надання адміністративних послуг вимагає жорсткого дотримання положень EU AI Act, та прозорості алгоритмів, а також забезпеченні обов'язкового людського втручання у процес прийняття юридично значущих рішень. У сучасній парадигмі прав суб'єктів даних фокус зміщено з формальних процедур подання запитів на користь реального проактивного контролю за доступом до персональних даних. Це реалізовано завдяки механізму автоматизованого логування: кожен громадянин тепер має змогу в режимі реального часу через цифровий інтерфейс відстежувати, хто з посадових осіб переглядав його дані та з якою метою.

Подальша інтеграція України до Єдиного цифрового ринку ЄС, а також відповідність стандартам European Digital Identity Wallet залежатимуть від завершення системних законодавчих реформ. Зокрема, важливе значення матиме остаточне ухвалення законопроєкту № 8153 та створення дійсно незалежного наглядового органу у сфері захисту персональних даних.

РОЗДІЛ 3. ПРОБЛЕМИ ГАРМОНІЗАЦІЇ УКРАЇНСЬКОГО ЗАКОНОДАВСТВА З ЄВРОПЕЙСЬКИМИ СТАНДАРТАМИ ТА ШЛЯХИ ЇХ ВИРІШЕННЯ.

3.1. Порівняльно-правовий аналіз української практики та вимог GDPR.

Сучасне правове регулювання захисту персональних даних в Україні потребує подолання концептуального розриву між застарілим Законом № 2297-VI [17] та вимогами Загального регламенту про захист даних. Наукові праці, зокрема дослідження О. Тимошенко, свідчать про еволюцію національної моделі приватності - “від імплементації Директиви 95/46/ЄС до сучасної необхідності рекодифікації цивільного законодавства відповідно до європейських стандартів” [24, с. 167]. Однією з ключових проблем є термінологічна невідповідність, що проявляється у використанні категорій “*володілець*” і “*розпорядник*” в українському праві, тоді як GDPR оперує поняттями “*контролер*” і “*процесор*”, які мають інше коло обов'язків та правових наслідків.

“Також акцентують на важливості принципів прозорості та згоди, однак в Україні згода часто має формальний характер і не відповідає встановленим критеріям добровільності та поінформованості” [24, с. 168].

Визначальним у контексті дотримання цифрових прав є правова позиція Великої Палати Верховного Суду. У постанові від 19 вересня 2018 року справа № 806/3265/17 Суд наголосив, що будь-яка обробка персональних даних державними органами становить втручання у право на повагу до приватного життя. Таке втручання визнається правомірним лише за умови неухильного дотримання справедливого балансу інтересів та принципу пропорційності, коли цифрова обробка не покладає на особу надмірного тягаря, а сама система гарантує надійний захист від витоку інформації [13]. Однак концепція “*легітимного інтересу*” як підстави для

обробки даних залишається недостатньо опрацьованою в національному праві, що обмежує потенціал цифрового ринку та застосування інноваційних технологій, зокрема штучного інтелекту. У постанові від 8 лютого 2024 року у справі № 925/200/22 Верховний Суд звернув увагу на ризики, пов’язані з використанням даних, згенерованих штучним інтелектом [14].

3.2. Відповідальність за порушення законодавства про захист персональних даних у сфері адмінпослуг.

Юридична відповідальність за порушення законів щодо захисту персональних даних у сфері надання адміністративних послуг обумовлюється необхідністю гарантування конфіденційності інформації, що міститься в державних реєстрах та інформаційних системах публічної адміністрації. Адміністративна відповідальність, передбачена статтею 188-39 КУпАП, встановлює штрафи для посадових осіб у розмірі від 3 400 до 17 000 гривень за недотримання вимог захисту, що спричинило незаконний доступ до даних чи порушення прав суб’єктів [7]. У разі повторного аналогічного порушення протягом року сума штрафу може зрости до 34 000 гривень, що відображає посилення превентивного аспекту адміністративного примусу [7].

Кримінальна відповідальність за статтею 182 КК України застосовується у випадку навмисного незаконного збору, зберігання чи розповсюдження конфіденційної інформації, особливо якщо це відбулося із застосуванням службового доступу або призвело до значної шкоди правам осіб. Такі дії можуть тягнути за собою обмеження чи позбавлення волі на строк до п'яти років [11].

