СУБ'ЄКТИ АДМІНІСТРАТИВНО-ПРАВОВОГО ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У СОЦІАЛЬНИХ МЕРЕЖАХ В УКРАЇНІ

КРАВЧУК Валерія Олександрівна - аспірантка кафедри конституційного і адміністративного права, Державний університет «Київський авіаційний інститут»

https://orcid.org/0009-0003-6660-2952

УДК 004:342.9(477)

DOI: https://doi.org/10.71404/EP.2025.2.7

Досліджено систему суб'єктів адміністративно-правового захисту персональних даних у соціальних мережах в Україні. Застосовано системний та структурно-функціональний аналіз для визначення особливостей правового статусу й компетенції уповноважених органів. Встановлено багаторівневу вертикальну модель захисту, яка поєднує централізовані та децентралізовані елементи управління. Проаналізовано функціональну спеціалізацію органів державної влади, зокрема Верховної Ради України, Президента України, Кабінету Міністрів, Міністерства юстиції, Міністерства цифрової трансформації та правоохоронних органів. Виявлено недоліки в інституційній структурі системи, насамперед відсутність спеціалізованого органу контролю у сфері захисту персональних даних. Обґрунтовано необхідність запровадження посади інформаційного уповноваженого для посилення інституційної спроможності держави відповідно до європейських стандартів.

Ключові слова: персональні дані, соціальні мережі, адміністративно-правовий захист, суб'єкти захисту, цифровізація, євроінтеграція, інформаційна безпека.

Постановка проблеми

Цифрова трансформація суспільних відносин та стрімкий розвиток соціальних мереж створили нові виклики для правової системи України в контексті захисту персональних даних громадян. Проблематика визначення й розмежування повноважень суб'єктів адміністративно-правового захисту персональних даних користувачів соціальних мереж набуває особливої актуальності з огляду на посилення інформаційних загроз, зростання кількості порушень прав на приватність та необхідність імплементації європейських стандартів захисту даних в умовах євроінтеграційних процесів. Як слушно зауважує К. Токарєва, рівень гарантування прав людини в цифровому просторі став важливим індикатором демократичності держави, що відкриває широке поле для наукових досліджень та вдосконалення нормативно-правової бази [1, с. 89]. Відсутність системного підходу до розподілу функцій між органами державної влади, недостатня координація їх діяльності, неузгодженість законодавства та обмеженість ресурсного забезпечення створюють суттєві перешкоди для формування ефективної системи адміністративно-правового захисту персональних даних у соціальних мережах, що потребує ґрунтовного наукового аналізу та відповідних пропозицій щодо вдосконалення.

Аналіз останніх досліджень і публікацій

Питання адміністративно-правового забезпечення захисту персональних даних висвітлювалися в роботах П. Діхтієвського, Н. Головацького, Ю. Самойленко та інших дослідників. У науковому дискурсі розроблено підходи до класифікації методів захисту, окреслено компетенцію окремих органів, сформульовано теоретичні засади нормативного регулювання у відповідній сфері.

Водночас наявна література не пропонує системної характеристики складу суб'єктів адміністративно-правового захисту, що зумовлює потребу в подальшому комплексному аналізі зазначеного напряму.

Мета дослідження – здійснити комплексний теоретико-правовий аналіз системи суб'єктів адміністративно-правового захисту персональних даних у соціальних мережах в Україні, визначити їх повноваження, функціональні обов'язки та особливості взаємодії в умовах цифровізації суспільних відносин та євроінтеграційних процесів.

Виклад основного матеріалу

Українська модель захисту персональних даних у соціальних мережах характеризується вертикальною багаторівневістю та функціональною диференціацією суб'єктів адміністративно-правового регулювання. Поєднання централізованих та децентралізованих елементів управління дозволяє забезпечити гнучкість реагування на нові виклики інформаційного середовища.

