

ПРИВАТНЕ АКЦІОНЕРНЕ ТОВАРИСТВО «ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«МІЖРЕГІОНАЛЬНА АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ»
ЗАХІДНОДОНБАСЬКИЙ ІНСТИТУТ

(назва навчального підрозділу)

КАФЕДРА ПРАВА

(повна назва кафедри, циклової комісії)

КУРСОВА РОБОТА

з дисципліни «Адміністративне право»

(назва дисципліни)

на тему: «Адміністративно-правове забезпечення захисту персональних даних в
Україні»

Студента (ки) Дірявко С.С.

групи ІН35-8-24-Б1П (4.6 з)

напряму підготовки (спеціальності) Право

Керівник, доцент, к.ю.н., доцент Леонова О.В.

(посада, вчене звання, науковий ступінь, прізвище та ініціали)

Оцінка:

Національна шкала _____

Кількість балів: ____ ECTS ____

Члени комісії

_____ (підпис) _____ (прізвище та ініціали)

_____ (підпис) _____ (прізвище та ініціали)

_____ (підпис) _____ (прізвище та ініціали)

Київ - 2026р.

ЗМІСТ

ВСТУП	3
РОЗДІЛ 1. ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ В УКРАЇНІ	6
1.1. Поняття та сутність захисту персональних даних	6
1.2. Нормативно-правове регулювання захисту персональних даних в Україні.....	11
РОЗДІЛ 2. ОСОБЛИВОСТІ АДМІНІСТРАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ	16
2.1. Система суб'єктів забезпечення захисту персональних даних	16
2.2. Механізми захисту персональних даних у сфері публічного управління	20
РОЗДІЛ 3. ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В УКРАЇНІ	25
3.1. Основні проблеми забезпечення захисту персональних даних	25
3.2. Перспективи вдосконалення механізму захисту персональних даних в Україні.....	29
ВИСНОВКИ	34
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	37

ВСТУП

У сучасних умовах розвитку інформаційного суспільства та цифрової трансформації державного управління питання захисту персональних даних є одним із ключових напрямів розвитку інформаційного права та адміністративно-правового регулювання. Активне впровадження інформаційно-комунікаційних технологій у діяльність органів державної влади, функціонування державних реєстрів, розвиток електронного урядування та цифрових адміністративних послуг зумовлюють необхідність забезпечення належного правового механізму захисту персональної інформації.

Захист персональних даних безпосередньо пов'язаний із забезпеченням конституційних прав людини та громадянина. Відповідно до статті 32 Конституції України ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених законом, а збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди не допускається, окрім випадків, визначених законом.

Сучасний розвиток цифрових технологій супроводжується постійним збільшенням обсягів персональної інформації, яка обробляється як органами публічної влади, так і приватними суб'єктами. У зв'язку з цим особливого значення набувають питання правового регулювання обробки персональних даних, забезпечення інформаційної безпеки, захисту прав людини у цифровому середовищі та запобігання незаконному використанню персональної інформації.

Актуальність. Особливої актуальності проблема захисту персональних даних набуває в умовах воєнного стану та розвитку цифрової держави. Функціонування електронних сервісів, державних інформаційних систем і цифрових платформ супроводжується ризиками витоку інформації, кібератак та несанкціонованого доступу до персональних даних. У зв'язку з цим формування ефективного адміністративно-правового механізму захисту персональних даних є важливою умовою забезпечення стабільного функціонування системи публічного управління.

Ступень наукової розробки. Питання адміністративно-правового забезпечення захисту персональних даних досліджували багато вітчизняних науковців, зокрема В. Б. Авер'янов, І. В. Арістова, О. В. Кохановська, Н. Б. Новицька, М. Я. Швець, І. Л. Бачило та інші. У працях зазначених учених досліджувалися проблеми інформаційного права, правового режиму персональних даних, інформаційної безпеки та цифровізації публічного управління. Разом із тим сучасні процеси розвитку електронного урядування та цифрової трансформації держави потребують подальшого наукового аналізу механізмів адміністративно-правового захисту персональних даних.

Метою курсової роботи є дослідження особливостей адміністративно-правового забезпечення захисту персональних даних в Україні, аналіз чинного законодавства у цій сфері, визначення основних проблем правового регулювання та перспектив удосконалення механізму захисту персональних даних.

Для досягнення поставленої мети необхідно вирішити такі **завдання**:

- визначити поняття та сутність захисту персональних даних;
- дослідити нормативно-правове регулювання захисту персональних даних в Україні;
- охарактеризувати систему суб'єктів забезпечення захисту персональних даних;
- проаналізувати механізми захисту персональних даних у сфері публічного управління;
- визначити основні проблеми адміністративно-правового забезпечення захисту персональних даних;
- дослідити перспективи вдосконалення механізму захисту персональних даних в Україні.

Об'єктом дослідження є суспільні відносини, що виникають у сфері захисту персональних даних.

Предметом дослідження є адміністративно-правове забезпечення захисту персональних даних в Україні.

Методологічну основу дослідження становлять загальнонаукові та спеціально-юридичні методи наукового пізнання, зокрема формально-юридичний, системно-структурний, порівняльно-правовий, аналітичний та логіко-юридичний методи.

Наукова новизна одержаних результатів полягає у комплексному дослідженні особливостей адміністративно-правового забезпечення захисту персональних даних в Україні в умовах цифровізації публічного управління та розвитку електронного урядування. У роботі проаналізовано сучасні проблеми правового регулювання захисту персональних даних та визначено перспективні напрями вдосконалення механізму їх адміністративно-правового захисту.

Практичне значення роботи полягає у можливості використання результатів дослідження для вдосконалення законодавства у сфері захисту персональних даних та розвитку механізмів інформаційної безпеки у системі публічного управління України.

Структура курсової роботи зумовлена метою та завданнями дослідження. Робота складається зі вступу, трьох розділів, шести підрозділів, висновків та списку використаних джерел.

РОЗДІЛ 1. ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ В УКРАЇНІ

1.1. Поняття та сутність захисту персональних даних

У сучасних умовах розвитку інформаційного суспільства та цифрової трансформації державного управління питання захисту персональних даних набуває особливого значення як для правової системи держави, так і для забезпечення основоположних прав і свобод людини. Активне впровадження електронного урядування, функціонування державних електронних реєстрів, автоматизація адміністративних процедур та розвиток цифрових адміністративних послуг зумовлюють постійне збільшення обсягів інформації про особу, яка обробляється органами публічної влади та іншими суб'єктами інформаційних відносин.

У зв'язку з цим проблема належного правового регулювання обробки та захисту персональних даних стає одним із ключових напрямів розвитку сучасного адміністративного та інформаційного права. У сучасних умовах персональні дані набувають не лише інформаційного, а й соціального та правового значення, оскільки їх використання безпосередньо пов'язане із реалізацією прав людини, забезпеченням приватності та функціонуванням демократичної держави.

Право на захист персональних даних є складовою права людини на повагу до приватного життя. Конституційною основою захисту персональних даних в Україні є стаття 32 Конституції України, відповідно до якої ніхто не може зазнавати втручання в його особисте і сімейне життя, а також не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом.[1] Аналіз зазначеної конституційної норми свідчить, що держава визнає право особи на контроль над інформацією про себе та покладає на органи публічної влади обов'язок забезпечити належний рівень правового захисту персональної інформації.