В умовах цифрової трансформації державне управління потребує переходу від фіксованих штрафів до моделі повної підзвітності, властивої стандартам GDPR. Окрім публічно-правових санкцій, посадові особи

органів влади та працівники Центрів надання адміністративних послуг несуть дисциплінарну відповідальність згідно зі статтями 64-66 Закону України “Про державну службу”. До таких санкцій належать зауваження, догани або звільнення за порушення службової дисципліни чи етики поводження з інформацією [16]. З точки зору цивільно-правової відповідальності, суб'єкти мають право вимагати відшкодування моральної та матеріальної шкоди, заподіяної незаконною обробкою даних, відповідно до статей 1166-1167 Цивільного кодексу України.

Законопроєкт № 8153 передбачає запровадження низки новацій, зокрема права на забуття, мобільність даних і обов'язкове призначення інспектора із захисту даних [19]. В умовах воєнного стану країна стикається зі складним викликом - знаходженням балансу між захистом прав людини і забезпеченням національної безпеки, що обґрунтовує певні відступи у сфері приватності. Незважаючи на це, реформа передбачає посилення відповідальності, перехід від символічних адміністративних стягнень до суттєвих санкцій - штрафів до 150 млн грн або до 8% обороту компанії. Це допоможе підвищити рівень відповідності законодавства сучасним вимогам.

3.3. Перспективи реформування законодавства України в контексті набуття членства в ЄС.

Перспективи реформування законодавства України у сфері захисту персональних даних обумовлені зобов’язаннями, передбаченими Угодою про асоціацію між Україною та ЄС, а також статусом країни як кандидата на членство в Європейському Союзі. Головний напрям модернізації спрямований на перехід від застарілої редакції Закону № 2297-VI до повноцінного впровадження стандартів Загального регламенту про захист даних та положень оновленої Конвенції 108+ [17]. Основним засобом досягнення цієї мети є законопроєкт № 8153 “Про захист персональних

даних", ухвалений Верховною Радою в першому читанні 20 листопада 2024 року. Цей документ має стати основою нового правового режиму, пристосованого до викликів цифрової економіки та технологій штучного інтелекту. "Реформа повинна не лише забезпечити юридичну гармонізацію, але й сприяти отриманню Україною рішення про адекватність від Європейської Комісії, яке є важливою умовою інтеграції в Єдиний цифровий ринок ЄС" [24, с. 169].

Оновлення законодавства охоплює впровадження ключових принципів обробки даних, таких як прозорість, мінімізація та підзвітність, що вимагає від контролерів не тільки дотримання норм, але й документального підтвердження виконання заходів безпеки. Законопроєкт № 8153 значно розширює права суб'єктів даних, впроваджуючи такі нові можливості, як право на забуття, право на передання даних та заперечення проти автоматизованого профілювання [15]. Також серед пріоритетів - встановлення особливих правил для роботи з чутливими даними, зокрема біометричними показниками та медичною інформацією, що відповідає практиці Європейського суду з прав людини та рішенням Суду справедливості ЄС .

Інституційне оновлення заплановане в законопроєкті № 6177, у якому передбачено створення незалежного регулятора - Національної комісії з питань захисту персональних даних та доступу до публічної інформації. Вона матиме квазісудові повноваження та право проводити аудити. Водночас, за спостереженнями С. Хаджирадєвої, "реалізація цих положень ускладнюється в умовах воєнного стану, що потребує чітко прописаних виключень для цілей національної безпеки та захисту державних реєстрів" [25, с. 251]. Поточні дискусії із представниками бізнесу вказують необхідність адаптаційного періоду тривалістю 24-36 місяців, щоб державні органи та приватний сектор змогли належно

підготувати свої процеси до нових стандартів європейської цифрової етики.

Висновок до РОЗДІЛУ 3

Адаптація законодавства України до стандартів GDPR передбачає перехід від формальної згоди до принципу підзвітності та гармонізацію термінології щодо контролерів і процесорів. Важливість захисту приватності в умовах цифровізації та воєнного стану, що кореспондує з актуальними позиціями Верховного Суду щодо пропорційності втручання та прозорості алгоритмів справи № 806/3265/17, № 925/200/22. Відповідальність у публічному секторі наразі реалізується через адміністративні ст. 188-39 КУпАП та кримінальні ст. 182 КК санкції, проте масштабна реформа за законопроєктом № 8153 передбачає зростання штрафів до 150 млн грн та створення незалежного регулятора згідно з проєктом № 6177, що є необхідною умовою для інтеграції України в Єдиний цифровий ринок ЄС.