Законодавчий базис системи захисту персональних даних формується Верховною Радою України, яка відповідно до ст. 75 Конституції виступає єдиним органом законодавчої влади [2]. Парламентська функція нормативного забезпечення охоплює широкий спектр питань – від концептуального визначення критеріїв персональних даних до встановлення процедурних гарантій реалізації інформаційних прав користувачів соціальних мереж. Міжнародно-правовий вимір діяльності Верховної Ради проявляється через ратифікацію ключових міжнародних інструментів, зокрема Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних [3], що відображає інтеграційні прагнення України. Нормотворча активність парламенту визначає інституційний каркас системи захисту персональних даних, зокрема правовий статус Уповноваженого з прав людини та органів виконавчої влади, відповідальних за імплементацію профільного законодавства [4]. Потенціал парламентського контролю, закріплений у п. 13 ст. 85 Конституції, дозволяє Верховній Раді здійснювати моніторинг ефективності урядової політики у сфері захисту персональних даних, коригуючи вектор розвитку системи за необхідності [2].

Глава держави, відповідно до гл. 5 Основного закону, виступає своєрідним координатором діяльності різних гілок влади в галузі захисту персональних даних. Президент України, видаючи укази та розпорядження, визначає стратегічні напрями державної політики в інформаційній сфері. Внесення главою держави на розгляд парламенту законопроєктів щодо захисту персональних даних дозволяє оперативно реагувати на зміни інформаційного середовища. Президентський вплив на формування персонального складу Кабінету Міністрів опосередковано визначає характер виконавчо-розпорядчої діяльності у сфері захисту персональних даних. Керівництво Радою національної безпеки та оборони надає главі держави додаткових важелів впливу на інформаційну безпеку в цілому. Повноваження Президента щодо координації діяльності правоохоронних органів мають важливе значення для протидії кіберзлочинності як однієї з основних загроз безпеці персональних даних у соціальних мережах [2].

Виконавча вертикаль органів державної влади у сфері захисту персональних даних очолюється Кабінетом Міністрів України, який відповідно до ст. 20 Закону України «Про Кабінет Міністрів України» від 27.02.2014 № 794-VII центральним координатором державної політики у сфері інформаційної безпеки. Уряд забезпечує формування та реалізацію державної політики у сфері захисту інформації, координує діяльність міністерств та інших центральних органів виконавчої влади [5]. Розробка та затвердження підзаконних нормативно-правових актів, спрямованих на реалізацію положень законів у сфері захисту персональних даних [4], становить вагому складову урядової діяльності. Фінансування програм і заходів з інформаційної безпеки дозволяє забезпечити матеріальну основу функціонування системи захисту персональних даних. Координація міжнародного співробітництва України у сфері захисту персональних даних через діяльність уряду сприяє гармонізації національного законодавства з між-

народними стандартами. Кабінет Міністрів створює умови для впровадження новітніх технологій захисту інформації, підтримуючи інноваційні проєкти та ініціативи у відповідній сфері [5].

Особливе місце в системі суб'єктів адміністративно-правового захисту персональних даних посідає Уповноважений Верховної Ради України з прав людини. Наділення омбудсмена функціями контролю за дотриманням законодавства у сфері захисту персональних даних відповідає європейській моделі незалежного нагляду. Згідно зі ст. 23 Закону України «Про захист персональних даних», Уповноважений має право проводити перевірки володільців та розпорядників персональних даних, видавати обов'язкові приписи щодо усунення виявлених порушень, а також складати протоколи про адміністративні правопорушення та передавати їх до суду для розгляду [4]. Розгляд скарг громадян на порушення їхніх прав у сфері захисту персональних даних забезпечує доступність юридичного захисту для пересічних користувачів соціальних мереж. Створення спеціалізованого Департаменту в структурі Секретаріату Уповноваженого підвищило інституційну спроможність здійснення нагляду за дотриманням законодавства про захист персональних даних [6]. Вважаємо, що незалежний статус Уповноваженого від виконавчої влади гарантує неупередженість контролю та відповідність міжнародним стандартам захисту персональних даних.

Водночас поділяємо думку Г. Проскури про те, що одним із нагальних завдань на шляху євроінтеграції України є запровадження окремої посади інформаційного омбудсмена або інформаційного уповноваженого як спеціалізованого органу контролю лише у сфері захисту персональних даних [7, с. 119]. Упровадження подібного інституту повністю відповідало б загальноєвропейському підходу до гарантування права на приватність і сприяло б посиленню інституційної спроможності держави в зазначеній сфері. Наявність незалежного спеціалізованого органу, що здійснює нагляд за дотриманням законодавства про персональні дані, дала б змогу запровадити дієвіші механізми відповідальності, зокрема фінансові санкції за порушення. Інформаційний уповноважений також міг би виконувати функції попереднього оцінювання ризиків, пов'язаних з обробкою чутливої інформації, що дозволило б ефективно запобігати порушенням. Розширення міжнародної взаємодії у сфері захисту персональних даних у межах компетенції такого спеціалізованого органу посилило б спроможність України до співпраці з інституціями ЄС та провідними світовими структурами у сфері інформаційної безпеки.