Конституційні положення у сфері захисту персональних даних отримали свій розвиток у Законі України «Про захист персональних даних». Відповідно до

статті 2 цього Закону персональні дані визначаються як відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Законодавче визначення свідчить про широке розуміння персональних даних, оскільки ними визнається будь-яка інформація, яка прямо чи опосередковано дозволяє встановити особу.

У сучасних умовах до персональних даних належать не лише традиційні ідентифікаційні відомості, такі як прізвище, ім'я, місце проживання чи паспортні дані, а й електронні ідентифікатори, IP-адреси, біометричні характеристики, інформація про місцезнаходження особи, медичні відомості, цифрові профілі та інші дані, що дозволяють ідентифікувати людину в інформаційному просторі.

Розвиток цифрових технологій суттєво вплинув на розуміння сутності персональних даних та механізмів їх правового захисту. Якщо раніше персональна інформація здебільшого існувала у паперовій формі та оброблялася обмеженим колом суб'єктів, то сьогодні персональні дані активно використовуються в електронних інформаційних системах, державних реєстрах, банківських сервісах, медичних електронних системах та цифрових платформах.

У науковій літературі існують різні підходи до визначення сутності захисту персональних даних. Так, І. В. Арістова визначає захист персональних даних як комплекс правових, організаційних та технічних заходів, спрямованих на забезпечення законності обробки інформації про особу та недопущення порушення її інформаційних прав. У цьому підході акцентується увага на комплексному характері захисту персональних даних, оскільки ефективне функціонування механізму їх охорони неможливе виключно за допомогою правових норм без належного технічного та організаційного забезпечення.[12]

О. В. Кохановська розглядає захист персональних даних як складову права людини на приватність та інформаційну автономію. На думку науковиці, особа повинна мати можливість самостійно визначати межі використання інформації про себе, а також контролювати процес збору, використання та поширення персональних даних. Такий підхід відповідає сучасній європейській концепції інформаційних прав людини, відповідно до якої персональні дані

розглядаються не лише як інформація, а як об'єкт особистих немайнових прав.[13]

Н. Б. Новицька акцентує увагу на адміністративно-правовому аспекті захисту персональних даних. На її думку, ефективний захист персональної інформації можливий лише за умови належного функціонування системи державного контролю за діяльністю суб'єктів, які здійснюють обробку персональних даних. У цьому контексті особливого значення набуває діяльність органів публічної влади, уповноважених забезпечувати дотримання законодавства у сфері інформаційної безпеки та захисту персональних даних.[14]

Аналіз зазначених наукових підходів свідчить, що захист персональних даних є складним правовим явищем, яке поєднує елементи конституційного, адміністративного та інформаційного права. У сучасних умовах захист персональних даних не обмежується лише заборонаю незаконного поширення інформації про особу. Він охоплює весь комплекс правовідносин, пов'язаних зі збором, зберіганням, використанням, передачею, зміною та знищенням персональної інформації.

Особливе значення у сфері захисту персональних даних мають принципи обробки персональної інформації. Відповідно до Закону України «Про захист персональних даних» обробка персональних даних повинна здійснюватися законно, добросовісно та виключно з визначеною метою. Крім того, законодавство вимагає, щоб обсяг персональних даних був співмірним із метою їх обробки, а сама інформація зберігалася не довше, ніж це необхідно для досягнення визначеної мети.[2]

Аналіз зазначених принципів свідчить, що законодавець намагається забезпечити баланс між інтересами держави, суспільства та правом особи на приватність. У сучасних умовах органи публічної влади потребують значного обсягу інформації для реалізації своїх функцій, однак така діяльність не повинна призводити до необґрунтованого втручання у приватне життя людини.

Особливо актуальним питання захисту персональних даних є у сфері публічного управління. Органи державної влади та місцевого самоврядування здійснюють обробку значних обсягів персональної інформації під час надання адміністративних послуг, ведення державних реєстрів, реалізації соціальних програм, податкового адміністрування, медичного забезпечення та виконання інших управлінських функцій.

Наприклад, функціонування Єдиного державного демографічного реєстру, електронної системи охорони здоров'я eHealth та державного порталу «Дія» пов'язане з обробкою значних масивів персональної інформації громадян. Це дозволяє значно спростити доступ населення до адміністративних послуг та підвищити ефективність функціонування системи публічного управління. Разом із тим цифровізація державного управління одночасно створює додаткові ризики незаконного використання персональних даних.

Практика свідчить, що витіки персональної інформації, кібератаки та несанкціонований доступ до державних інформаційних систем можуть становити реальну загрозу для прав і свобод людини. Особливо актуальною проблема інформаційної безпеки стала в умовах воєнного стану, коли державні інформаційні ресурси постійно перебувають під загрозою кібератак та інших форм інформаційного втручання.

У сучасних умовах захист персональних даних тісно пов'язаний із забезпеченням інформаційної безпеки держави. Саме тому адміністративно-правове забезпечення захисту персональних даних охоплює не лише правове регулювання порядку обробки інформації, а й створення ефективної системи державного контролю, кіберзахисту та технічної безпеки інформаційних систем.

Важливим елементом механізму захисту персональних даних є юридична відповідальність за порушення законодавства у цій сфері. Законодавством України передбачено адміністративну, цивільно-правову, дисциплінарну та кримінальну відповідальність за незаконне використання або поширення персональних даних.

Зокрема, стаття 182 Кримінального кодексу України встановлює відповідальність за незаконне збирання, зберігання, використання або поширення конфіденційної інформації про особу без її згоди.[8] Наявність кримінально-правового захисту персональних даних свідчить про особливу суспільну значущість права людини на приватність та необхідність забезпечення ефективної охорони персональної інформації.

Разом із тим сучасний стан правового регулювання у сфері захисту персональних даних характеризується наявністю низки проблем. Насамперед це стосується недостатньої ефективності механізмів контролю за обробкою персональних даних, фрагментарності законодавства, недостатнього рівня кібербезпеки та складності практичної реалізації права особи на захист персональної інформації.

Крім того, важливою проблемою залишається недостатній рівень правової культури у сфері захисту персональних даних. На практиці громадяни часто не усвідомлюють значення персональної інформації та ризиків її незаконного використання, а окремі суб'єкти обробки персональних даних формально ставляться до виконання вимог законодавства.

У сучасних умовах особливого значення набуває гармонізація українського законодавства із європейськими стандартами у сфері захисту персональних даних. Значний вплив на розвиток правового регулювання у цій сфері справляє Загальний регламент Європейського Союзу про захист даних (GDPR), який встановлює високі стандарти забезпечення інформаційних прав людини та визначає сучасні підходи до правового регулювання обробки персональних даних.[11]

Тому, вважаємо, що захист персональних даних є важливою складовою забезпечення прав людини в умовах розвитку цифрового суспільства та одним із ключових напрямів сучасного адміністративного й інформаційного права. Аналіз законодавства та наукових підходів дозволяє зробити висновок, що ефективний механізм захисту персональних даних повинен поєднувати правові, організаційні та технічні засоби забезпечення безпеки інформації, гарантувати

право особи на приватність та забезпечувати належний баланс між інтересами держави і правами людини у сфері інформаційних відносин.

1.2. Нормативно-правове регулювання захисту персональних даних в Україні

Нормативно-правове регулювання захисту персональних даних в Україні є важливою складовою сучасної системи інформаційного та адміністративного права. Розвиток цифрових технологій, електронного урядування та автоматизованих інформаційних систем зумовив необхідність формування комплексного правового механізму, спрямованого на забезпечення належного рівня захисту інформації про особу та гарантування права людини на приватність.

