

ПРИВАТНЕ АКЦІОНЕРНЕ ТОВАРИСТВО
«ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«МІЖРЕГІОНАЛЬНА АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ»
Херсонський інститут

КУРСОВА РОБОТА

з дисципліни: Інформаційне право

на тему:

Відповідальність за витік персональних даних

Виконала:
Студентка групи ІН19-9-22-Б1Пр (4,0дс)
Лютик Ольга
Керівник: к.ю.н., доцент Мкртчян Р.С.

Оцінка:
Національна шкала _____
Кількість балів: _____ ECTS _____

Члени комісії

_____	_____
(підпис)	(прізвище та ініціали)
_____	_____
(підпис)	(прізвище та ініціали)
_____	_____
(підпис)	(прізвище та ініціали)

2026 рік

ЗМІСТ

ВСТУП	3
РОЗДІЛ 1. ТЕОРЕТИКО-ПРАВОВІ ОСНОВИ ВІДПОВІДАЛЬНОСТІ ЗА ВИТІК ПЕРСОНАЛЬНИХ ДАНИХ	6
1.1. Поняття персональних даних та їх правова природа.....	6
1.2. Витік персональних даних як правове явище	9
1.3. Загальні засади юридичної відповідальності у сфері захисту персональних даних	12
РОЗДІЛ 2. ПРАВОВЕ РЕГУЛЮВАННЯ ТА ВИДИ ВІДПОВІДАЛЬНОСТІ ЗА ВИТІК ПЕРСОНАЛЬНИХ ДАНИХ	16
2.1. Національне законодавство України у сфері захисту персональних даних	16
2.2. Міжнародно-правові стандарти та європейський досвід (GDPR)	18
2.3. Види юридичної відповідальності за витік персональних даних	21
РОЗДІЛ 3. ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ ВДОСКОНАЛЕННЯ ВІДПОВІДАЛЬНОСТІ ЗА ВИТІК ПЕРСОНАЛЬНИХ ДАНИХ	26
3.1. Актуальні проблеми притягнення до відповідальності за витік персональних даних	26
3.2. Захист прав суб'єктів персональних даних та механізми їх реалізації..	29
3.3. Напрями вдосконалення законодавства та практики застосування відповідальності	32
ВИСНОВКИ.....	36
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	39

ВСТУП

У сучасних умовах цифровізації суспільства та стрімкого розвитку інформаційних технологій персональні дані набувають особливої цінності та значення. Вони стали важливим ресурсом, який активно використовується у різних сферах — від електронної комерції та банківської діяльності до державного управління та соціальних послуг. Водночас розширення обсягів обробки персональних даних супроводжується зростанням ризиків їх незаконного використання, витоку та порушення права на приватність.

Проблема витоку персональних даних є однією з найбільш актуальних у сучасному інформаційному суспільстві. Масові витoki інформації, зокрема баз даних користувачів, банківських клієнтів або державних реєстрів, стають дедалі поширенішими та можуть призводити до значних негативних наслідків як для окремих осіб, так і для суспільства в цілому. Такі інциденти створюють загрозу фінансовій безпеці, репутації, а також порушують фундаментальні права людини, зокрема право на недоторканність приватного життя.

Особливої актуальності ця проблема набуває в умовах розвитку цифрових сервісів та активного використання інтернет-технологій, коли обробка персональних даних здійснюється в автоматизованому режимі та часто має транскордонний характер. Це ускладнює контроль за дотриманням законодавства та притягнення винних осіб до відповідальності. Крім того, значна частина персональних даних обробляється приватними компаніями, що створює додаткові виклики для забезпечення їх захисту.

Складність правового регулювання відповідальності за витік персональних даних полягає у необхідності поєднання різних галузей права — інформаційного, адміністративного, цивільного та кримінального. Водночас законодавство України у цій сфері потребує подальшого вдосконалення,

оскільки не завжди забезпечує ефективні механізми притягнення до відповідальності та захисту прав суб'єктів персональних даних.

Важливим фактором є також вплив міжнародно-правових стандартів, зокрема європейського законодавства, яке встановлює високі вимоги до захисту персональних даних та відповідальності за їх порушення. У контексті євроінтеграційних процесів Україна повинна адаптувати своє законодавство до цих стандартів, що обумовлює необхідність глибокого наукового аналізу відповідних правових механізмів.

Таким чином, актуальність теми дослідження зумовлена зростанням кількості випадків витоку персональних даних, необхідністю забезпечення ефективного правового захисту інформації та вдосконаленням механізмів юридичної відповідальності у цій сфері в умовах сучасного інформаційного суспільства.

Метою курсової роботи є комплексне дослідження правових засад відповідальності за витік персональних даних, визначення особливостей її нормативного регулювання, виявлення проблем у цій сфері та обґрунтування напрямів вдосконалення законодавства і практики його застосування.

Для досягнення поставленої мети визначено такі завдання:

- розкрити поняття персональних даних та їх правову природу;
- дослідити сутність витоку персональних даних як правового явища;
- визначити види та особливості юридичної відповідальності у сфері захисту персональних даних;
- проаналізувати національне законодавство України щодо захисту персональних даних;
- дослідити міжнародно-правові стандарти та європейський досвід у цій сфері;
- охарактеризувати види відповідальності за витік персональних даних;

- виявити актуальні проблеми притягнення до відповідальності;
- обґрунтувати напрями вдосконалення законодавства та механізмів захисту персональних даних.

Об’єктом дослідження є суспільні відносини, що виникають у процесі обробки, зберігання та захисту персональних даних.

Предметом дослідження є норми національного та міжнародного права, що регулюють відповідальність за витік персональних даних, а також механізми їх реалізації та застосування.

У процесі дослідження використано такі методи: діалектичний метод, формально-логічний метод, системно-структурний метод, порівняльно-правовий метод, історико-правовий метод, метод аналізу та синтезу, узагальнення, а також метод правового моделювання.

Структура курсової роботи зумовлена метою та завданнями дослідження і складається зі вступу, трьох розділів, які поділяються на підрозділи, висновків та списку використаних джерел.

РОЗДІЛ 1. ТЕОРЕТИКО-ПРАВОВІ ОСНОВИ ВІДПОВІДАЛЬНОСТІ ЗА ВИТІК ПЕРСОНАЛЬНИХ ДАНИХ

1.1. Поняття персональних даних та їх правова природа

У сучасному інформаційному суспільстві персональні дані виступають одним із ключових об'єктів правового регулювання, що зумовлено їх значенням для реалізації прав і свобод людини. Активне використання інформаційно-комунікаційних технологій призводить до постійного зростання обсягів обробки персональних даних, що, у свою чергу, потребує чіткого правового визначення цього поняття та встановлення ефективних механізмів їх захисту.

У законодавстві України поняття персональних даних закріплено в Законі України «Про захист персональних даних». Відповідно до цього нормативного акту, персональні дані визначаються як відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована [1]. Таке визначення підкреслює, що персональні дані охоплюють не лише прямі ідентифікатори особи, але й будь-яку інформацію, яка у поєднанні з іншими даними дозволяє встановити її особу.