Міністерство юстиції України, відповідно до Положення, затвердженого наказом Мін'юсту від 02.07.2014 № 228/5, є головним органом у сфері захисту персональних даних (п. 3 розд. I) та реалізує державну правову політику в цій сфері (підп. 3 п. 4 розд. II). У межах покладених повноважень Мін'юст забезпечує нормативно-правове регулювання у сфері захисту персональних даних (підп. 58 п. 3 розд. III), а також проводить правову експертизу проєктів нормативно-правових актів для виявлення можливих правових колізій і неузгодженостей (підп. 12 п. 3 розд. III) [8]. Міністерство координує роботу щодо адаптації законодавства України до вимог Європейського Союзу у сфері захисту персональних даних, зокрема впровадження стандартів Загального регламенту про захист даних (GDPR) [9]. Здійснення міжнародно-правового співробітництва у сфері захисту персональних даних сприяє обміну досвідом та кращими практиками з іноземними партнерами. Узагальнення практики застосування законодавства про захист персональних даних та розробка рекомендацій щодо його вдосконалення становлять важливу складову аналітичної діяльності Міністерства юстиції [8].

Специфічна роль Міністерства цифрової трансформації України зумовлена його компетенцією у сфері цифровізації та розвитку інформаційного суспільства. Відповідно до його правового статусу, закріпленого у постанові Кабінету Міністрів України від 18.09.2019 року № 856 «Питання Міністерства цифрової трансформації», міністерство визначає напрями державної політики у сфері електронного врядування, цифрових

послуг, онлайн-ідентифікації громадян та загального підвищення цифрової обізнаності населення [10]. Зазначені сфери безпосередньо стосуються захисту персональних даних в умовах цифрового середовища. У межах своєї діяльності відомство встановлює технічні вимоги до інформаційних систем, у яких здійснюється обробка персональних даних, та впроваджує технологічні рішення, спрямовані на запобігання несанкціонованому доступу або втраті інформації. Затверджений наказом Міністерства цифрової трансформації України від 20.05.2020 року № 72 порядок визначає вимоги до безпечного зберігання, доступу та захисту персональних даних у внутрішніх інформаційних системах органу [11]. У рамках просвітницької діяльності міністерство впровадило платформу «Дія.Освіта», яка підвищує рівень знань з кібербезпеки та захисту особистої інформації [12]. Серед інших повноважень – координація заходів із кіберзахисту державних ресурсів, що оперують персональними даними. Пріоритетом діяльності також є адаптація українського цифрового середовища до стандартів Європейського Союзу у сфері персональної інформаційної безпеки.

Правоохоронна складова системи захисту персональних даних представлена насамперед Національною поліцією України. Відповідно до ст. 23 Закону України «Про Національну поліцію» від 02.07.2015 року № 580-VIII, поліція має повноваження здійснювати оперативно-розшукові заходи та досудове розслідування порушень, пов'язаних з обігом інформації [13]. Протидія кіберзлочинам, спрямованим на отримання несанкціонованого доступу до персональних даних користувачів соціальних мереж, становить пріоритетний напрям діяльності кіберполіції. Співпраця з міжнародними правоохоронними організаціями у розслідуванні транскордонних злочинів, пов'язаних з персональними даними, забезпечує ефективну протидію глобальним кіберзагрозам. Запровадження сучасних технологій виявлення та документування кіберзлочинів підвищує результативність розслідування посягань на персональні дані. Проведення профілактичної роботи, спрямованої на запобігання порушенням у сфері захисту персональних даних у соціальних мережах, доповнює систему правоохоронних заходів.