Система нормативно-правового регулювання захисту персональних даних в Україні ґрунтується на конституційних положеннях, міжнародно-правових актах, спеціальному законодавстві у сфері інформаційних відносин, а також нормативних актах, що визначають порядок функціонування інформаційних систем та діяльність органів публічної влади у сфері обробки персональної інформації.

Конституційною основою захисту персональних даних є стаття 32 Конституції України, відповідно до якої ніхто не може зазнавати втручання в його особисте і сімейне життя, а збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди не допускається, окрім випадків, визначених законом. [1] Аналіз зазначеної норми свідчить, що право на захист персональних даних є однією з конституційних гарантій права людини на приватність та інформаційну безпеку.

Важливе значення у сфері нормативно-правового регулювання захисту персональних даних мають міжнародні стандарти. Україна як держава, що орієнтується на європейську модель правового регулювання, поступово гармонізує національне законодавство із міжнародними та європейськими стандартами у сфері інформаційного права.

Одним із ключових міжнародних актів у цій сфері є Конвенція Ради Європи № 108 «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» від 1981 року. Значення цієї Конвенції полягає у тому, що вона стала першим міжнародним документом, який закріпив базові принципи правового захисту персональних даних та визначив стандарти їх обробки.[10]

Крім того, суттєвий вплив на розвиток українського законодавства у сфері захисту персональних даних має Загальний регламент Європейського Союзу про захист даних (GDPR). Незважаючи на те, що GDPR безпосередньо не є частиною законодавства України, його положення активно враховуються під час реформування національної системи правового регулювання інформаційних відносин.[11]

Європейський підхід до захисту персональних даних базується на визнанні права особи контролювати використання інформації про себе. Саме тому сучасні тенденції розвитку українського законодавства спрямовані на посилення прав суб'єктів персональних даних та забезпечення прозорості діяльності суб'єктів, які здійснюють обробку інформації.

Основним спеціальним нормативно-правовим актом у сфері захисту персональних даних в Україні є Закон України «Про захист персональних даних» від 1 червня 2010 року. Прийняття цього Закону стало важливим етапом формування національної системи інформаційного права та забезпечення правових гарантій захисту приватного життя особи.

Відповідно до статті 2 Закону персональні дані визначаються як відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. [2] Аналіз зазначеної норми свідчить, що законодавець закріпив широкий підхід до розуміння персональної інформації, що відповідає сучасним міжнародним стандартам.

Важливе значення мають положення Закону, які визначають принципи обробки персональних даних. Законодавство вимагає, щоб обробка персональної інформації здійснювалася законно, добросовісно, із чітко визначеною метою та у межах необхідного обсягу. Крім того, Закон встановлює обов'язок суб'єктів

обробки персональних даних забезпечувати належний рівень захисту інформації від незаконного доступу чи поширення.

Особливе значення у Законі України «Про захист персональних даних» приділяється правам суб'єкта персональних даних. Відповідно до статті 8 Закону особа має право знати про джерела збору інформації про себе, мету її обробки, місцезнаходження бази персональних даних, а також право вимагати зміни чи знищення персональної інформації у випадках, передбачених законом.

Аналіз положень статті 8 свідчить, що законодавець намагається забезпечити баланс між потребами держави та правом особи на інформаційну автономію. У сучасних умовах саме можливість контролювати використання персональної інформації є одним із ключових елементів права людини на приватність.

Разом із Законом України «Про захист персональних даних» важливе значення у сфері правового регулювання мають також інші нормативно-правові акти інформаційного законодавства.

Зокрема, Закон України «Про інформацію» визначає загальні принципи інформаційних відносин, встановлює види інформації та гарантії права на інформацію. Відповідно до статті 11 цього Закону інформація про фізичну особу належить до конфіденційної інформації, а її збір, використання та поширення допускаються лише за згодою особи або у випадках, передбачених законом. [3]

Важливе значення має також Закон України «Про доступ до публічної інформації». Аналіз положень цього Закону свідчить, що законодавець намагається забезпечити баланс між принципом відкритості діяльності органів публічної влади та необхідністю захисту персональних даних. Зокрема, стаття 6 Закону передбачає можливість обмеження доступу до інформації у випадках, коли її поширення може порушити право особи на приватність.

У сучасних умовах розвитку цифрового суспільства особливого значення набуває правове регулювання функціонування електронних інформаційних систем та цифрових адміністративних послуг. У зв'язку з цим важливу роль відіграють Закони України «Про електронні документи та електронний

документообіг», «Про електронні довірчі послуги», «Про електронні комунікації» та інші нормативні акти, що регулюють використання цифрових технологій у сфері публічного управління.

Функціонування державних електронних реєстрів та цифрових платформ безпосередньо пов'язане з обробкою значних обсягів персональної інформації. Наприклад, портал державних послуг «Дія» забезпечує доступ громадян до електронних документів та адміністративних сервісів, що потребує належного рівня правового та технічного захисту персональних даних.

Разом із позитивними наслідками цифровізації виникають і суттєві ризики незаконного використання інформації. Практика свідчить, що витоки персональних даних, кібератаки та незаконне втручання в інформаційні системи можуть створювати серйозну загрозу правам людини та інформаційній безпеці держави.

У зв'язку з цим важливе місце у системі нормативно-правового регулювання займає законодавство у сфері кібербезпеки та технічного захисту інформації. Зокрема, Закон України «Про основні засади забезпечення кібербезпеки України» визначає правові та організаційні основи захисту інформаційних ресурсів держави та забезпечення кібербезпеки. [7]

Особливого значення проблема правового захисту персональних даних набула в умовах воєнного стану. У сучасних умовах державні інформаційні системи постійно перебувають під загрозою кібератак та інших форм інформаційного втручання. Це зумовлює необхідність посилення державного контролю у сфері інформаційної безпеки та вдосконалення законодавства про захист персональних даних.

У науковій літературі існують різні підходи до оцінки сучасного стану правового регулювання захисту персональних даних в Україні. Так, І. В. Арістова зазначає, що українське законодавство у сфері захисту персональних даних загалом відповідає базовим європейським стандартам, однак потребує подальшого вдосконалення механізмів практичної реалізації права особи на захист інформації. [12]

О. В. Кохановська звертає увагу на недостатню ефективність механізмів державного контролю у сфері обробки персональних даних та наявність прогалин у законодавстві щодо функціонування цифрових інформаційних систем.

Н. Б. Новицька акцентує увагу на тому, що сучасний розвиток цифрового суспільства потребує комплексного оновлення інформаційного законодавства та гармонізації української системи захисту персональних даних із європейськими стандартами. [14]

Тому, нормативно-правове регулювання захисту персональних даних в Україні має комплексний характер та охоплює норми конституційного, адміністративного, інформаційного та міжнародного права. Аналіз чинного законодавства свідчить, що українська система правового регулювання захисту персональних даних поступово адаптується до сучасних європейських стандартів та потреб цифрового суспільства. Разом із тим сучасний розвиток інформаційних технологій, цифровізація публічного управління та зростання кібернетичних загроз потребують подальшого вдосконалення механізмів правового захисту персональної інформації та підвищення ефективності державного контролю у цій сфері.