ВИСНОВОК

Підсумовуючи результати проведеного дослідження, можна констатувати, що правовий режим захисту персональних даних у сфері надання адміністративних послуг в Україні перебуває на етапі суттєвих трансформацій. Ці зміни зумовлені імперативом інтеграції стандартів Загального регламенту про захист даних і підготовкою до повноправного членства в Європейському Союзі. Аналіз теоретико-правових аспектів демонструє, що в умовах цифровізації персональні дані перестали виконувати функцію виключно технічного інструменту ідентифікації, трансформувавшись у цифрове відображення особистості, яке потребує найвищого рівня правового захисту. Водночас специфіка адміністративних послуг обумовлює обов'язковість збору даних, на відміну від приватного сектора з його принципом диспозитивності, у взаємодії з державою громадянин повинен надавати інформацію задля отримання публічних благ. Це, відповідно, накладає на органи влади посилену відповідальність за забезпечення максимального рівня безпеки цих даних.

Чинна нормативна база України, зокрема Закон № 2297-VI, залишається прив'язаною до застарілої Директиви 95/46/ЄС та вже не відповідає сучасним інформаційним викликам. Хоча впровадження принципу "Privacy by Design" сприяло децентралізації зберігання даних та мінімізації ризиків, відсутність чіткого закріплення прав на забуття чи мобільність даних у національному законодавстві стає перешкодою для встановлення цифрового суверенітету особистості.

Аналіз системи відповідальності свідчить на користь необхідності перегляду санкційного механізму. Діючі штрафи за порушення законодавства у сфері персональних даних стаття 188-39 КУпАП, що наразі не перевищують 34 000 гривень, є недостатніми для виконання своєї превентивної ролі, особливо порівняно із санкціями GDPR, які сягнули 20

мільйонів євро або 4 % річного обороту. Законопроєкт № 8153 пропонує радикальне збільшення розмірів штрафів до 150 мільйонів гривень, таким чином стимулюючи суб'єктів надання адміністративних послуг дотримуватися вимог комплаєнсу та впроваджувати надійні технічні й організаційні заходи захисту. Кримінальна відповідальність за статтею 182 КК України залишається крайнім заходом, застосування якого стосується випадків заподіяння істотної шкоди через розголошення конфіденційної інформації. Утім, практика її використання потребує вдосконалення, особливо у контексті зловживань службовим доступом до державних реєстрів.

Одним із ключових викликів залишається адаптація системи захисту приватності до умов воєнного стану. Повномасштабна агресія РФ підкреслила важливість пошуку балансу між національною безпекою та правом на приватність, що спричинило певні обмеження, зокрема у сфері транскордонної передачі даних для медичних потреб. Проте, як свідчить практика Верховного Суду, будь-яке втручання держави у приватне життя повинно відповідати тесту пропорційності та необхідності в демократичному суспільстві, що узгоджується з позицією ЄСПЛ у таких справах, як Breyer v. Germany і S. and Marper v. the United Kingdom. Зростання ролі штучного інтелекту в публічному управлінні також створює нові виклики в забезпеченні прозорості алгоритмів і захисту громадян від автоматизованих рішень без участі людини, що регламентується новим EU AI Act і потребує інтеграції в національне законодавство.

Інституційна реформа, передбачена законопроєктом № 6177, запланована на створення Національної комісії з питань захисту персональних даних як незалежного регулятора. Це є ключовою умовою для отримання рішення Європейської Комісії про адекватність , яке дозволить вільно передавати дані між Україною та ЄС без додаткових бюрократичних

бар'єрів. Запровадження такого органу, що матиме повноваження проводити аудити та накладати значні штрафи, трансформує підхід держави - від пасивного спостерігача до активного гаранта цифрових прав. Реформа українського законодавства спрямована на перехід від формального виконання вимог до принципу реальної підзвітності. Майбутня система захисту персональних даних у рамках адміністративних послуг повинна базуватися на трьох ключових компонентах - оновленому законодавстві, повністю сумісному з нормами GDPR, незалежному та технічно оснащеному регуляторі, і культурі цифрової етики, де приватність визнається однією з найвищих цінностей інформаційного суспільства. Лише за таких умов Україна зможе забезпечити стійку інтеграцію до Єдиного цифрового ринку ЄС і захистити інтереси своїх громадян у глобалізованому середовищі. Розробка і ухвалення нових нормативно-правових актів у 2025-2026 роках стане завершальним етапом створення цілісної системи інформаційної безпеки особи, яка відповідатиме стандартам верховенства права.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Баранов О. А., Брижко В. М. Захист персональних даних в сфері Інтернету речей. С. 85-91.
2. Берназюк Я. Штучний інтелект та право на приватність: баланс між інноваціями та захистом персональних даних : презентація доповіді. Судова влада України, лютий 2025.
3. Дорожня карта з питань верховенства права : затверджена Кабінетом Міністрів України від 14.05.2025.
   URL: https://eAu-ua.kmu.gov.ua/wp-content/uploads/UA_Dorozhnya_karta_z_pytan_verhovenstva_prava_2.pdf
   (дата звернення: 29.01.2026)
4. Електронне звернення до Омбудсмена. Офіційний сайт Уповноваженого Верховної Ради України з прав людини.
   UR https://ombudsman.gov.ua/uk/about
   (дата звернення: 29.01.2026)
5. Еннан Р. Є. Захист цифрових прав людини в інформаційній сфері // Права людини в період збройних конфліктів : зб. матеріалів Міжнар. наук.-практ. конф. (м. Одеса, 18 листопада 2022 р.). Одеса, 2022. С. 544–551.
6. Звіт Європейської Комісії щодо прогресу України в межах розширення ЄС (2024).
   URL:https://enlargement.ec.europa.eu/document/download/1924a044-b30f-48a2-99c1-50edeac14da1_en (дата звернення: 29.01.2026)
7. Кодекс України про адміністративні правопорушення : Закон України від 07.12.1984 № 8073-X.
   URL:zakon.rada.gov.ua/laws/show/80731-10
   (дата звернення: 29.01.2026)
8. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР // Відомості Верховної Ради України. 1996. № 30. Ст. 141.