Місцеві органи виконавчої влади та органи місцевого самоврядування утворюють регіональний рівень системи захисту персональних даних. Відповідно до ст. 2 та ст. 13 Закону України «Про місцеві державні адміністрації» від 09.04.1999 року № 586-XIV [14], місцеві державні адміністрації забезпечують виконання законодавства про захист персональних даних на відповідній території, координуючи діяльність територіальних підрозділів центральних органів виконавчої влади. Органи місцевого самоврядування, спираючись на ст. 29 і ст. 38 Закону України «Про місцеве самоврядування в Україні» від 21.05.1997 року № 280/97-ВР [15], встановлюють правила обробки персональних даних у комунальних підприємствах, установах та організаціях, забезпечуючи дотримання прав громадян на захист персональної інформації. Інформаційно-просвітницька діяльність місцевих органів влади сприяє підвищенню рівня обізнаності населення щодо захисту персональних даних у соціальних мережах. Розгляд звернень громадян з питань захисту персональних даних на місцевому рівні забезпечує доступність правового захисту для жителів віддалених населених пунктів. Співпраця місцевих органів влади з громадськими організаціями дозволяє ефективно виявляти та реагувати на порушення у сфері захисту персональних даних на локальному рівні.

Європейський суд з прав людини відіграє роль наднаціонального регулятора у сфері захисту персональних даних. Рішення ЄСПЛ формують єдині стандарти тлумачення та застосування положень Конвенції про захист прав людини і основоположних свобод щодо права на приватність, гарантованого ст. 8 цього міжнародного договору, яка визнає право кожної особи на повагу до приватного й сімейного життя, житла та кореспонденції. Визнання порушень права на повагу до приватного життя в конкретних справах слугує орієнтиром для національних судів та органів державної влади при вирішенні аналогічних спорів. Формування

прецедентної практики щодо захисту персональних даних у цифровому середовищі відбувається з урахуванням стрімкого розвитку інформаційних технологій та появи нових загроз приватності. Присудження справедливої сатисфакції за порушення прав на захист персональних даних, передбаченої ст. 41 Конвенції, стимулює держави до вдосконалення національних систем правового захисту [16]. Імплементація рішень ЄСПЛ у національне законодавство та правозастосовну практику забезпечує гармонізацію підходів до захисту персональних даних у європейському правовому просторі.

Колегіальні та консультативно-дорадчі органи доповнюють інституційну структуру системи захисту персональних даних в Україні. Міжвідомчі робочі групи та комісії з питань захисту персональних даних забезпечують координацію дій різних органів державної влади при розробці та реалізації державної політики у відповідній сфері (ст. 48 Закону України «Про Кабінет Міністрів України» [5]). Громадські ради при органах державної влади сприяють залученню представників громадянського суспільства до формування та реалізації державної політики у сфері захисту персональних даних (ст. 133 Закону України «Про місцеве самоврядування в Україні» [15]). Науково-консультативні ради надають експертну підтримку органам державної влади при розробці нормативно-правових актів та методичних рекомендацій з питань захисту персональних даних у соціальних мережах. Проведення громадських обговорень проєктів нормативно-правових актів з питань захисту персональних даних забезпечує врахування інтересів різних зацікавлених сторін. Аналітична діяльність консультативно-дорадчих органів сприяє виявленню системних проблем у функціонуванні механізмів захисту персональних даних та розробці рекомендацій щодо їх вирішення.

Громадський сектор відіграє дедалі більшу роль у системі захисту персональних даних у соціальних мережах. Відповідно до Закону України «Про захист персональних даних» громадські організації здійснюють моніторинг дотримання законодавства про захист персональних даних, виявляючи порушення та інформуючи про них компетентні органи державної влади. Надання правової допомоги громадянам у випадках порушення їхніх прав на захист персональних даних у соціальних мережах підвищує доступність правового захисту для користувачів (ст. 8). Проведення просвітницьких кампаній, спрямованих на підвищення обізнаності населення щодо безпечного використання соціальних мереж, сприяє формуванню культури захисту персональних даних (ст. 23). Участь у розробці законодавчих ініціатив та державних програм у сфері захисту персональних даних забезпечує врахування громадської думки при формуванні державної політики (ст. 27). Міжнародна співпраця громадських організацій дозволяє обмінюватися досвідом та кращими практиками у сфері захисту персональних даних у соціальних мережах (ст. 29) [4].