РОЗДІЛ 2. ОСОБЛИВОСТІ АДМІНІСТРАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

2.1. Система суб'єктів забезпечення захисту персональних даних

Ефективність адміністративно-правового забезпечення захисту персональних даних значною мірою залежить від належного функціонування системи суб'єктів, уповноважених здійснювати правове регулювання, контроль, обробку та захист персональної інформації. У сучасних умовах цифровізації публічного управління та розвитку електронного урядування саме діяльність відповідних суб'єктів забезпечує практичну реалізацію права людини на приватність та інформаційну безпеку.

Система суб'єктів забезпечення захисту персональних даних в Україні має комплексний характер та охоплює органи державної влади, органи місцевого самоврядування, спеціально уповноважені контролюючі органи, судові органи, суб'єктів обробки персональних даних та фізичних осіб як носіїв права на захист персональної інформації.

Конституційною основою діяльності суб'єктів забезпечення захисту персональних даних є стаття 32 Конституції України, відповідно до якої не допускається втручання в особисте та сімейне життя особи, а також забороняється збирання, зберігання, використання та поширення конфіденційної інформації без згоди особи, окрім випадків, визначених законом. [1] Аналіз цієї норми свідчить, що держава не лише гарантує право людини на приватність, а й покладає на органи публічної влади обов'язок забезпечити належний механізм захисту персональних даних.

Ключове значення у системі суб'єктів захисту персональних даних має Верховна Рада України як єдиний орган законодавчої влади. Саме парламент визначає основні засади державної політики у сфері інформаційних відносин та здійснює нормативно-правове регулювання обробки персональної інформації шляхом прийняття законів.

Важливе місце у системі суб'єктів займає Кабінет Міністрів України, який забезпечує реалізацію державної політики у сфері цифрової трансформації та функціонування державних інформаційних систем. У сучасних умовах цифровізації діяльність уряду безпосередньо пов'язана із впровадженням електронного урядування, цифрових адміністративних послуг та функціонуванням державних електронних реєстрів, що передбачає постійну обробку значних обсягів персональної інформації.

Особливого значення у сфері захисту персональних даних набуває діяльність Міністерства цифрової трансформації України. Саме цей орган забезпечує формування та реалізацію державної політики у сфері цифровізації, розвитку електронних послуг та функціонування цифрової держави.

Практичним прикладом діяльності Міністерства цифрової трансформації є функціонування державного порталу «Дія». Через зазначену цифрову платформу громадяни отримують доступ до електронних документів, адміністративних послуг, податкової інформації, відомостей про місце реєстрації та інших персональних даних. У зв'язку з цим особливого значення набуває питання забезпечення належного рівня інформаційної безпеки та недопущення незаконного доступу до персональної інформації громадян. [14]

Разом із тим функціонування електронних сервісів супроводжується ризиками витоку інформації та незаконного використання персональних даних. Практика свідчить, що в умовах розвитку цифрового суспільства державні інформаційні системи дедалі частіше стають об'єктами кібератак та незаконного втручання.

Важливе місце у системі суб'єктів забезпечення захисту персональних даних займає Уповноважений Верховної Ради України з прав людини. Відповідно до Закону України «Про захист персональних даних» саме Уповноважений здійснює парламентський контроль за додержанням законодавства у сфері захисту персональних даних. [2]

Аналіз повноважень Уповноваженого свідчить, що цей орган має право проводити перевірки суб'єктів обробки персональних даних, розглядати

звернення громадян, вимагати усунення порушень законодавства та складати протоколи про адміністративні правопорушення.

Практична діяльність Уповноваженого Верховної Ради України з прав людини свідчить про наявність значної кількості порушень у сфері обробки персональних даних. Зокрема, поширеними є випадки незаконного розміщення персональної інформації у відкритому доступі, обробки даних без належної згоди особи, а також неналежного технічного захисту інформаційних систем.

На думку І. В. Арістової, діяльність Уповноваженого є важливою гарантією забезпечення інформаційних прав людини та одним із ключових елементів механізму державного контролю у сфері захисту персональних даних.

Разом із тим Н. Б. Новицька зазначає, що ефективність державного контролю у цій сфері значною мірою ускладнюється швидким розвитком цифрових технологій та постійним збільшенням обсягів інформації, яка обробляється органами публічної влади. [14]

Важливу роль у системі суб'єктів захисту персональних даних відіграють судові органи. Саме суд забезпечує захист порушених прав особи у випадках незаконного використання персональної інформації або порушення законодавства у сфері захисту персональних даних.

Важливе значення для формування судової практики у сфері захисту персональних даних має Рішення Конституційного Суду України від 20 січня 2012 року № 2-рп/2012 у справі щодо офіційного тлумачення положень частин першої та другої статті 32 Конституції України. Конституційний Суд України зазначив, що інформація про особисте та сімейне життя особи є конфіденційною, а її збирання, зберігання, використання та поширення без згоди особи є втручанням у право на приватне життя. Суд також наголосив, що таке втручання допускається лише у випадках, прямо передбачених законом та в інтересах національної безпеки, економічного добробуту та прав людини. [9]

Зазначене рішення Конституційного Суду фактично стало основою для подальшого розвитку судової практики у сфері захисту персональних даних та визначення меж допустимого втручання держави у приватне життя особи.

Важливе значення має також практика Верховного Суду. Так, у постанові Верховного Суду у справі № 757/70264/17-ц суд дійшов висновку, що номер телефону, адреса проживання та інші контактні дані особи належать до персональних даних та підлягають правовому захисту. Суд зазначив, що поширення такої інформації без згоди особи є порушенням права на приватність.[19]

Практика Європейського суду з прав людини також суттєво впливає на формування національної системи захисту персональних даних. Зокрема, у справі «S. and Marper v. the United Kingdom» ЄСПЛ визнав, що зберігання державою персональних та біометричних даних осіб без достатніх правових підстав є порушенням статті 8 Конвенції про захист прав людини і основоположних свобод, яка гарантує право на повагу до приватного життя. [20]

У рішенні у справі «Rotaru v. Romania» Європейський суд з прав людини зазначив, що держава не може здійснювати безконтрольне накопичення інформації про особу, а будь-яке втручання у сферу приватності повинно бути законним, необхідним та пропорційним поставленій меті. [21]

Аналіз практики ЄСПЛ свідчить, що сучасний європейський підхід до захисту персональних даних базується на пріоритеті прав людини та необхідності встановлення ефективних механізмів контролю за діяльністю держави у сфері обробки персональної інформації.

Важливу роль у системі суб'єктів забезпечення захисту персональних даних відіграють також органи місцевого самоврядування та інші органи виконавчої влади. Саме вони здійснюють безпосередню обробку значних обсягів інформації про фізичних осіб у процесі реалізації адміністративних процедур та надання публічних послуг.

Наприклад, органи соціального захисту населення обробляють інформацію про соціальний статус особи, органи Державної податкової служби - дані про доходи фізичних осіб, а медичні заклади - інформацію про стан здоров'я громадян.

Особливість діяльності зазначених суб'єктів полягає в тому, що вони одночасно виступають носіями владних повноважень та володільцями персональних даних. Саме тому на них покладається підвищений обов'язок забезпечення належного рівня захисту інформації.