Наукова доктрина розширює підхід до розуміння персональних даних, розглядаючи їх як особливий вид інформації, що має індивідуалізований характер та безпосередньо пов'язаний із особистістю людини. Дослідники підкреслюють, що персональні дані є складовою права на приватність та виступають об'єктом правової охорони, оскільки їх незаконне використання може призвести до порушення прав і свобод особи [2, с. 54].

Особливістю персональних даних є їх тісний зв'язок із особою, до якої вони належать. Вони відображають різні аспекти життя людини — від базових ідентифікаційних даних до інформації про її соціальний статус, фінансове

становище, стан здоров'я чи особисті вподобання. У зв'язку з цим персональні дані мають підвищений рівень правового захисту порівняно з іншими видами інформації.

У сучасних умовах важливим є також розмежування понять «персональні дані» та «інформація про особу». Хоча ці категорії є близькими за змістом, персональні дані мають більш конкретизований характер і безпосередньо пов'язані з можливістю ідентифікації фізичної особи. Це має важливе значення для визначення обсягу правового регулювання та застосування відповідних норм законодавства.

Значну роль у формуванні підходів до визначення персональних даних відіграють міжнародні стандарти, зокрема європейське законодавство. У цьому контексті важливим є підхід, за яким персональні дані охоплюють будь-яку інформацію, що прямо або опосередковано дозволяє ідентифікувати особу, включаючи цифрові ідентифікатори, такі як IP-адреси, геолокаційні дані тощо. Це свідчить про розширення змісту поняття персональних даних у сучасних умовах цифровізації.

Таким чином, поняття персональних даних у законодавстві та науковій доктрині розглядається як сукупність інформації, що дозволяє ідентифікувати фізичну особу та пов'язана з її приватним життям. Розуміння цього поняття є основою для подальшого дослідження механізмів їх захисту та відповідальності за порушення у сфері обробки персональних даних.

Персональні дані як об'єкт правового регулювання характеризуються значною різноманітністю, що зумовлює необхідність їх класифікації. Поділ персональних даних на окремі види має важливе значення для визначення рівня їх правового захисту, порядку обробки та відповідальності за їх незаконне використання або витік.

Одним із основних критеріїв класифікації є зміст персональних даних. Залежно від цього виділяють загальні (звичайні) персональні дані, до яких належать відомості про ім'я, прізвище, дату народження, місце проживання, контактні дані тощо. Такі дані використовуються для ідентифікації особи у повсякденних правовідносинах і є найбільш поширеними.

Окрему категорію становлять чутливі (спеціальні) персональні дані, які потребують підвищеного рівня захисту. До них належать відомості про расове або етнічне походження, політичні погляди, релігійні переконання, стан здоров'я, біометричні та генетичні дані. Обробка таких даних, як правило, допускається лише за наявності спеціальних правових підстав, оскільки їх розголошення може призвести до суттєвого порушення прав особи [2, с. 61].

Іншим важливим критерієм класифікації є спосіб отримання та обробки персональних даних. За цим критерієм виділяють дані, що надаються особою добровільно, та дані, які збираються автоматично за допомогою інформаційних систем. До останніх належать, зокрема, технічні дані, такі як IP-адреси, дані про місцезнаходження, історія використання інтернет-ресурсів.

У сучасних умовах особливого значення набуває класифікація персональних даних залежно від рівня ризику для прав і свобод особи. Дані, обробка яких може призвести до значних негативних наслідків (наприклад, фінансові дані або медична інформація), потребують більш суворого контролю та захисту.

Також персональні дані можна класифікувати залежно від сфери їх використання. Зокрема, виділяють дані, що використовуються у сфері державного управління, комерційній діяльності, банківській сфері, медицині тощо. Кожна з цих сфер має свої особливості обробки персональних даних та відповідні правові вимоги.

Важливим є також поділ персональних даних на відкриті та конфіденційні. Відкриті дані можуть бути доступними для широкого кола осіб за згодою суб'єкта даних або на підставі закону, тоді як конфіденційні дані підлягають обмеженому доступу та потребують особливого захисту.

Таким чином, класифікація персональних даних дозволяє систематизувати їх різновиди та визначити особливості правового регулювання кожного з них. Вона має важливе значення для забезпечення ефективного захисту персональних даних та запобігання їх незаконному використанню або витоку.

1.2. Витік персональних даних як правове явище

У сучасному цифровому середовищі проблема витоку персональних даних набуває особливої актуальності у зв'язку зі зростанням обсягів інформації, що обробляється в електронній формі. Витік персональних даних розглядається як правове явище, що пов'язане з порушенням встановленого порядку обробки, зберігання та захисту інформації про фізичних осіб.

У законодавстві України відсутнє чітке визначення поняття «витік персональних даних», однак у науковій літературі під ним зазвичай розуміють несанкціоноване розкриття, поширення або доступ до персональних даних, що відбулося внаслідок порушення вимог їх захисту [3, с. 102]. Таке визначення охоплює як умисні дії (наприклад, незаконне передавання інформації третім особам), так і випадкові порушення, пов'язані з технічними або організаційними недоліками.

Однією з ключових характеристик витоку персональних даних є відсутність згоди суб'єкта даних на їх розголошення. Це безпосередньо порушує право особи на приватність та контроль над власною інформацією.

Витік може відбуватися як у межах діяльності державних органів, так і в приватному секторі, зокрема у банківській сфері, електронній комерції, соціальних мережах та інших сферах.

Причини витоку персональних даних є різноманітними та можуть мати як технічний, так і організаційний або людський характер. До основних технічних причин належать недосконалість систем захисту інформації, відсутність належного шифрування даних, використання застарілого програмного забезпечення або наявність вразливостей у системах. Такі фактори створюють умови для несанкціонованого доступу до інформації.

Організаційні причини пов'язані з неналежною організацією процесів обробки та захисту персональних даних. Це може бути відсутність внутрішніх політик безпеки, недостатній контроль за доступом до інформації, а також недотримання встановлених процедур обробки даних.

Особливе значення мають людські фактори, які є однією з найпоширеніших причин витоків. До них належать помилки працівників, недбале поводження з інформацією, а також умисні дії, такі як передача даних третім особам або їх незаконне використання. У деяких випадках витoki можуть бути результатом кібератак, зокрема хакерських зламів, фішингу або інших форм кіберзлочинності [4].

Важливим аспектом є також розвиток цифрових технологій, який, з одного боку, сприяє підвищенню ефективності обробки даних, а з іншого — створює нові ризики для їх безпеки. Зокрема, використання хмарних технологій, великих даних (Big Data) та штучного інтелекту ускладнює контроль за обробкою інформації та підвищує ймовірність її витоку.

Таким чином, витік персональних даних є складним правовим явищем, що виникає внаслідок порушення вимог щодо їх захисту та має різноманітні причини. Його дослідження є необхідним для розробки ефективних механізмів

запобігання таким порушенням та забезпечення належного рівня захисту прав суб'єктів персональних даних.

Витік персональних даних має значні негативні наслідки як для окремої особи, так і для суспільства в цілому. Його вплив виходить за межі індивідуального порушення прав і може створювати серйозні загрози для соціальної стабільності, економічної безпеки та функціонування державних інститутів.