Комерційні суб'єкти, зокрема оператори соціальних мереж, посідають подвійне становище в системі захисту персональних даних. З одного боку, вони виступають об'єктами державного регулювання та контролю, зобов'язаними дотримуватися вимог законодавства про захист персональних даних. З іншого боку, оператори соціальних мереж самостійно розробляють та впроваджують політики конфіденційності, визначаючи правила обробки персональних даних користувачів. Технічний захист персональних даних від несанкціонованого доступу, модифікації, знищення становить важливу складову діяльності операторів соціальних мереж у сфері інформаційної безпеки. Надання користувачам інструментів контролю за доступом до їхніх персональних даних реалізує принцип прозорості обробки інформації. Транснаціональний характер діяльності більшості соціальних мереж створює додаткові виклики для національної системи захисту персональних даних, потребуючи розробки механізмів забезпечення дотримання українського законодавства іноземними компаніями. Зазначені положення регулюються Законом України «Про захист персональних даних», зокрема його статтями 6, 8, 24 та 1 [4].

Судова гілка влади виконує функцію остаточного арбітра в спорах щодо захис-

ту персональних даних у соціальних мережах. Розгляд адміністративних справ щодо оскарження рішень, дій чи бездіяльності суб'єктів владних повноважень у сфері захисту персональних даних забезпечує судовий контроль за законністю діяльності органів державної влади. Вирішення справ про адміністративні правопорушення у сфері захисту персональних даних реалізує функцію притягнення до відповідальності осіб, винних у порушенні законодавства. Розгляд цивільних справ про відшкодування шкоди, завданої порушенням права на захист персональних даних, забезпечує відновлення порушених прав та компенсацію заподіяних збитків. Формування єдиної судової практики в справах щодо захисту персональних даних у соціальних мережах сприяє однаковому застосуванню законодавства. Звернення судів до практики Європейського суду з прав людини при вирішенні спорів щодо захисту персональних даних забезпечує впровадження європейських стандартів у національну правозастосовну практику.

Висновок

Комплексне дослідження системи суб'єктів адміністративно-правового захисту персональних даних у соціальних мережах в Україні розкриває унікальне поєднання централізованих та децентралізованих елементів управління, що забезпечує адаптивність інституційної архітектури до динамічних викликів цифрового середовища. Вертикальна модель включає широкий спектр інституцій – від Верховної Ради України та Президента, які формують законодавчий фундамент і стратегічні орієнтири державної політики, до Кабінету Міністрів, профільних міністерств та місцевих органів влади, відповідальних за практичну реалізацію нормативних приписів на загальнодержавному та регіональному рівнях. Функціональна спеціалізація Міністерства юстиції, Міністерства цифрової трансформації та Національної поліції дозволяє комплексно охопити правові, технологічні та правоохоронні аспекти захисту персональних даних, однак недостатня координація їхніх зусиль знижує ефективність системи в цілому. Наявність Уповноваженого Верховної Ради з прав людини як контрольно-наглядового органу частково відповідає європейській моделі незалежного нагляду, проте відсутність спеціалізованого інституту інформаційного уповноваженого з розширеними повноваженнями щодо накладення санкцій та попереднього оцінювання ризиків залишається істотним недоліком української системи, що потребує законодавчого врегулювання з урахуванням євроінтеграційних прагнень України.

Література

1. Токарєва К. Забезпечення інформаційних прав людини в соціальних мережах. *Актуальні проблеми правознавства*. 2021. № 4(32). С. 88-93.

2. Конституція України : від 28.06.1996 № 254к/96-ВР : станом на 1 січ. 2020 р. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text (дата звернення: 29.04.2025).

3. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних : Конвенція Ради Європи від 28.01.1981 : станом на 6 лип. 2010 р. URL: https://zakon.rada.gov.ua/laws/show/994_326#Text (дата звернення: 03.05.2025).

4. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI : станом на 18 січ. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 03.05.2025).

5. Про Кабінет Міністрів України : Закон України від 27.02.2014 № 794-VII : станом на 24 груд. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/794-18#Text (дата звернення: 03.05.2025).

6. Уповноважений Верховної Ради України з прав людини. *Офіційний вебсайт*. URL: https://ombudsman.gov.ua/uk/informaciya-pro-pidrozdil-zpd (дата звернення: 03.05.2025).

7. Проскура Г. Перспективи створення інституту інформаційного комісара в Україні. *Конституційно-правові академічні студії*. 2016. № 1. С. 118-123.

8. Про затвердження Положення про Міністерство юстиції України : Постанова Каб. Міністрів України від 02.07.2014 № 228 : станом на 9 квіт. 2025 р. URL: https://zakon.

rada.gov.ua/laws/show/228-2014-п#Text (дата звернення: 04.05.2025).