Отже, система суб'єктів забезпечення захисту персональних даних в Україні має комплексний характер та охоплює органи законодавчої, виконавчої та судової влади, спеціально уповноважені контролюючі органи, органи місцевого самоврядування, суб'єктів обробки персональних даних та фізичних осіб як носіїв права на приватність. Аналіз законодавства, наукових підходів та судової практики свідчить, що ефективність адміністративно-правового забезпечення захисту персональних даних безпосередньо залежить від рівня взаємодії між зазначеними суб'єктами, ефективності державного контролю та здатності держави забезпечити баланс між потребами цифрового суспільства та правом людини на захист приватного життя.

2.2. Механізми захисту персональних даних у сфері публічного управління

У сучасних умовах цифровізації державного управління питання забезпечення належного механізму захисту персональних даних у сфері публічного управління набуває особливого значення. Органи державної влади та місцевого самоврядування здійснюють обробку значних обсягів інформації про фізичних осіб у процесі реалізації управлінських функцій, надання адміністративних послуг, ведення державних реєстрів та функціонування електронних інформаційних систем. У зв'язку з цим ефективність функціонування системи публічного управління значною мірою залежить від рівня правового, організаційного та технічного захисту персональних даних.

Механізм захисту персональних даних у сфері публічного управління є комплексною системою правових, організаційних та інформаційно-технічних заходів, спрямованих на забезпечення законності обробки персональної

інформації, недопущення її незаконного використання та гарантування права людини на приватність. [17]

Правовою основою функціонування механізмів захисту персональних даних є Конституція України, Закон України «Про захист персональних даних», Закон України «Про інформацію», Закон України «Про доступ до публічної інформації», а також нормативно-правові акти у сфері електронного урядування, кібербезпеки та технічного захисту інформації.

Відповідно до статті 6 Закону України «Про захист персональних даних» обробка персональних даних повинна здійснюватися з конкретною та законною метою, а обсяг персональної інформації має бути співмірним із визначеною метою її обробки. [2] Аналіз цієї норми свідчить, що законодавець встановлює принцип цільового використання персональних даних та забороняє необґрунтоване накопичення інформації про особу.

Особливість функціонування механізмів захисту персональних даних у сфері публічного управління полягає в тому, що органи державної влади одночасно виступають як суб'єктами владних повноважень, так і володільцями значних обсягів персональної інформації. Саме тому законодавство покладає на органи публічної влади підвищений обов'язок щодо забезпечення належного рівня інформаційної безпеки.

У сучасних умовах одним із ключових механізмів захисту персональних даних є правове регулювання доступу до інформації. Законодавство України встановлює, що доступ до персональних даних можливий лише за наявності законних підстав або за згодою особи. Водночас органи державної влади зобов'язані забезпечити обмеження доступу до конфіденційної інформації та недопущення її незаконного поширення. [18]

Практика свідчить, що порушення порядку доступу до персональних даних є одним із найбільш поширених порушень у сфері інформаційних правовідносин. Зокрема, нерідко виникають випадки незаконного поширення персональної інформації через неналежний рівень захисту електронних реєстрів або неправомірні дії посадових осіб.

Важливе значення для формування механізмів правового захисту персональних даних має Рішення Конституційного Суду України від 20 січня 2012 року № 2-рп/2012. Конституційний Суд України зазначив, що інформація про особисте та сімейне життя особи є конфіденційною, а її збирання, використання та поширення без згоди особи є втручанням у право на приватне життя. Суд наголосив, що будь-яке втручання у сферу приватності повинно бути законним, необхідним та пропорційним.[9]

Зазначена правова позиція Конституційного Суду України має важливе значення для діяльності органів публічної влади, оскільки встановлює межі допустимого втручання держави у сферу приватного життя особи.

Одним із ключових механізмів захисту персональних даних у сфері публічного управління є функціонування системи державного контролю. Відповідно до Закону України «Про захист персональних даних» парламентський контроль за додержанням законодавства у цій сфері здійснює Уповноважений Верховної Ради України з прав людини.[2]

Практична діяльність Уповноваженого свідчить про наявність значної кількості порушень у сфері обробки персональних даних. Зокрема, поширеними є випадки неналежного технічного захисту інформаційних систем, незаконного поширення персональної інформації та порушення порядку доступу до персональних даних.

На думку Н. Б. Новицької, сучасна система державного контролю у сфері захисту персональних даних потребує подальшого вдосконалення, оскільки стрімкий розвиток цифрових технологій значно ускладнює ефективне здійснення контрольних функцій. [14]

У сучасних умовах особливого значення набувають технічні механізми захисту персональних даних. Функціонування електронних інформаційних систем, державних реєстрів та цифрових платформ потребує використання сучасних засобів кіберзахисту та інформаційної безпеки.

Практичним прикладом функціонування цифрових механізмів захисту персональних даних є державний портал «Дія». Використання електронних

документів та цифрових сервісів супроводжується застосуванням електронної ідентифікації, електронного підпису та засобів криптографічного захисту інформації.

Разом із тим функціонування цифрових платформ супроводжується і значними ризиками. Практика свідчить, що державні інформаційні системи можуть ставати об'єктами кібератак, незаконного втручання та витоку інформації. Особливо актуальною ця проблема стала в умовах воєнного стану, коли кіберзагрози є одним із елементів інформаційної війни.

У зв'язку з цим важливим механізмом захисту персональних даних є забезпечення кібербезпеки державних інформаційних ресурсів. Закон України «Про основні засади забезпечення кібербезпеки України» визначає правові та організаційні основи захисту інформаційних систем держави та встановлює обов'язок суб'єктів забезпечувати належний рівень кіберзахисту.

Окреме значення у системі механізмів захисту персональних даних має судовий захист прав особи. Відповідно до статті 55 Конституції України права і свободи людини та громадянина захищаються судом. Особа має право звернутися до суду у випадку незаконного використання або поширення персональних даних. [1]

Важливе значення для формування судової практики має постанова Верховного Суду у справі № 757/70264/17-ц, у якій суд визнав, що номер телефону та інші контактні дані особи належать до персональних даних і підлягають правовому захисту. Суд наголосив, що поширення такої інформації без згоди особи є порушенням права на приватність. [19]

Практика Європейського суду з прав людини також суттєво впливає на формування механізмів захисту персональних даних в Україні. Зокрема, у справі «S. and Marper v. the United Kingdom» ЄСПЛ зазначив, що зберігання державою персональних та біометричних даних без достатніх правових підстав є порушенням права на повагу до приватного життя, гарантованого статтею 8 Конвенції про захист прав людини і основоположних свобод. [20]

У рішенні «Rotaru v. Romania» Європейський суд з прав людини наголосив, що держава не може здійснювати безконтрольне накопичення інформації про особу, а будь-яке втручання у сферу приватності повинно бути пропорційним та здійснюватися виключно на підставі закону. [21]

Аналіз практики ЄСПЛ свідчить, що сучасний європейський підхід до захисту персональних даних базується на необхідності забезпечення ефективного контролю за діяльністю держави у сфері обробки інформації про особу.

Науковці також по-різному оцінюють сучасний стан механізмів захисту персональних даних у сфері публічного управління. Так, І. В. Арістова зазначає, що ефективність захисту персональних даних безпосередньо залежить від поєднання правових та технічних механізмів інформаційної безпеки. [12]

О. В. Кохановська звертає увагу на те, що розвиток цифрового суспільства потребує переходу від формального нормативного регулювання до створення реальних механізмів контролю за використанням персональної інформації.