Для фізичної особи витік персональних даних насамперед означає порушення права на приватність. Інформація, яка повинна залишатися конфіденційною, стає доступною стороннім особам, що може призвести до різних форм зловживань. Одним із найбільш поширених наслідків є фінансові втрати, пов'язані з використанням персональних даних для шахрайських операцій, зокрема оформлення кредитів або здійснення незаконних платежів.

Крім того, витік персональних даних може призводити до репутаційних втрат. Розголошення конфіденційної інформації, зокрема даних про стан здоров'я, особисте життя або професійну діяльність, може негативно вплинути на соціальний статус особи, її ділову репутацію та міжособистісні відносини.

Суттєвим є також психологічний аспект наслідків витоку персональних даних. Особа може відчувати втрату контролю над власною інформацією, що викликає стрес, тривожність та інші негативні емоційні стани. Це особливо актуально у випадках масових витоків, коли велика кількість людей одночасно стає жертвами порушення їх прав.

На рівні суспільства витік персональних даних може мати ще більш серйозні наслідки. Він підриває довіру громадян до державних органів та приватних компаній, які здійснюють обробку інформації. У разі регулярних витоків формується недовіра до цифрових сервісів, що може гальмувати розвиток електронного урядування та цифрової економіки.

Важливим є також вплив витоків на інформаційну безпеку держави. У випадках, коли витікають дані, що мають стратегічне значення, це може створювати загрози національній безпеці. Зокрема, персональні дані можуть використовуватися для проведення інформаційних операцій, маніпуляцій або інших форм впливу на суспільство.

Крім того, витік персональних даних може сприяти розвитку кіберзлочинності. Використання отриманої інформації дозволяє зловмисникам здійснювати більш складні та цілеспрямовані атаки, що підвищує рівень загроз у цифровому середовищі.

Таким чином, наслідки витоку персональних даних є багатограними та охоплюють як індивідуальний, так і суспільний рівень. Вони включають фінансові, репутаційні, психологічні та безпекові аспекти, що обумовлює необхідність забезпечення ефективного правового захисту персональних даних та запобігання їх незаконному поширенню.

1.3. Загальні засади юридичної відповідальності у сфері захисту персональних даних

Юридична відповідальність є одним із ключових елементів механізму забезпечення дотримання правових норм у сфері захисту персональних даних. Вона виступає засобом реагування держави на порушення встановлених правил обробки, зберігання та використання інформації про фізичних осіб, а також важливим інструментом захисту прав суб'єктів персональних даних.

У загальнотеоретичному розумінні юридична відповідальність визначається як передбачений нормами права обов'язок правопорушника зазнати негативних наслідків у вигляді певних обмежень або санкцій за вчинене правопорушення [5, с. 211]. У сфері захисту персональних даних така

відповідальність настає у випадках порушення законодавчих вимог щодо обробки інформації, її незаконного поширення або витоку.

Особливістю юридичної відповідальності у цій сфері є її комплексний характер. Порушення законодавства про персональні дані може тягнути за собою застосування різних видів відповідальності залежно від характеру правопорушення, його наслідків та суб'єкта, який його вчинив.

Одним із основних видів є адміністративна відповідальність, яка застосовується за порушення встановленого порядку обробки та захисту персональних даних. Вона передбачає накладення штрафів або інших адміністративних стягнень і є найбільш поширеним видом відповідальності у цій сфері.

Цивільно-правова відповідальність полягає у відшкодуванні шкоди, завданої особі внаслідок незаконного використання або витоку її персональних даних. Така відповідальність має відновлювальний характер і спрямована на компенсацію матеріальних та моральних збитків.

Кримінальна відповідальність застосовується у випадках найбільш серйозних порушень, пов'язаних із незаконним збиранням, використанням або поширенням персональних даних, що завдало значної шкоди або було вчинене з корисливих мотивів. Вона передбачає застосування більш суворих санкцій, включаючи обмеження або позбавлення волі.

Окремо можна виділити дисциплінарну відповідальність, яка застосовується до працівників, що порушили внутрішні правила обробки персональних даних у межах виконання своїх службових обов'язків. Такий вид відповідальності має внутрішньоорганізаційний характер і спрямований на забезпечення належного рівня дисципліни.

Таким чином, юридична відповідальність у сфері захисту персональних даних є багаторівневою системою, що включає різні види санкцій та

механізмів впливу. Її ефективне застосування є необхідною умовою забезпечення належного рівня захисту інформації та прав суб'єктів персональних даних.

Юридична відповідальність у сфері захисту персональних даних ґрунтується на певних принципах, які визначають її зміст, межі та порядок застосування. Ці принципи забезпечують справедливість, ефективність та відповідність правового регулювання вимогам сучасного інформаційного суспільства.

Одним із основних є принцип законності, який передбачає, що відповідальність може наставати лише за ті діяння, які прямо передбачені законом. У сфері персональних даних це означає, що притягнення до відповідальності можливе лише за порушення встановлених норм щодо обробки, зберігання та захисту інформації.

Важливим є принцип вини, відповідно до якого особа підлягає відповідальності лише за наявності її вини у вчиненні правопорушення. У випадку витоку персональних даних це може бути як умисел (наприклад, незаконне передавання інформації), так і необережність (недбале поводження з даними).

Принцип пропорційності передбачає, що застосовані санкції повинні відповідати тяжкості правопорушення та його наслідкам. Це особливо важливо у сфері захисту персональних даних, де необхідно враховувати як обсяг витоку, так і його вплив на права та інтереси особи.

Суттєве значення має принцип невідворотності відповідальності, який означає, що кожне правопорушення повинно отримати належну правову оцінку. Це сприяє запобіганню новим порушенням та підвищує рівень правової дисципліни у сфері обробки персональних даних.

Окремо слід виділити принцип захисту прав суб'єкта персональних даних. Він передбачає, що у разі порушення прав особи держава повинна забезпечити ефективні механізми їх відновлення, включаючи можливість звернення до суду та отримання компенсації завданої шкоди.

Важливим є також принцип превентивності, який спрямований на запобігання правопорушенням у сфері персональних даних. Він передбачає впровадження заходів, спрямованих на мінімізацію ризиків витоку інформації, зокрема встановлення внутрішніх політик безпеки та підвищення рівня обізнаності працівників.

У сучасних умовах дедалі більшого значення набуває принцип підзвітності, який передбачає, що суб'єкти, які здійснюють обробку персональних даних, повинні не лише дотримуватися вимог законодавства, але й бути готовими довести це. Це відповідає сучасним європейським підходам до регулювання у сфері захисту даних.

Таким чином, принципи юридичної відповідальності у сфері захисту персональних даних визначають основні засади її застосування та забезпечують баланс між інтересами особи, суспільства і держави. Їх дотримання є необхідною умовою ефективного функціонування системи правового захисту персональних даних.

РОЗДІЛ 2. ПРАВОВЕ РЕГУЛЮВАННЯ ТА ВИДИ ВІДПОВІДАЛЬНОСТІ ЗА ВИТІК ПЕРСОНАЛЬНИХ ДАНИХ

2.1. Національне законодавство України у сфері захисту персональних даних

Правове регулювання захисту персональних даних в Україні є складною та багаторівневою системою, що охоплює норми різних галузей права. Його основною метою є забезпечення реалізації права людини на приватність, захист інформації про особу та встановлення ефективних механізмів відповідальності за порушення у сфері обробки персональних даних, зокрема у випадках їх витоку.