9. General Data Protection Regulation : Regulation (EU) of 25.05.2018 no. 2016/679. URL: https://gdpr-info.eu/ (дата звернення: 03.05.2025).

10. Питання Міністерства цифрової трансформації : Постанова Каб. Міністрів України від 18.09.2019 № 856 : станом на 8 квіт. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/856-2019-п#Text (дата звернення: 04.05.2025).

11. Про затвердження Порядку обробки та захисту персональних даних, володільцем яких є Міністерство цифрової трансформації України : Наказ М-ва цифр. трансформації України від 20.05.2020 № 72 : станом на 3 груд. 2021 р. URL: https://zakon.rada.gov.ua/laws/show/z0495-20#Text (дата звернення: 04.05.2025).

12. Дія.Освіта. *Офіційний веб-сайт*. URL: https://osvita.diia.gov.ua/catalog/topic/online-security (дата звернення: 04.05.2025).

13. Про Національну поліцію : Закон України від 02.07.2015 № 580-VIII : станом на 16 серп. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text (дата звернення: 04.05.2025).

14. Про місцеві державні адміністрації : Закон України від 09.04.1999 № 586-XIV : станом на 8 січ. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/586-14#Text (дата звернення: 04.05.2025).

15. Про місцеве самоврядування в Україні : Закон України від 21.05.1997 № 280/97-ВР : станом на 5 берез. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/280/97-вр#Text (дата звернення: 04.05.2025).

16. Конвенція про захист прав людини і основоположних свобод : Конвенція Ради Європи від 04.11.1950 : станом на 1 серп. 2021 р. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text (дата звернення: 04.05.2025).

References

1. Tokarieva, K. (2021). Zabezpechennia informatsiinykh prav liudyny v sotsialnykh merezhakh [Ensuring human information rights in social networks]. *Aktualni problemy pravoznavstva – Ensuring human information rights in social networks. Current problems of jurisprudence*, (4(32)), 88-93 [in Ukrainian].

2. Konstytutsiia Ukrainy [Constitution of Ukraine], № 254k/96-VR (2020). Retrieved from: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text [in Ukrainian].

3. Konventsiia pro zakhyst osib u zviazku z avtomatyzovanoiu obrobkoiu personalnykh danykh [Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe Convention] (2010). *zakon.rada.gov.ua*. Retrieved from: https://zakon.rada.gov.ua/laws/show/994_326#Text [in Ukrainian].

4. Zakon Ukrainy"Pro zakhyst personalnykh danykh" [Law of Ukraine "On the Protection of Personal Data"] (n.d.). *zakon.rada.gov.ua*. Retrieved from: https://zakon.rada.gov.ua/laws/show/2297-17#Text [in Ukrainian].

5. Zakon Ukrainy "Pro Kabinet Ministriv Ukrainy" [Law of Ukraine "On the Cabinet of Ministers of Ukraine"] (n.d.). *zakon.rada.gov.ua*. Retrieved from: https://zakon.rada.gov.ua/laws/show/794-18#Text [in Ukrainian].

6. Upovnovazhenyi Verkhovnoi Rady Ukrainy z prav liudyny [Ombudsman of the Verkhovna Rada of Ukraine for Human Rights] (n.d.). *Official website*. Retrieved from: https://ombudsman.gov.ua/uk/informaciya-pro-pidrozdil-zpd [in Ukrainian].

7. Proskura, H. (2016). Perspektyvy stvorennia instytutu informatsiinoho komisara v Ukraini [Prospects for the establishment of the institution of the Information Commissioner in Ukraine]. *Konstytutsiino-pravovi akademichni studii – Constitutional and Legal Academic Studies*, (1), 118-123 [in Ukrainian].

8. Postanova Kabinetu Ministriv Ukrainy № 228 "Pro zatverdzhennia Polozhennia pro Ministerstvo yustytsii Ukrainy" [Resolution of the Cabinet of Ministers of Ukraine No. 228 "On the Approval of the Position of the Ministry of Justice of Ukraine"] (n.d.). *zakon.rada.gov.ua*. Retrieved from: https://zakon.rada.gov.ua/laws/show/228-2014-п#Text [in Ukrainian].

