

УДК 351.861:004.6.056.5; 342.7

DOI <https://doi.org/10.24144/2788-6018.2025.06.2.69>

АКТУАЛЬНІ ПРОБЛЕМИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ЯК НАПРЯМУ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ В УМОВАХ ВІЙНИ

Пальчик М.Л.,

*кандидат юридичних наук,
доцент кафедри цивільно-правових дисциплін
Національної академії Служби безпеки України,
ORCID: 0000-0003-3639-0488
e-mail: lawstudies.ua@gmail.com*

Шкрібляк К.П.,

*кандидатка юридичних наук,
доцентка кафедри цивільно-правових дисциплін
Національної академії Служби безпеки України,
ORCID: 0000-0001-5486-788X
e-mail: notar5888@gmail.com*

Берездецький Ю.М.

*старший викладач кафедри цивільно-правових дисциплін
Національної академії Служби безпеки України,
ORCID: 0009-0009-6980-9856
e-mail: kcpd.ss@gmail.com*

Пальчик М.Л., Шкрібляк К.П., Берездецький Ю.М. Актуальні проблеми захисту персональних даних як напряму забезпечення національної безпеки України в умовах війни.

Вказується, воєнний стан в Україні змінив звичайний правовий режим суспільного життя, зокрема він вплинув і на захист персональних даних, перетворивши його на один із ключових елементів національної безпеки. Стаття присвячена дослідженню проблемних питань захисту персональних даних як напрямку забезпечення національної безпеки в умовах війни на прикладі законодавства України. Передумовою дослідження стали нові виклики, пов'язані з війною, зокрема активізація кібератак на державні реєстри та інформаційні системи, що підкреслює стратегічне значення захисту персональних даних. Метою дослідження є визначення особливостей досвіду України у сфері правового та безпекового захисту персональних даних в умовах війни.

Отримані результати свідчать, що українське законодавство окреслює персональні дані у загальних рисах, акцентуючи на можливості ідентифікації особи, тоді як європейський підхід вирізняється вищим рівнем нормативної деталізації. Сформульовано основні ознаки персональних даних та здійснено аналіз особливостей їх правового режиму в умовах мирного часу та під час війни.

Авторами підкреслено, що в Україні надзвичайний правовий режим захисту персональних даних офіційно не запроваджений, що створює ризики для інформаційної безпеки. Дослідницький внесок статті полягає у визначенні ознак надзвичайного правового режиму захисту даних та обґрунтуванні його значення для забезпечення національної безпеки. Межі дослідження зумовлені переважною орієнтацією на український досвід і законодавство, що потребує швидкого реагування та адаптації до міжнародних стандартів. Автори роблять висновок, що умови воєнного стану посилюють потребу у застосуванні спеціальних технічних і правових механізмів захисту персональних даних, оскільки стандартні політики конфіденційності, характерні для звичайного режиму функціонування цифрових сервісів, не забезпечують належного рівня безпеки в умовах надзвичайного чи воєнного стану. Тому практичні й соціальні наслідки дослідження пов'язані з можливістю вдосконалення національного законодавства, підвищення ефективності державної політики у сфері кібербезпеки та забезпечення прав людини в умовах надзвичайних ситуацій.

Ключові слова: персональні дані, національне законодавство, захист інформації, інформаційна безпека, забезпечення прав, національна безпека, війна.

Palchyk M.L., Shkriblyak K.P., Berezdetsky Y.M. Current problems of the protection of personal data as a direction of ensuring guarantee of the national security of Ukraine in wartime.

It is indicated that martial law in Ukraine has changed the usual legal regime of public life, in particular, it has affected the protection of personal data, turning it into one of the key elements of national security. The article is devoted to the study of problematic issues of personal data protection as a direction of ensuring national security in wartime using the example of Ukrainian legislation. The premise of the study was new challenges associated with the war, in particular, the intensification of cyberattacks on state registers and information systems, which emphasizes the strategic importance of personal data protection. The purpose of the study is to determine the features of Ukraine's experience in the field of legal and security protection of personal data in wartime.

The obtained results indicate that Ukrainian legislation outlines personal data in general terms, emphasising the possibility of identifying an individual, whereas the European approach is characterised by a higher level of regulatory detail. The main features of personal data have been formulated, and an analysis of the specifics of their legal regime during peacetime and wartime has been carried out.