Базовим нормативно-правовим актом у цій сфері є Закон України «Про захист персональних даних», який визначає правові та організаційні засади захисту інформації про фізичних осіб. Цей закон встановлює основні принципи обробки персональних даних, права суб'єктів даних, обов'язки володільців і розпорядників баз даних, а також вимоги до забезпечення їх захисту [7]. Важливим є те, що закон закріплює обов'язок отримання згоди суб'єкта даних на їх обробку, а також встановлює обмеження щодо використання інформації без належних правових підстав.

Особливу роль у системі правового регулювання відіграє Конституція України, яка гарантує право кожної особи на невтручання в її особисте і сімейне життя. Відповідно до статті 32 Конституції, збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди не допускається, за винятком випадків, передбачених законом. Це положення є фундаментальною основою для формування всієї системи захисту персональних даних.

Важливим елементом національного законодавства є також норми цивільного права, які передбачають можливість захисту особистих

немайнових прав, зокрема права на приватність. У разі порушення цих прав особа має право на відшкодування моральної та матеріальної шкоди, що є важливим механізмом захисту у випадках витоку персональних даних.

Значну роль відіграє адміністративне законодавство, яке встановлює відповідальність за порушення вимог щодо обробки персональних даних. Зокрема, Кодекс України про адміністративні правопорушення передбачає накладення штрафів за недотримання встановлених правил, що сприяє запобіганню правопорушенням у цій сфері.

Кримінальне законодавство також містить норми, спрямовані на захист персональних даних. Зокрема, Кримінальний кодекс України передбачає відповідальність за незаконне збирання, використання або поширення конфіденційної інформації про особу, що може включати випадки витоку персональних даних. Такі правопорушення визнаються суспільно небезпечними, оскільки можуть завдати значної шкоди правам і свободам людини [8].

Окрему увагу слід приділити законодавству у сфері кібербезпеки, яке відіграє важливу роль у запобіганні витокам персональних даних. Закон України «Про основні засади забезпечення кібербезпеки України» встановлює правові та організаційні основи захисту інформації в інформаційно-комунікаційних системах. Він визначає повноваження державних органів у сфері кібербезпеки, а також встановлює вимоги до захисту інформаційних ресурсів від несанкціонованого доступу.

Слід також зазначити, що важливим елементом правового регулювання є підзаконні нормативно-правові акти, які конкретизують вимоги щодо обробки та захисту персональних даних. До них належать постанови Кабінету Міністрів України, накази центральних органів виконавчої влади, а також рекомендації уповноважених органів у сфері захисту персональних даних.

Водночас аналіз національного законодавства свідчить про наявність певних проблем. Зокрема, відсутність чітких механізмів реагування на витоки персональних даних, недостатня деталізація обов'язків суб'єктів обробки інформації, а також обмежена ефективність механізмів контролю ускладнюють забезпечення належного рівня захисту.

Крім того, важливою проблемою є недостатній рівень узгодженості українського законодавства з європейськими стандартами, зокрема з положеннями Загального регламенту захисту даних (GDPR). Це ускладнює інтеграцію України у міжнародний інформаційний простір та знижує ефективність захисту персональних даних у транскордонних правовідносинах.

Таким чином, національне законодавство України у сфері захисту персональних даних є комплексною системою правових норм, що охоплює різні аспекти регулювання інформаційних відносин. Водночас воно потребує подальшого вдосконалення, спрямованого на підвищення ефективності захисту персональних даних та забезпечення належного рівня відповідальності за їх витік.

2.2. Міжнародно-правові стандарти та європейський досвід (GDPR)

У сучасному глобалізованому інформаційному просторі питання захисту персональних даних набуває міжнародного значення, оскільки обробка інформації часто здійснюється поза межами однієї держави. У зв'язку з цим особливу роль відіграють міжнародно-правові стандарти та європейський досвід, які формують сучасні підходи до регулювання захисту персональних даних та відповідальності за їх порушення.

Одним із ключових міжнародних документів у цій сфері є Конвенція Ради Європи № 108 про захист осіб у зв'язку з автоматизованою обробкою

персональних даних. Вона стала першим міжнародним актом, який закріпив основні принципи захисту персональних даних, зокрема законність їх обробки, цільове призначення використання та забезпечення безпеки інформації [10]. Конвенція визначає обов'язки держав щодо створення ефективних механізмів захисту персональних даних та сприяє гармонізації національних законодавств.

Важливе значення має також практика Європейського суду з прав людини, яка розглядає захист персональних даних як складову права на повагу до приватного життя. Відповідно до статті 8 Конвенції про захист прав людини і основоположних свобод, кожна особа має право на захист свого приватного і сімейного життя, що включає контроль над інформацією про себе. Суд неодноразово підкреслював, що обробка персональних даних без належних гарантій може становити порушення цього права.

Найбільш значущим сучасним актом у сфері захисту персональних даних є Загальний регламент Європейського Союзу про захист даних (General Data Protection Regulation — GDPR), який набрав чинності у 2018 році. Цей документ встановлює єдині правила обробки персональних даних на території Європейського Союзу та є одним із найбільш розвинених нормативних актів у світі у цій сфері [11].

GDPR базується на низці ключових принципів, серед яких законність, справедливість і прозорість обробки даних, обмеження мети їх використання, мінімізація обсягу даних, точність, обмеження строків зберігання, а також забезпечення цілісності та конфіденційності інформації. Ці принципи визначають загальні вимоги до обробки персональних даних та є обов'язковими для всіх суб'єктів, які здійснюють таку діяльність.

Особливістю GDPR є також закріплення широкого кола прав суб'єктів персональних даних. До них належать право на доступ до своїх даних, право

на їх виправлення, право на видалення (так зване «право на забуття»), право на обмеження обробки, а також право на перенесення даних. Це значно підвищує рівень захисту прав особи та забезпечує контроль над власною інформацією.

Важливим аспектом GDPR є встановлення суворих вимог до безпеки персональних даних. Суб'єкти, які здійснюють їх обробку, зобов'язані впроваджувати відповідні технічні та організаційні заходи для запобігання несанкціонованому доступу, втраті або витоку інформації. У разі порушення безпеки даних передбачено обов'язок повідомлення відповідних органів та суб'єктів даних.

Особливу увагу в GDPR приділено відповідальності за порушення вимог щодо захисту персональних даних. Регламент передбачає значні штрафи, які можуть досягати мільйонів євро, що стимулює суб'єктів дотримуватися встановлених правил. Такий підхід є важливим інструментом забезпечення ефективності правового регулювання.

Окрім GDPR, у Європейському Союзі діють також інші нормативні акти та рекомендації, спрямовані на забезпечення захисту персональних даних у різних сферах, зокрема в електронних комунікаціях та цифрових послугах. Вони доповнюють загальні положення GDPR та формують комплексну систему правового регулювання.

Європейський досвід характеризується також розвитком інституційних механізмів контролю, зокрема створенням незалежних органів з питань захисту персональних даних. Такі органи здійснюють нагляд за дотриманням законодавства, розглядають скарги та застосовують санкції у разі порушень.