9. General Data Protection Regulation, № 2016/679 (2016) (EU). Retrieved from: https://gdpr-info.eu/ [in English].

10. Postanova Kabinetu Ministriv Ukrainy № 856 "Pytannia Ministerstva tsyfrovoi

transformatsii" [Resolution of the Cabinet of Ministers of Ukraine No. 856 "Issues of the Ministry of Digital Transformation"] (n.d.). *zakon.rada.gov.ua*. Retrieved from: https://zakon.rada.gov.ua/laws/show/856-2019-п#Text [in Ukrainian].

11. Nakaz Ministerstva tsyfrovoi transformatsii Ukrainy № 72 "Pro zatverdzhennia Poriadku obrobky ta zakhystu personalnykh danykh, volodiltsem yakykh ye Ministerstvo tsyfrovoi transformatsii Ukrainy" [Order of the Ministry of Digital Transformation of Ukraine No. 72 "On Approval of the Procedure for Processing and Protection of Personal Data, the Controller of which is the Ministry of Digital Transformation of Ukraine"] (2021). *zakon.rada.gov.ua*. Retrieved from: https://zakon.rada.gov.ua/laws/show/z0495-20#Text [in Ukrainian].

12. Diia.Osvita [Action.Education]. (n. d.). *Official website*. Retrieved from: https://osvita.diia.gov.ua/catalog/topic/online-security [in Ukrainian].

13. Zakon Ukrainy № 580-VIII "Pro Natsionalnu politsiiu" [Law of Ukraine No. 580-VIII "On the National Police"] (n.d.). *zakon.rada.gov.ua*. Retrieved from: https://zakon.rada.gov.ua/laws/show/580-19#Text [in Ukrainian].

14. Zakon Ukrainy № 586-XIV "Pro mistsevi derzhavni administratsii" [Law of Ukraine No. 586-XIV "On Local State Administrations"] (n.d.). *zakon.rada.gov.ua*. Retrieved from: https://zakon.rada.gov.ua/laws/show/586-14#Text [in Ukrainian].

15. Zakon Ukrainy № 280/97-VR "Pro mistseve samovriaduvannia v Ukraini" [Law of Ukraine No. 280/97-VR "On Local Self-Government in Ukraine"] (n.d.). *zakon.rada.gov.ua*. Retrieved from: https://zakon.rada.gov.ua/laws/show/280/97-вр#Text [in Ukrainian].

16. Konventsiia pro zakhyst prav liudyny i osnovopolozhnykh svobod [Convention for the Protection of Human Rights and Fundamental Freedoms] (2021). *zakon.rada.gov.ua*. Retrieved from https://zakon.rada.gov.ua/laws/show/995_004#Text [in Ukrainian].

Kravchuk Valeriia,
Ph.D. Candidate, Department of Constitutional and Administrative Law, State University "Kyiv Aviation Institute", Kyiv, Ukraine. https://orcid.org/0009-0003-6660-2952

ENTITIES OF ADMINISTRATIVE-LEGAL PROTECTION OF PERSONAL DATA IN SOCIAL NETWORKS IN UKRAINE

A comprehensive theoretical and legal analysis of the system of subjects involved in administrative and legal protection of personal data in social networks in Ukraine has been conducted. Methods of systematic analysis and comparative legal research were applied to determine the functional responsibilities, powers, and interaction features of these subjects in the context of European integration processes. The examination revealed a unique combination of centralized and decentralized management elements that ensures the adaptability of the institutional architecture to the dynamic challenges of the digital environment. The vertical model includes a wide spectrum of institutions – from the Verkhovna Rada of Ukraine and the President, who form the legislative foundation and strategic guidelines of state policy, to the Cabinet of Ministers, relevant ministries, and local authorities responsible for the practical implementation of regulatory requirements at national and regional levels. The functional specialization of the Ministry of Justice, Ministry of Digital Transformation, and National Police allows for comprehensive coverage of legal, technological, and law enforcement aspects of personal data protection. However, insufficient coordination of their efforts reduces the effectiveness of the system as a whole. The presence of the Parliamentary Commissioner for Human Rights as a supervisory body partially corresponds to the European model of independent oversight. The necessity of establishing an Information Commissioner institution with expanded powers regarding sanctions and preliminary risk assessment has been substantiated to bring the Ukrainian system in line with European standards of independent supervision, considering Ukraine's European integration aspirations.

Keywords: personal data, social networks, administrative and legal protection, protection entities, digitalization, European integration, information security.