URL: zakon.rada.gov.ua/laws/show/254к/96-вр
(дата звернення: 29.01.2026)

9. Конвенція про захист прав людини і основоположних свобод (з протоколами) (Європейська конвенція з прав людини).
URL: https://zakon.rada.gov.ua/laws/show/995_004#Text
(дата звернення: 29.01.2026)
10. Кохановська О. В. Теоретичні проблеми інформаційних відносин у цивільному праві : монографія. Київ : НДІ приватного права і підприємництва, 2006. С. 40–43.
URL:https://k.twirpx.link/file/339200/ (дата звернення: 29.01.2026)
11. Кримінальний кодекс України : Закон України від 05.04.2001 № 2341-III.
URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text
(дата звернення: 29.01.2026)
12. Політика приватності порталу «Дія». Офіційний вебпортал.
URL: https://diia.gov.ua/app_policy (дата звернення: 29.01.2026)
13. Постанова Великої Палати Верховного Суду від 19.09.2018 у справі № 806/3265/17.
URL:
https://supreme.court.gov.ua/supreme/pro_sud/apel_zrazk_spravi_vs_vp/2023_12_01_806_3265_17 (дата звернення: 29.01.2026)
14. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI.
URL: zakon.rada.gov.ua/laws/show/2939-17
(дата звернення: 29.01.2026)
15. Про державну службу : Закон України від 10.12.2015 № 889-VIII.
URL: zakon.rada.gov.ua/laws/show/889-19
(дата звернення: 29.01.2026)

16. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI // Відомості Верховної Ради України.
URL:zakon.rada.gov.ua/laws/show/2297-17
(дата звернення: 29.01.2026)
17. Про особливості надання публічних (електронних публічних) послуг : Закон України від 15.07.2021 № 1689-IX.
URL: https://zakon.rada.gov.ua/laws/show/1689-20#Text
(дата звернення: 29.01.2026)
18. Проєкт Закону про захист персональних даних № 8153 від 25.10.2022. (дата звернення: 29.01.2026)
URL: https://itd.rada.gov.ua/billinfo/Bills/Card/40707
20. Регламент (ЄС) 2024/1689 від 13 червня 2024 року щодо штучного інтелекту.
URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng
(дата звернення: 29.01.2026)
21. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних та про скасування Директиви 95/46/ЄС.
URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text
(дата звернення: 29.01.2026)
22. Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради щодо офіційного тлумачення положень ч. 1, 2 ст. 32 Конституції України від 20.01.2012 № 2-рп/2012.
URL: https://zakon.rada.gov.ua/laws/show/v002p710-12#Text
(дата звернення: 29.01.2026)
23. Стефанчук Р. О. Особисті немайнові права фізичних осіб монографія. К. : КНТ, 2008. 625 с.

24. Тимошенко О. Захист персональних даних у цивільних правовідносинах: національне правове забезпечення крізь призму практики ЄСПЛ.

25. Хаджирадєва С. та ін. Захист персональних даних: між захистом прав людини та національною безпекою // Social and Legal Studios. 2024. Т. 7, № 3.

26. Case of Breyer v. Germany (Application no. 50001/12).
URL: hudoc.echr.coe.int/eng?i=001-200442 (дата звернення: 29.01.2026)

27. Case of S. and Marper v. the United Kingdom. Applications nos. 30562/04 and 30566/04. Judgment of 4 December 2008. Strasbour
URL: https://hudoc.echr.coe.int/eng#{"itemid":["001-90051"]}
(дата звернення: 29.01.2026)