Для України врахування міжнародно-правових стандартів та європейського досвіду має особливе значення у контексті євроінтеграційних процесів. Адаптація національного законодавства до вимог GDPR сприятиме

підвищенню рівня захисту персональних даних, зміцненню довіри до цифрових сервісів та інтеграції України у європейський правовий простір.

Таким чином, міжнародно-правові стандарти та європейський досвід, зокрема GDPR, формують сучасну модель регулювання захисту персональних даних, яка базується на поєднанні високого рівня захисту прав людини та ефективних механізмів відповідальності. Їх впровадження є необхідною умовою розвитку національної системи правового регулювання у цій сфері.

2.3. Види юридичної відповідальності за витік персональних даних

У системі юридичної відповідальності за витік персональних даних адміністративна та цивільно-правова відповідальність займають важливе місце, оскільки саме вони найчастіше застосовуються у практиці реагування на порушення у сфері обробки інформації. Їх призначення полягає як у покаранні правопорушників, так і у відновленні порушених прав суб'єктів персональних даних.

Адміністративна відповідальність є одним із основних інструментів державного впливу у сфері захисту персональних даних. Вона застосовується у випадках порушення встановлених законодавством вимог щодо порядку обробки, зберігання та захисту персональних даних. До таких порушень належать, зокрема, обробка даних без належної згоди суб'єкта, недотримання вимог щодо їх захисту, ненадання доступу до інформації або незаконне поширення персональних даних.

В Україні адміністративна відповідальність у цій сфері передбачена нормами Кодексу України про адміністративні правопорушення. Застосування адміністративних санкцій, зокрема штрафів, має превентивний характер і спрямоване на запобігання новим правопорушенням. Водночас

ефективність такого механізму значною мірою залежить від рівня контролю та практики його застосування [13, с. 142].

Особливістю адміністративної відповідальності є її оперативність та відносна простота застосування. Вона не потребує складних процедур доказування, характерних для кримінального процесу, що дозволяє швидко реагувати на порушення. Однак у багатьох випадках розмір адміністративних санкцій є недостатнім для стримування серйозних правопорушень, особливо з боку великих компаній, які обробляють значні обсяги персональних даних.

Цивільно-правова відповідальність має відновлювальний характер і спрямована на захист прав суб'єктів персональних даних шляхом компенсації завданої шкоди. У випадку витоку персональних даних особа має право вимагати відшкодування як матеріальної, так і моральної шкоди, завданої внаслідок незаконного використання або розголошення інформації.

Правовою основою для застосування цивільно-правової відповідальності є норми Цивільного кодексу України, які передбачають захист особистих немайнових прав, зокрема права на приватність. Витік персональних даних може розглядатися як порушення цього права, що дає підстави для звернення до суду з вимогою про відшкодування шкоди.

Особливістю цивільно-правової відповідальності є необхідність доведення факту шкоди, причинно-наслідкового зв'язку між діями правопорушника та наслідками, а також вини особи, яка допустила порушення. Це може ускладнювати процес захисту прав, особливо у випадках, коли витік даних має масовий характер або здійснюється через складні технічні механізми.

Водночас цивільно-правова відповідальність є важливим механізмом забезпечення справедливості, оскільки дозволяє компенсувати негативні наслідки для постраждалих осіб. Крім того, вона стимулює суб'єктів, які

обробляють персональні дані, до більш відповідального ставлення до забезпечення їх захисту.

Слід зазначити, що у сучасних умовах дедалі більшого значення набуває поєднання адміністративної та цивільно-правової відповідальності. Такий комплексний підхід дозволяє забезпечити як покарання правопорушників, так і відновлення порушених прав, що підвищує ефективність правового регулювання у сфері захисту персональних даних.

Таким чином, адміністративна та цивільно-правова відповідальність є важливими складовими системи юридичної відповідальності за витік персональних даних. Вони забезпечують як превентивний, так і відновлювальний вплив на правопорушників і відіграють ключову роль у захисті прав суб'єктів персональних даних.

Кримінальна відповідальність за витік персональних даних є найбільш суворим видом юридичної відповідальності, що застосовується у випадках вчинення суспільно небезпечних діянь, пов'язаних із незаконним збиранням, використанням, поширенням або іншим неправомірним втручанням у сферу приватного життя особи. Її призначення полягає не лише у покаранні винних осіб, але й у запобіганні подальшим правопорушенням у сфері інформаційних відносин.

В Україні кримінально-правове регулювання відповідальності за порушення у сфері персональних даних здійснюється, зокрема, на підставі статті 182 Кримінального кодексу України, яка передбачає відповідальність за незаконне збирання, зберігання, використання або поширення конфіденційної інформації про особу без її згоди [15]. У контексті витоку персональних даних такі дії можуть кваліфікуватися як кримінальне правопорушення, якщо вони спричинили істотну шкоду правам та інтересам особи.

Особливістю кримінальної відповідальності у цій сфері є необхідність встановлення всіх елементів складу злочину: об'єкта, об'єктивної сторони, суб'єкта та суб'єктивної сторони. Об'єктом посягання виступають суспільні відносини у сфері забезпечення права на приватність та захист персональних даних. Об'єктивна сторона полягає у вчиненні дій, пов'язаних із незаконним доступом до інформації або її поширенням.

Суб'єктом кримінального правопорушення може бути як фізична особа, так і службова особа, яка має доступ до персональних даних у зв'язку з виконанням своїх професійних обов'язків. У випадках, коли витік даних здійснюється посадовими особами, це може розглядатися як обтяжуюча обставина, що впливає на міру покарання.

Суб'єктивна сторона злочину передбачає наявність вини у формі умислу або необережності. У більшості випадків витік персональних даних, що тягне кримінальну відповідальність, має умисний характер, коли особа усвідомлює протиправність своїх дій та бажає або свідомо допускає настання негативних наслідків.

Однією з ключових особливостей застосування кримінальної відповідальності є складність доказування. У випадках витоку персональних даних необхідно встановити факт незаконного доступу або поширення інформації, визначити джерело витоку, а також довести причинно-наслідковий зв'язок між діями правопорушника та завданою шкодою. Це ускладнюється використанням сучасних інформаційних технологій, які дозволяють приховувати сліди правопорушення.

Крім того, важливою проблемою є латентність таких правопорушень. Значна частина випадків витоку персональних даних залишається нерозкритою або не доходить до стадії кримінального провадження. Це

пов'язано як із труднощами виявлення правопорушень, так і з недостатньою обізнаністю громадян щодо своїх прав.

У сучасних умовах особливого значення набуває боротьба з кіберзлочинністю, яка є однією з основних причин витоку персональних даних. Хакерські атаки, фішинг та інші форми незаконного доступу до інформації становлять серйозну загрозу для безпеки персональних даних і потребують ефективного кримінально-правового реагування [16, с. 198].

Слід також зазначити, що кримінальна відповідальність має важливе превентивне значення. Встановлення суворих санкцій за порушення у сфері персональних даних сприяє формуванню відповідального ставлення до обробки інформації та підвищує рівень правової культури у суспільстві.

Таким чином, кримінальна відповідальність є важливим елементом системи захисту персональних даних, який забезпечує реагування на найбільш небезпечні правопорушення у цій сфері. Водночас ефективність її застосування залежить від удосконалення законодавства, розвитку практики правозастосування та підвищення рівня кібербезпеки.