На думку М. Я. Швеця, ключовою проблемою сучасної системи захисту персональних даних є недостатній рівень цифрової та правової культури як посадових осіб, так і громадян.

Отже, механізми захисту персональних даних у сфері публічного управління мають комплексний характер та охоплюють правові, організаційні, контрольні, технічні та судові засоби забезпечення інформаційної безпеки. Аналіз законодавства, судової практики та наукових підходів свідчить, що ефективний захист персональних даних є необхідною умовою функціонування сучасної цифрової держави та важливою гарантією забезпечення права людини на приватність в умовах розвитку інформаційного суспільства.

РОЗДІЛ 3. ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В УКРАЇНІ

3.1. Основні проблеми забезпечення захисту персональних даних

У сучасних умовах розвитку цифрового суспільства проблема забезпечення належного рівня захисту персональних даних набуває особливого значення. Активна цифровізація публічного управління, функціонування державних електронних реєстрів, розвиток електронного урядування та використання автоматизованих інформаційних систем суттєво збільшують обсяги персональної інформації, яка обробляється органами державної влади та іншими суб'єктами інформаційних правовідносин. Разом із позитивними наслідками цифрової трансформації виникає і значна кількість проблем, пов'язаних із забезпеченням належного правового та технічного захисту персональних даних.

Однією з ключових проблем у сфері захисту персональних даних в Україні є недосконалість чинного законодавства та наявність окремих прогалин у правовому регулюванні інформаційних відносин. Незважаючи на існування Закону України «Про захист персональних даних», сучасний розвиток цифрових технологій значно випереджає темпи оновлення законодавства. У результаті окремі правові механізми вже не повною мірою відповідають сучасним викликам цифрового суспільства.[18]

Особливо гостро проблема недосконалості правового регулювання проявляється у сфері функціонування цифрових платформ, автоматизованої обробки інформації, використання штучного інтелекту та великих масивів даних. Чинне законодавство не містить достатньо чітких механізмів регулювання окремих сучасних інформаційних технологій, що створює ризики порушення права особи на приватність.

На думку О. В. Кохановської, українське законодавство у сфері захисту персональних даних значною мірою зберігає формальний характер та потребує адаптації до сучасних цифрових процесів. Науковиця зазначає, що розвиток

електронного урядування та цифрових сервісів вимагає комплексного оновлення механізмів правового регулювання інформаційних відносин.[13]

Важливою проблемою залишається недостатня гармонізація українського законодавства із сучасними європейськими стандартами у сфері захисту персональних даних. Незважаючи на орієнтацію України на європейський правовий простір, окремі положення національного законодавства все ще не повною мірою відповідають підходам, закріпленим у Загальному регламенті Європейського Союзу про захист даних (GDPR).[11]

Європейський підхід до захисту персональних даних базується на принципі інформаційної автономії особи та передбачає високий рівень контролю громадянина над використанням інформації про себе. Водночас в Україні механізми практичної реалізації права особи на контроль за обробкою персональних даних залишаються недостатньо ефективними.

Однією з найбільш поширених проблем є неналежний рівень технічного захисту державних інформаційних систем та електронних реєстрів. У сучасних умовах значна частина персональної інформації зберігається в електронній формі, що підвищує ризики кібератак, витоку інформації та незаконного доступу до персональних даних.

Практика свідчить, що випадки витоку персональної інформації в Україні залишаються досить поширеним явищем. Особливої актуальності ця проблема набула в умовах воєнного стану, коли державні інформаційні ресурси постійно перебувають під загрозою кібернетичного втручання.

Важливе значення у цьому контексті має Закон України «Про основні засади забезпечення кібербезпеки України», який визначає правові та організаційні основи забезпечення кібербезпеки держави. Однак аналіз практики функціонування державних інформаційних систем свідчить, що наявність законодавчого регулювання не завжди забезпечує належний рівень технічного захисту інформації.

На думку І. В. Арістової, однією з причин недостатньої ефективності механізмів захисту персональних даних є відсутність належної координації між

правовими та технічними засобами забезпечення інформаційної безпеки. Науковиця наголошує, що сучасний механізм захисту персональних даних повинен поєднувати нормативно-правове регулювання із сучасними технологіями кіберзахисту.[12]

Суттєвою проблемою у сфері захисту персональних даних є також недостатня ефективність державного контролю. Відповідно до Закону України «Про захист персональних даних» парламентський контроль у цій сфері здійснює Уповноважений Верховної Ради України з прав людини. Разом із тим стрімке збільшення обсягів інформації та кількості суб'єктів обробки персональних даних значно ускладнює здійснення ефективного контролю за дотриманням законодавства.

Н. Б. Новицька зазначає, що сучасна система державного контролю у сфері захисту персональних даних характеризується недостатнім рівнем інституційної спроможності та обмеженими можливостями оперативного реагування на порушення інформаційних прав громадян.[14]

Однією з проблем залишається і низький рівень правової культури у сфері захисту персональних даних. На практиці громадяни часто не усвідомлюють значення персональної інформації та ризиків її незаконного використання. У багатьох випадках особи самостійно поширюють значні обсяги інформації про себе у соціальних мережах, електронних сервісах та цифрових платформах без належного усвідомлення можливих наслідків.

Водночас окремі суб'єкти обробки персональних даних формально ставляться до виконання вимог законодавства та не забезпечують належного рівня інформаційної безпеки. Особливо це стосується приватних суб'єктів, діяльність яких пов'язана зі збором та обробкою значних масивів персональної інформації.

Важливою проблемою є і недостатній рівень судового захисту права особи на приватність. Незважаючи на поступове формування судової практики у сфері захисту персональних даних, кількість судових рішень у цій категорії справ залишається відносно невеликою.

Водночас судова практика свідчить про поступове посилення уваги судів до питань захисту персональної інформації. Зокрема, у Рішенні Конституційного Суду України від 20 січня 2012 року № 2-рп/2012 суд наголосив, що збирання, використання та поширення конфіденційної інформації про особу без її згоди є втручанням у приватне життя та допускається лише у випадках, прямо передбачених законом. [9]

У постанові Верховного Суду у справі № 757/70264/17-ц було зазначено, що персональні дані особи підлягають правовому захисту, а їх незаконне поширення є порушенням права людини на приватність. [19]

Разом із тим практика застосування законодавства у сфері захисту персональних даних залишається недостатньо однорідною. Судові органи не завжди однаково підходять до визначення меж допустимого втручання у приватне життя особи, що створює труднощі у практичному застосуванні законодавства.

Окремою проблемою є стрімкий розвиток цифрових технологій та використання автоматизованих систем обробки інформації. Сучасні технології дозволяють здійснювати збір, аналіз та обробку значних обсягів персональної інформації, що створює ризики формування цифрових профілів особи та використання персональних даних без належного контролю з боку громадянина.

Особливо актуальним це питання є у сфері використання соціальних мереж, мобільних застосунків та цифрових платформ, діяльність яких нерідко пов'язана із масовим збором персональної інформації користувачів.

На думку М. Я. Швеця, сучасний розвиток інформаційного суспільства потребує переходу від формального правового регулювання до створення ефективного механізму цифрової безпеки особи, який поєднуватиме правові, технічні та організаційні засоби захисту інформації.