The authors emphasize that in Ukraine the emergency legal regime for the protection of personal data has not been officially introduced, which creates risks for information security. The research contribution of the article is to identify the features of the emergency legal regime for data protection and to substantiate its importance for ensuring national security. The limits of the study are determined by the predominant orientation to the Ukrainian experience and legislation, which requires a quick response and adaptation to international standards. The authors conclude that martial law conditions increase the need for special technical and legal mechanisms to protect personal data, as standard privacy policies typical for the normal functioning of digital services do not provide an adequate level of security in a state of emergency or martial law. The practical and social consequences of the study are related to the possibility of improving national legislation, increasing the effectiveness of state policy in the field of cybersecurity and ensuring human rights in emergency situations.

Key words: personal data, national legislation, information protection, information security, security of rights, national security, war.

Постановка проблеми. Стратегією інформаційної безпеки, що затверджена Указом Президента України від 28 грудня 2021 року № 685/2021 визначено актуальні виклики та загрози національній безпеці України в інформаційній сфері, а також стратегічні цілі та завдання, що спрямовані на протидію таким загрозам, захист прав осіб на інформацію та захист персональних даних [1]. Воєнний стан в Україні змінив звичайний правовий режим суспільного життя, зокрема він вплинув і на захист персональних даних, перетворивши його на один із ключових елементів національної безпеки. В умовах війни поширились кібератаки, які були безпосередньо пов'язані з атаками на державні реєстри, що містять персональні дані. Досвід України щодо захисту персональних даних в умовах війни підкреслює, що ця проблема має комплексний і системний характер. Виявилося, що важливим аспектом є як міжвідомча координація між Держспецзв'язку, Службою безпеки України, Міністерством юстиції України, так і міжнародна співпраця щодо обміну досвідом захисту персональних даних та отримання новітніх інноваційних технологій у сфері захисту даних. Водночас війна актуалізувала потребу у швидкому реагуванні та адаптації національної правової системи до міжнародних стандартів, зокрема, Загальної декларації прав людини [2], Конвенції про захист прав людини і основоположних свобод [3], Міжнародного пакту про громадянські і політичні права [4], Загального регламенту ЄС про захист даних (GDPR) [5] та Конвенції ЄС про захист осіб у зв'язку з автоматизованою обробкою персональних даних [6], які встановлюють комплексні вимоги до обробки та захисту персональної інформації.

В Україні досвід спеціальної правової регламентації персональних даних було започатковано лише у 2010 році з моменту прийняття Закону України «Про захист персональних даних», який був спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя у зв'язку з обробкою персональних даних [7]. Водночас, необхідно зазначити, що загальні положення права фізичної особи на недоторканість приватного та сімейного життя, а також підстави можливого правомірного втручання в особисте та сімейне життя особи закріплені в Конституції України, зокрема в ст. 32.

Правомірність втручання в конституційне право особи на недоторканність особистого і сімейного життя обґрунтована у низці рішень Конституційного Суду України. Так, у *Рішенні від 20 січня 2012 року N 2-рп/2012* встановлено, що «право на приватне та сімейне життя є засадничою цінністю, необхідною для повного розквіту людини в демократичному суспільстві, та розглядається як право фізичної особи на автономне буття незалежно від держави, органів місцевого самоврядуван-

ня, юридичних і фізичних осіб», а також, що «збирання, зберігання, використання та поширення державою, органами місцевого самоврядування, юридичними або фізичними особами конфіденційної інформації про особу без її згоди є втручанням в її особисте та сімейне життя, яке допускається винятково у визначених законом випадках і лише в інтересах національної безпеки, економічного добробуту та прав людини» [8].

Втручання у конституційне право особи на приватне і сімейне життя шляхом збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди допускається, якщо воно передбачене законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини, про це констатовано у Рішенні Конституційного Суду від 11 жовтня 2018 року N 7-р/2018 [9]. Поряд з тим, «обмеження щодо реалізації конституційних прав і свобод не можуть бути свавільними та несправедливими, їх установлюють виключно і закони України, вони мають відповідати правомірній меті, бути обумовлені суспільною потребою досягнення цієї мети, домірними. У разі обмеження конституційного права (свободи) законодавець зобов'язаний запровадити таке нормативне регулювання, яке уможливить оптимальне досягнення правомірної мети з мінімальним втручанням у реалізацію цього права (свободи) і не порушуватиме сутності такого права» Рішення від 22 березня 2023 року № 3-р(II)/2023 [10].