РОЗДІЛ 3. ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ ВДОСКОНАЛЕННЯ ВІДПОВІДАЛЬНОСТІ ЗА ВИТІК ПЕРСОНАЛЬНИХ ДАНИХ

3.1. Актуальні проблеми притягнення до відповідальності за витік персональних даних

Однією з ключових проблем у сфері притягнення до відповідальності за витік персональних даних є складність виявлення самих фактів правопорушення. У сучасному цифровому середовищі значна частина процесів обробки інформації здійснюється автоматизовано, що ускладнює контроль за рухом даних та своєчасне встановлення факту їх несанкціонованого поширення.

Витік персональних даних часто має прихований характер і може залишатися непоміченим тривалий час. У багатьох випадках особи дізнаються про порушення лише після настання негативних наслідків, таких як шахрайські дії, несанкціоноване використання банківських рахунків або поширення конфіденційної інформації. Це значно ускладнює процес фіксації правопорушення та збирання доказів.

Суттєвою проблемою є також складність встановлення джерела витоку. У випадках, коли персональні дані обробляються кількома суб'єктами або передаються між різними інформаційними системами, визначити, на якому етапі відбулося порушення, є вкрай складно. Це особливо актуально для великих організацій та цифрових платформ, де обробка даних має багаторівневий характер [17, с. 133].

Ще одним важливим аспектом є технічна складність доказування. Для встановлення факту витоку персональних даних часто необхідні спеціальні знання у сфері інформаційних технологій, кібербезпеки та цифрової криміналістики. Це потребує залучення експертів, що ускладнює та подовжує процес розгляду справ.

Крім того, доказування у таких справах ускладнюється можливістю видалення або зміни цифрових слідів. Персональні дані можуть бути швидко скопійовані, передані або знищені, що робить їх фіксацію проблематичною. У багатьох випадках відсутність належної системи логування та збереження даних ускладнює встановлення обставин правопорушення.

Важливою проблемою є також транскордонний характер витоків персональних даних. У випадках, коли дані обробляються або зберігаються за межами України, виникають труднощі із застосуванням національного законодавства та отриманням доказів від іноземних суб'єктів.

Таким чином, проблеми виявлення та доказування витоків персональних даних мають комплексний характер і пов'язані як із технічними, так і з правовими аспектами. Їх вирішення потребує вдосконалення механізмів контролю, розвитку експертної бази та впровадження сучасних технологій кібербезпеки.

Ще однією важливою проблемою у сфері притягнення до відповідальності за витік персональних даних є недосконалість правозастосовної практики. Незважаючи на наявність нормативно-правової бази, ефективність її реалізації залишається недостатньою, що знижує рівень захисту персональних даних.

Однією з основних причин є недостатній рівень спеціалізації органів, які здійснюють контроль та розгляд справ у цій сфері. Відсутність достатнього досвіду та знань у сфері інформаційних технологій ускладнює правильну кваліфікацію правопорушень та застосування відповідних норм законодавства.

Крім того, існує проблема фрагментарності правового регулювання. Норми, що стосуються відповідальності за витік персональних даних, містяться у різних нормативно-правових актах, що ускладнює їх застосування

на практиці. Це призводить до неоднозначності у тлумаченні законодавства та формування різної судової практики.

Суттєвою проблемою є також низька ефективність санкцій. Адміністративні штрафи, передбачені законодавством України, часто є недостатніми для стримування порушень, особливо з боку великих компаній. У порівнянні з європейськими стандартами, де передбачені значні фінансові санкції, українські механізми відповідальності виглядають менш ефективними [18, с. 215].

Ще одним аспектом є складність притягнення до кримінальної відповідальності. Як правило, такі справи потребують значного обсягу доказів, що ускладнює їх доведення та знижує кількість випадків притягнення винних осіб до відповідальності.

Важливим фактором є також низький рівень правової культури як серед суб'єктів, що обробляють персональні дані, так і серед самих громадян. Багато осіб не усвідомлюють значення захисту персональних даних та не звертаються за захистом своїх прав у випадку їх порушення.

Крім того, недостатній рівень контролю з боку державних органів сприяє збереженню високого рівня правопорушень у цій сфері. Відсутність системного моніторингу та ефективних механізмів реагування на витоки персональних даних знижує загальний рівень правової дисципліни.

Таким чином, недосконалість правозастосовної практики та низька ефективність санкцій є суттєвими проблемами у сфері притягнення до відповідальності за витік персональних даних. Їх вирішення потребує комплексного підходу, що включає вдосконалення законодавства, підвищення рівня спеціалізації правозастосовних органів та посилення відповідальності за порушення.

3.2. Захист прав суб'єктів персональних даних та механізми їх реалізації

Захист персональних даних є невід'ємною складовою забезпечення прав і свобод людини у сучасному інформаційному суспільстві. Особливе значення у цій сфері мають права суб'єктів персональних даних, які забезпечують можливість особи контролювати обробку інформації про себе та захищати свої інтереси у разі їх порушення.

Відповідно до законодавства України, суб'єкт персональних даних наділений широким колом прав, спрямованих на забезпечення прозорості та законності обробки інформації. До основних прав належить право знати про джерела збирання своїх персональних даних, мету їх обробки та місцезнаходження бази даних. Це право забезпечує можливість особи усвідомлювати, як саме використовується інформація про неї.

Важливим є право доступу до персональних даних, яке дозволяє суб'єкту отримувати інформацію про наявність та зміст своїх даних, що обробляються відповідними суб'єктами. Реалізація цього права є ключовою умовою ефективного контролю за обробкою персональних даних.

Суттєве значення має право на виправлення або оновлення персональних даних. У разі виявлення неточностей або застарілої інформації особа має право вимагати їх зміни або доповнення. Це сприяє забезпеченню достовірності даних та запобігає негативним наслідкам, пов'язаним із використанням неправдивої інформації.

Окрему роль відіграє право на заперечення проти обробки персональних даних, яке дозволяє особі обмежити або заборонити використання інформації у певних випадках. Також важливим є право вимагати припинення обробки даних та їх видалення, особливо у випадках, коли така обробка здійснюється без законних підстав.

Крім того, суб'єкт персональних даних має право на захист своїх прав у разі їх порушення. Це включає можливість звернення до суду, уповноважених державних органів або інших інституцій, які здійснюють контроль у сфері захисту персональних даних.

Способи захисту прав суб'єктів персональних даних можна умовно поділити на юрисдикційні та неюрисдикційні. До юрисдикційних належать судовий захист, який передбачає можливість подання позову про відшкодування шкоди, а також звернення до органів державної влади, уповноважених здійснювати контроль за дотриманням законодавства.

Неюрисдикційні способи захисту включають звернення безпосередньо до володільця персональних даних із вимогою усунути порушення, а також використання внутрішніх механізмів контролю, що діють у відповідних організаціях. Такий підхід дозволяє вирішити проблему на ранніх етапах без звернення до суду.

Важливим є також використання превентивних заходів, спрямованих на запобігання порушенням. До них належать підвищення обізнаності громадян щодо своїх прав, використання засобів захисту інформації, а також контроль за наданням персональних даних третім особам.