Таким чином, сучасна система захисту персональних даних в Україні характеризується наявністю низки суттєвих проблем, пов'язаних із недосконалістю законодавства, недостатньою гармонізацією із європейськими стандартами, неналежним рівнем технічного захисту інформації, недостатньою

ефективністю державного контролю та низьким рівнем правової культури у сфері інформаційних правовідносин. Аналіз законодавства, наукових підходів та судової практики свідчить, що забезпечення належного рівня захисту персональних даних є одним із ключових завдань сучасної системи публічного управління та важливою умовою розвитку цифрової держави.

3.2. Перспективи вдосконалення механізму захисту персональних даних в Україні

Сучасний розвиток інформаційного суспільства, цифровізація публічного управління та активне впровадження електронних інформаційних систем зумовлюють необхідність постійного вдосконалення механізму захисту персональних даних в Україні. Стрімкий розвиток цифрових технологій, використання автоматизованих систем обробки інформації, електронних сервісів та державних реєстрів створюють не лише нові можливості для функціонування системи публічного управління, а й формують додаткові ризики порушення права особи на приватність.

У сучасних умовах забезпечення ефективного захисту персональних даних є важливою складовою розвитку демократичної правової держави та необхідною умовою функціонування цифрового суспільства. Саме тому одним із ключових напрямів державної політики має стати вдосконалення правового, організаційного та технічного механізму захисту персональної інформації.

Однією з основних перспектив розвитку системи захисту персональних даних є подальша гармонізація національного законодавства із європейськими стандартами у сфері інформаційного права. Особливе значення у цьому процесі має адаптація українського законодавства до положень Загального регламенту Європейського Союзу про захист даних (GDPR). [11]

Європейський підхід до захисту персональних даних базується на принципі пріоритету прав людини та необхідності забезпечення ефективного

контролю особи над використанням інформації про себе. У зв'язку з цим подальший розвиток українського законодавства повинен бути спрямований на посилення гарантій реалізації права особи на приватність та удосконалення механізмів контролю за обробкою персональних даних.

На думку О. В. Кохановської, сучасне інформаційне законодавство України потребує переходу від формального нормативного регулювання до створення ефективної системи практичного захисту персональних даних. Науковиця наголошує, що правове регулювання повинно враховувати сучасні цифрові процеси та особливості функціонування електронного урядування. [13]

Одним із перспективних напрямів удосконалення механізму захисту персональних даних є посилення інституційного контролю у цій сфері. В умовах постійного збільшення обсягів інформації, яка обробляється державними органами та приватними суб'єктами, особливого значення набуває підвищення ефективності діяльності органів, уповноважених здійснювати контроль за дотриманням законодавства про захист персональних даних.

Відповідно до Закону України «Про захист персональних даних» парламентський контроль у цій сфері здійснює Уповноважений Верховної Ради України з прав людини. Разом із тим сучасні умови розвитку цифрового суспільства потребують розширення можливостей здійснення державного контролю, підвищення рівня технічного забезпечення контрольних механізмів та вдосконалення процедур реагування на порушення інформаційних прав громадян.

Н. Б. Новицька зазначає, що ефективність системи захисту персональних даних значною мірою залежить від здатності держави створити сучасний механізм моніторингу та оперативного реагування на порушення законодавства у сфері інформаційних відносин. [14]

Важливою перспективою розвитку механізму захисту персональних даних є вдосконалення системи кібербезпеки державних інформаційних ресурсів. У сучасних умовах більшість персональної інформації зберігається та

обробляється в електронній формі, що значно підвищує ризики кібератак, незаконного втручання та витоку інформації.

Особливо актуальною ця проблема є в умовах воєнного стану, коли державні інформаційні системи перебувають під постійною загрозою кібернетичних атак. У зв'язку з цим важливого значення набуває вдосконалення технічних механізмів захисту інформації, використання сучасних засобів криптографічного захисту та посилення системи цифрової безпеки держави.

Практика функціонування електронних сервісів свідчить, що подальший розвиток цифрової держави неможливий без забезпечення належного рівня захисту персональних даних. Наприклад, функціонування порталу «Дія» передбачає обробку значних обсягів персональної інформації громадян, що потребує постійного вдосконалення системи кіберзахисту та технічної безпеки інформаційних ресурсів.

На думку І. В. Арістової, сучасний механізм захисту персональних даних повинен базуватися на поєднанні правових та технічних засобів забезпечення інформаційної безпеки. Науковиця зазначає, що самостійне нормативне регулювання без використання сучасних цифрових механізмів захисту інформації вже не може забезпечити належний рівень охорони персональних даних. [12]

Однією з важливих перспектив розвитку системи захисту персональних даних є підвищення рівня правової культури населення та формування відповідального ставлення до використання персональної інформації. У сучасних умовах значна кількість громадян самостійно поширює інформацію про себе у соціальних мережах, електронних сервісах та цифрових платформах, не усвідомлюючи можливих ризиків незаконного використання персональних даних.

У зв'язку з цим важливе значення має розвиток системи інформаційної освіти та підвищення рівня цифрової грамотності населення. Формування належної правової культури у сфері захисту персональних даних повинно стати одним із пріоритетних напрямів державної інформаційної політики.

Перспективним напрямом розвитку механізму захисту персональних даних є також удосконалення судового захисту права особи на приватність. У сучасних умовах судова практика поступово формує правові підходи до визначення меж допустимого втручання у сферу приватного життя особи та порядку використання персональної інформації.

Важливе значення для розвитку механізмів судового захисту мають правові позиції Конституційного Суду України та Верховного Суду. Зокрема, у Рішенні Конституційного Суду України від 20 січня 2012 року № 2-рп/2012 було наголошено, що втручання у сферу приватного життя особи допускається лише у випадках, прямо передбачених законом та за умови дотримання принципу пропорційності. [9]

Практика Європейського суду з прав людини також суттєво впливає на формування сучасного механізму захисту персональних даних в Україні. У справі «S. and Marper v. the United Kingdom» ЄСПЛ зазначив, що необґрунтоване зберігання персональних та біометричних даних державою є порушенням права особи на приватне життя. [20]

Аналіз практики ЄСПЛ свідчить, що сучасна європейська модель захисту персональних даних базується на принципі мінімізації втручання держави у приватне життя особи та необхідності забезпечення ефективного контролю громадянина над використанням інформації про себе.

Важливою перспективою вдосконалення механізму захисту персональних даних є також розвиток міжнародного співробітництва у сфері інформаційної безпеки та кіберзахисту. У сучасних умовах цифрові інформаційні системи мають глобальний характер, а тому ефективний захист персональних даних неможливий без міжнародної взаємодії держав у сфері боротьби з кіберзлочинністю та незаконним використанням інформації.

На думку М. Я. Швеця, сучасний розвиток цифрового суспільства потребує створення комплексної системи інформаційної безпеки, яка поєднуватиме правові, технічні та організаційні механізми захисту персональних даних.

На нашу думку, перспективи вдосконалення механізму захисту персональних даних в Україні пов'язані з подальшою гармонізацією законодавства із європейськими стандартами, посиленням державного контролю, розвитком системи кібербезпеки, удосконаленням судового захисту права на приватність та підвищенням рівня правової культури населення. Аналіз сучасних проблем та тенденцій розвитку інформаційного суспільства свідчить, що ефективний механізм захисту персональних даних є необхідною умовою функціонування цифрової держави та важливою гарантією забезпечення прав і свобод людини в умовах сучасного інформаційного простору.