Таким чином, права суб'єктів персональних даних є основою системи їх правового захисту, а ефективність їх реалізації залежить від наявності дієвих механізмів захисту. Забезпечення належного рівня захисту цих прав є важливою умовою функціонування сучасного інформаційного суспільства.

У разі витоку персональних даних особа має право на ефективний захист своїх прав і законних інтересів. Такий захист може здійснюватися як у судовому, так і в позасудовому порядку, що забезпечує можливість вибору найбільш доцільного механізму залежно від характеру порушення та його наслідків.

Судовий захист є одним із найбільш ефективних способів відновлення порушених прав суб'єктів персональних даних. Він передбачає звернення до суду з позовом про захист особистих немайнових прав, відшкодування матеріальної та моральної шкоди, а також припинення незаконних дій, пов'язаних із обробкою або поширенням персональних даних.

У межах судового розгляду особа може вимагати визнання факту порушення її прав, зобов'язання відповідача припинити незаконну обробку даних, а також відшкодування завданих збитків. Судовий захист забезпечує офіційне встановлення правопорушення та застосування відповідних правових наслідків.

Разом із тим судовий механізм має певні недоліки, зокрема тривалість розгляду справ, складність доказування та необхідність залучення спеціальних знань у сфері інформаційних технологій. Це може ускладнювати доступ до правосуддя для окремих осіб.

Позасудовий захист прав суб'єктів персональних даних є альтернативним та більш оперативним механізмом реагування на порушення. Він включає звернення до органів державної влади, уповноважених здійснювати контроль у сфері захисту персональних даних, зокрема до Уповноваженого Верховної Ради України з прав людини. Такий орган має право розглядати скарги, проводити перевірки та вживати заходів реагування у разі виявлення порушень.

Крім того, позасудовий захист може здійснюватися шляхом звернення безпосередньо до володільця або розпорядника персональних даних із вимогою усунути порушення. У багатьох випадках це дозволяє вирішити проблему без застосування складних юридичних процедур.

Важливим елементом позасудового захисту є також механізми внутрішнього контролю в організаціях, що обробляють персональні дані.

Наявність відповідних політик, процедур реагування на інциденти та відповідальних осіб сприяє оперативному виявленню та усуненню порушень.

У сучасних умовах дедалі більшого значення набувають альтернативні способи вирішення спорів, зокрема медіація. Вона дозволяє сторонам досягти компромісу без звернення до суду, що сприяє зменшенню навантаження на судову систему та підвищенню ефективності захисту прав.

Таким чином, судовий та позасудовий захист прав суб'єктів персональних даних є взаємодоповнюючими механізмами, які забезпечують можливість ефективного реагування на витік персональних даних. Вибір конкретного способу захисту залежить від обставин справи, характеру порушення та бажаного результату.

3.3. Напрями вдосконалення законодавства та практики застосування відповідальності

У сучасних умовах інтеграції України до європейського правового простору особливого значення набуває гармонізація національного законодавства у сфері захисту персональних даних із міжнародними та європейськими стандартами. Одним із ключових орієнтирів у цьому процесі є Загальний регламент Європейського Союзу про захист даних (GDPR), який встановлює високі вимоги до обробки персональних даних та відповідальності за їх порушення.

Чинне законодавство України, незважаючи на наявність базових норм у сфері захисту персональних даних, не повною мірою відповідає сучасним європейським стандартам. Зокрема, потребує вдосконалення система прав суб'єктів персональних даних, яка в Україні є менш деталізованою порівняно з GDPR. У європейському праві передбачено широкий спектр прав,

включаючи право на забуття, право на перенесення даних, а також право на обмеження їх обробки.

Важливим напрямом гармонізації є також запровадження принципу підзвітності (accountability), який передбачає, що суб'єкти, які обробляють персональні дані, повинні не лише дотримуватися законодавства, але й мати можливість довести це. В Україні цей принцип ще не отримав належного нормативного закріплення та практичного застосування.

Крім того, необхідним є вдосконалення вимог до безпеки персональних даних. GDPR передбачає обов'язок впровадження технічних та організаційних заходів захисту, а також обов'язкове повідомлення про порушення безпеки даних (data breach notification). У національному законодавстві такі механізми потребують більш чіткого регулювання [21, с. 178].

Суттєвим аспектом є також посилення відповідальності за порушення законодавства про захист персональних даних. У країнах Європейського Союзу передбачені значні штрафи, які стимулюють суб'єктів дотримуватися встановлених правил. В Україні ж рівень санкцій залишається відносно низьким, що знижує їх стримуючий ефект.

Гармонізація законодавства також передбачає розвиток інституційної спроможності органів, що здійснюють контроль у сфері захисту персональних даних. Це включає підвищення їх незалежності, розширення повноважень та забезпечення належного рівня ресурсного забезпечення.

Таким чином, гармонізація національного законодавства з європейськими стандартами є необхідною умовою підвищення ефективності правового регулювання у сфері захисту персональних даних. Вона сприятиме не лише покращенню рівня захисту прав громадян, але й інтеграції України у європейський правовий простір.

Одним із ключових напрямів вдосконалення системи захисту персональних даних є розвиток ефективних механізмів контролю та підвищення рівня юридичної відповідальності за їх порушення. Без належного контролю навіть найбільш досконале законодавство не забезпечує реального захисту прав суб'єктів персональних даних.

Важливим кроком у цьому напрямі є посилення ролі уповноважених органів, які здійснюють нагляд у сфері захисту персональних даних. Необхідно забезпечити їхню незалежність, підвищити рівень професійної підготовки працівників та розширити їх повноваження щодо проведення перевірок і застосування санкцій.

Суттєвим є також впровадження системного підходу до контролю, який передбачає регулярний моніторинг діяльності суб'єктів, що обробляють персональні дані. Це дозволить своєчасно виявляти порушення та запобігати витокам інформації.

Одним із перспективних напрямів є запровадження обов'язкових внутрішніх механізмів контролю в організаціях, таких як політики захисту персональних даних, аудит безпеки та призначення відповідальних осіб (Data Protection Officer). Це відповідає сучасним міжнародним стандартам і сприяє підвищенню рівня відповідальності суб'єктів обробки даних.

Важливим є також удосконалення системи санкцій. Підвищення розміру штрафів та їх диференціація залежно від тяжкості правопорушення сприятиме підвищенню ефективності відповідальності. Крім того, доцільним є запровадження додаткових заходів впливу, таких як обмеження діяльності або тимчасове припинення обробки персональних даних.

Слід також звернути увагу на необхідність розвитку судової практики у цій сфері. Формування сталої судової практики сприятиме однаковому застосуванню законодавства та підвищенню правової визначеності.

Важливим напрямом є підвищення рівня правової обізнаності населення. Інформування громадян про їхні права та механізми їх захисту сприятиме більш активному використанню правових інструментів та підвищенню загального рівня захисту персональних даних.

Крім того, необхідним є розвиток міжнародного співробітництва у сфері боротьби з витоками персональних даних. Обмін інформацією, спільні розслідування та координація дій між державами дозволять ефективніше реагувати на транскордонні правопорушення.

Таким чином, удосконалення механізмів контролю та підвищення ефективності відповідальності є комплексним процесом, який потребує поєднання правових, організаційних та технічних заходів. Реалізація цих напрямів сприятиме підвищенню рівня захисту персональних даних та ефективності правового регулювання у цій сфері.

ВИСНОВКИ

У результаті проведеного дослідження теми відповідальності за витік персональних даних було всебічно проаналізовано теоретико-правові засади, нормативне регулювання, а також проблеми та перспективи розвитку цієї сфери. Отримані результати дозволяють сформулювати низку узагальнюючих висновків.

По-перше, встановлено, що персональні дані є особливим об'єктом правового регулювання, який безпосередньо пов'язаний із реалізацією фундаментальних прав людини, насамперед права на приватність. У сучасному інформаційному суспільстві вони набувають значної цінності, що обумовлює необхідність їх належного правового захисту. Персональні дані охоплюють широкий спектр інформації, яка дозволяє ідентифікувати особу, а їх обробка потребує дотримання чітко визначених правових вимог.

По-друге, витік персональних даних було охарактеризовано як складне правове явище, що виникає внаслідок порушення встановлених правил обробки та захисту інформації. Основними причинами витоків є технічні недоліки систем захисту, організаційні помилки, а також людський фактор і кіберзлочинність. Наслідки таких витоків мають багатовимірний характер і включають фінансові, репутаційні та психологічні втрати для особи, а також негативний вплив на рівень довіри до державних інституцій та цифрових сервісів.

По-третє, встановлено, що система юридичної відповідальності за витік персональних даних має комплексний характер і включає адміністративну, цивільно-правову, кримінальну та дисциплінарну відповідальність. Кожен із цих видів відповідальності виконує свою функцію: адміністративна — превентивну, цивільно-правова — відновлювальну, кримінальна — каральну

та стримуючу. Водночас ефективність цієї системи залежить від узгодженості її елементів та практики їх застосування.

По-четверте, аналіз національного законодавства України показав, що воно формує базові правові засади захисту персональних даних, однак не повною мірою відповідає сучасним викликам цифрового середовища. Наявність норм у різних галузях права забезпечує комплексний підхід до регулювання, проте їх фрагментарність та недостатня деталізація ускладнюють ефективне правозастосування.

По-п'яте, дослідження міжнародно-правових стандартів та європейського досвіду, зокрема положень GDPR, дозволило встановити, що сучасна модель регулювання захисту персональних даних базується на принципах прозорості, підзвітності, безпеки та пріоритету прав суб'єкта даних. Європейський підхід передбачає високий рівень відповідальності суб'єктів обробки даних та ефективні механізми контролю, що значно підвищує рівень захисту персональних даних.

По-шосте, у ході дослідження було виявлено низку актуальних проблем у сфері притягнення до відповідальності за витік персональних даних. До них належать складність виявлення та доказування правопорушень, недосконалість правозастосовної практики, низька ефективність санкцій, а також недостатній рівень правової обізнаності населення. Ці проблеми суттєво знижують ефективність існуючих механізмів захисту.

По-сьоме, встановлено, що важливу роль у забезпеченні захисту персональних даних відіграють права суб'єктів даних та механізми їх реалізації. Судовий та позасудовий захист є взаємодоповнюючими інструментами, які дозволяють ефективно реагувати на порушення. Водночас доступ до цих механізмів потребує спрощення, а їх ефективність — підвищення.

По-восьме, обґрунтовано, що вдосконалення системи відповідальності за витік персональних даних має здійснюватися шляхом гармонізації національного законодавства з європейськими стандартами, зокрема GDPR. Це передбачає розширення прав суб'єктів даних, впровадження принципу підзвітності, посилення вимог до безпеки інформації та підвищення рівня санкцій.

По-дев'яте, визначено, що підвищення ефективності правового регулювання можливе за умови розвитку механізмів контролю, зокрема шляхом посилення ролі уповноважених органів, впровадження внутрішніх систем захисту даних у організаціях та підвищення рівня кібербезпеки. Важливим є також розвиток міжнародного співробітництва у сфері протидії витокам персональних даних.

Таким чином, проблема відповідальності за витік персональних даних є складною та багатогранною, що потребує комплексного підходу до її вирішення. Забезпечення ефективного захисту персональних даних можливе лише за умови поєднання сучасного законодавства, ефективної правозастосовної практики та високого рівня правової культури суспільства.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17> (дата звернення: 01.03.2026).
2. Дзюбань О. П. Інформаційне право: сучасні виклики та перспективи розвитку: монографія. Харків: Право, 2021. 360 с.
3. Костецька Т. А. Інформаційна безпека в умовах цифрового суспільства: правові аспекти: монографія. Київ: Юридична думка, 2021. 320 с.
4. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19> (дата звернення: 01.03.2026).
5. Скаун О. Ф. Теорія права і держави: підручник. 4-те вид. Київ: Алерта, 2021. 528 с.
6. Рабінович П. М. Основи загальної теорії права та держави: навч. посіб. Львів: Край, 2020. 256 с.
7. Кобець М. В. Захист персональних даних в Україні: правові засади та практика застосування: монографія. Київ: Юрінком Інтер, 2021. 280 с.
8. Кримінальний кодекс України від 05.04.2001 № 2341-III. URL: <https://zakon.rada.gov.ua/laws/show/2341-14> (дата звернення: 02.03.2026).
9. Кодекс України про адміністративні правопорушення від 07.12.1984 № 8073-X. URL: <https://zakon.rada.gov.ua/laws/show/80731-10> (дата звернення: 03.03.2026).
10. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108). URL: <https://www.coe.int/en/web/data-protection/convention108-and-protocol> (дата звернення: 04.03.2026).

11. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj> (дата звернення: 05.03.2026).
12. Kuner C. European Data Protection Law: Corporate Compliance and Regulation. Oxford: Oxford University Press, 2020. 504 p.
13. Харитонов Є. О., Харитонova О. І. Цивільне право України: підручник. Одеса: Юридична література, 2021. 512 с.
14. Гаврилюк Р. О. Адміністративно-правова відповідальність у сфері інформаційних відносин: монографія. Київ: Алерта, 2020. 280 с.
15. Кримінальне право України. Особлива частина: підручник / за ред. В. Я. Тація. Харків: Право, 2021. 768 с.
16. Баранов О. А. Інформаційне право України: проблеми теорії та практики. Київ: Юрінком Інтер, 2020. 360 с.
17. Пилипчук В. Г. Правові засади інформаційної безпеки в Україні: монографія. Київ: Наукова думка, 2021. 340 с.
18. Кушнір І. В. Захист персональних даних в Україні: проблеми та перспективи: монографія. Львів: ЛНУ ім. І. Франка, 2022. 280 с.
19. Конституція України від 28.06.1996 № 254к/96-ВР. URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80> (дата звернення: 07.03.2026).
20. Цивільний кодекс України від 16.01.2003 № 435-IV. URL: <https://zakon.rada.gov.ua/laws/show/435-15> (дата звернення: 08.03.2026).
21. Головка Л. В. Європейські стандарти захисту персональних даних: монографія. Київ: Юридична думка, 2022. 300 с.
22. Брижко В. М. Захист персональних даних: теорія і практика: монографія. Київ: Юрінком Інтер, 2021. 280 с.