ВИСНОВКИ

У результаті проведеного дослідження було проаналізовано особливості адміністративно-правового забезпечення захисту персональних даних в Україні, досліджено чинне законодавство у сфері інформаційних відносин, визначено систему суб'єктів забезпечення захисту персональної інформації та основні проблеми функціонування механізму захисту персональних даних в умовах розвитку цифрового суспільства.

Захист персональних даних є важливою складовою забезпечення права людини на приватність та одним із ключових напрямів розвитку сучасного адміністративного й інформаційного права. В умовах цифровізації публічного управління, функціонування електронних реєстрів та розвитку цифрових адміністративних послуг питання правового регулювання обробки персональної інформації набуває особливого значення як для гарантування прав і свобод людини, так і для забезпечення інформаційної безпеки держави.

Дослідження показало, що нормативно-правове регулювання захисту персональних даних в Україні має комплексний характер та ґрунтується на положеннях Конституції України, Закону України «Про захист персональних даних», міжнародних нормативно-правових актів та інших законодавчих актів у сфері інформаційних відносин. Водночас чинне законодавство не повною мірою відповідає сучасним викликам цифрового суспільства та потребує подальшого вдосконалення з урахуванням європейських стандартів у сфері захисту персональних даних.

Система суб'єктів забезпечення захисту персональних даних охоплює органи державної влади, органи місцевого самоврядування, Уповноваженого Верховної Ради України з прав людини, судові органи, суб'єктів обробки персональних даних та фізичних осіб як носіїв права на приватність. Особливе місце у системі державного контролю займає діяльність Уповноваженого Верховної Ради України з прав людини, однак сучасні умови цифровізації потребують посилення інституційної спроможності цього органу та вдосконалення механізмів контролю за обробкою персональної інформації.

Аналіз механізмів захисту персональних даних у сфері публічного управління свідчить, що вони мають комплексний характер та охоплюють правові, організаційні, контрольні, технічні й судові засоби забезпечення інформаційної безпеки. Разом із тим сучасна практика функціонування електронних інформаційних систем свідчить про наявність ризиків витоку інформації, незаконного доступу до персональних даних та недостатнього рівня технічного захисту державних інформаційних ресурсів.

Однією з ключових проблем у сфері захисту персональних даних є недостатня гармонізація українського законодавства із Загальним регламентом Європейського Союзу про захист даних (GDPR). Тому доцільним є подальше вдосконалення Закону України «Про захист персональних даних» шляхом закріплення більш чітких механізмів контролю за обробкою інформації, посилення відповідальності за порушення законодавства та розширення прав суб'єктів персональних даних.

Серйозною проблемою залишається недостатній рівень кібербезпеки державних інформаційних систем. Для підвищення ефективності захисту персональних даних необхідним є посилення технічного захисту державних електронних реєстрів, використання сучасних засобів криптографічного захисту інформації, регулярне проведення аудиту інформаційної безпеки та вдосконалення механізмів реагування на кіберінциденти. Особливо актуальними зазначені заходи є в умовах воєнного стану, коли державні інформаційні ресурси перебувають під постійною загрозою кібератак.

Проблемним залишається і недостатній рівень правової культури у сфері захисту персональних даних. Значна кількість громадян не усвідомлює ризиків незаконного використання персональної інформації та самостійно поширює значні обсяги даних у цифровому середовищі. У зв'язку з цим одним із напрямів удосконалення механізму захисту персональних даних має стати підвищення рівня цифрової грамотності населення та проведення інформаційно-роз'яснювальної роботи щодо безпечного використання персональної інформації.

Аналіз судової практики свідчить про поступове формування механізму судового захисту права особи на приватність. Важливе значення для розвитку практики захисту персональних даних мають Рішення Конституційного Суду України від 20 січня 2012 року № 2-рп/2012, практика Верховного Суду та рішення Європейського суду з прав людини, зокрема у справах «S. and Marper v. the United Kingdom» та «Rotaru v. Romania». Разом із тим для забезпечення більш ефективного судового захисту необхідним є формування єдиної судової практики щодо застосування законодавства у сфері захисту персональних даних.

Отже, ефективний механізм захисту персональних даних є необхідною умовою функціонування сучасної цифрової держави та важливою гарантією забезпечення прав і свобод людини в умовах розвитку інформаційного суспільства. Подальше вдосконалення системи адміністративно-правового забезпечення захисту персональних даних повинно бути спрямоване на оновлення законодавства, посилення державного контролю, розвиток системи кібербезпеки, гармонізацію із європейськими стандартами та підвищення ефективності практичного захисту права людини на приватність.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Конституція України : Закон України від 28 червня 1996 р. № 254к/96-ВР. URL: <https://zakon.rada.gov.ua/laws/show/254к/96-вр>
2. Про захист персональних даних : Закон України від 1 червня 2010 р. № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17>
3. Про інформацію : Закон України від 2 жовтня 1992 р. № 2657-XII. URL: <https://zakon.rada.gov.ua/laws/show/2657-12>
4. Про доступ до публічної інформації : Закон України від 13 січня 2011 р. № 2939-VI. URL: <https://zakon.rada.gov.ua/laws/show/2939-17>
5. Про електронні документи та електронний документообіг : Закон України від 22 травня 2003 р. № 851-IV. URL: <https://zakon.rada.gov.ua/laws/show/851-15>
6. Про електронні довірчі послуги : Закон України від 5 жовтня 2017 р. № 2155-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2155-19>
7. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 р. № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19>
8. Кримінальний кодекс України : Закон України від 5 квітня 2001 р. № 2341-III. URL: <https://zakon.rada.gov.ua/laws/show/2341-14>
9. Рішення Конституційного Суду України від 20 січня 2012 р. № 2-рп/2012. URL: <https://zakon.rada.gov.ua/laws/show/v002p710-12>
10. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28 січня 1981 р. URL: https://zakon.rada.gov.ua/laws/show/994_326
11. General Data Protection Regulation (GDPR) : Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
12. Арістова І. В. Державна інформаційна політика: організаційно-правові аспекти : монографія. Харків : Ун-т внутр. справ, 2000. 368 с.

13. Кохановська О. В. Теоретико-правові проблеми інформаційних відносин в Україні : монографія. Київ : Видавничо-поліграфічний центр «Київський університет», 2006. 463 с.

14. Новицька Н. Б. Захист персональних даних в умовах цифровізації державного управління. *Інформація і право*. 2021. № 2. С. 98–104.

15. Авер'янов В. Б. Адміністративне право України. Академічний курс : підручник : у 2 т. Київ : Юридична думка, 2007. Т. 1. 592 с.

16. Стеценко С. Г. Адміністративне право України : навч. посіб. Київ : Атіка, 2011. 624 с

17. Баранов О. А. Право на захист персональних даних: проблеми становлення та розвитку в Україні. *Правова інформатика*. 2013. № 2. С. 5–11.

18. Пилипчук В. Г., Брижко В. М. Проблеми захисту персональних даних у сучасних умовах розвитку інформаційного суспільства. *Інформація і право*. 2018. № 3. С. 34–40.

19. Постанова Верховного Суду у справі № 757/70264/17-ц. URL: <https://reyestr.court.gov.ua>

20. Case of S. and Marper v. the United Kingdom (Applications nos. 30562/04 and 30566/04). URL: <https://hudoc.echr.coe.int>

21. Case of Rotaru v. Romania (Application no. 28341/95). URL: <https://hudoc.echr.coe.int>