В умовах повномасштабного вторгнення проблематика захисту персональних даних набуває не лише правового, а й стратегічного значення задля забезпечення національної безпеки. Така ситуація зумовлена тим, що сучасні війни мають гібридний характер, зокрема й у кіберпросторі. Досвід України це підтверджує. Тому захист персональних даних як єдиної системи є частиною стратегії національної безпеки, що полягає у недопущенні використання конфіденційної інформації для підризу обороноздатності, стабільності державних інституцій та громадського порядку. Наведене вказує на необхідність розмежування та розроблення правової регламентації режиму захисту персональних даних як за звичайних умов життя суспільства, так і під час дії режиму воєнного стану. При цьому важливим є збереження балансу між ефективними заходами безпеки та дотриманням прав людини. Варто звернути увагу, що в умовах воєнного стану законодавством було допущено обмеження прав людини. Незважаючи на це, захист персональних даних громадян в Україні лише посилюється. Таким чином, в Україні фактично сформувався певний феномен у цій сфері, що є предметом окремого наукового дослідження. Вивчення цього явища дозволить сформулювати нові підходи до досягнення балансу між потребами у захисті національної безпеки та правами людини.

Аналіз останніх досліджень і публікацій. Захист персональних даних є комплексною науковою проблемою, вивченню якої приділяють увагу науковці юридичної науки. Так, особливості правового забезпечення захисту персональних даних у цивільних правовідносинах крізь призму практики європейського суду з прав людини досліджувала О.А. Тимошенко. На її думку, захист персональних даних в умовах воєнного стану в Україні має низку особливостей, зумовлених легальною можливістю обмеження конституційних прав і свобод, а також специфічними умовами здійснення такого захисту (активні бойові дії, регулярні кібератаки ворога, перебування громадян на тимчасово окупованій території тощо) [11, с. 170]. Окремого значення набувають підходи Полонської О.І., яка у своїй праці досліджувала правову регламентацію правомірного обмеження права на недоторканність приватного життя в умовах правового режиму воєнного стану [12, с. 323].

Особливості захисту персональних даних в Інтернеті досліджувала Т.П. Попович. Вчена зазначає, що право на захист персональних даних в Інтернеті є однією з сучасних форм реалізації права особи на повагу до її приватного та сімейного життя, його недоторканності у віртуальній сфері реальності, що забезпечується фактором невтручання в індивідуальний інформаційний простір особи [13, с. 54].

Захист персональних даних працівників був предметом дослідження А. С. Михайлика [14] та авторів даної публікації [15]. Сучасну проблематику захисту персональних даних розглядали Г. Спіцина та С. Гуцу у контексті захисту даних працівників під час відеоспостереження на робочому місці [16, с. 176]. Зокрема вчені зазначали, що права роботодавців на управління, підпорядкованість працівників і раціональне використання персональної інформації створюють багато перешкод для захисту працівниками власних законних інтересів та особистої інформації.

В.М. Брижко та В.Г. Пилипчук, досліджуючи приватність, конфіденційність та безпеку персональних даних стверджують, що баланс між безпекою та приватністю персональних даних є складним питанням, яке в епоху інформатизації не може вирішуватися політиками, юристами, технічними фахівцями або спецслужбами на підставі поглядів минулого часу [17, с. 54].

У роботі В.М. Кірієнко акцентовано увагу на захисті персональних даних в умовах війни, зокрема військовослужбовців. Зокрема зазначено, що під час дії правового режиму воєнного стану зростають загрози національній безпеці в інформаційній сфері, а тому забезпечення захисту персональних даних військовослужбовців та працівників оборонного сектору є важливим завданням, з метою унеможливлення їх витоку [18, с. 399].

Захист персональних даних в умовах воєнного стану в Україні вивчав також В.А. Світличний, який наголошував, що освіта користувачів щодо можливих загроз та підготовка до них є вирішальним фактором для зменшення ризику злочинних втручань. Ба більше, на думку науковця ключові засоби захисту персональних даних в умовах воєнного стану включають у себе фізичний захист об'єктів інформаційної інфраструктури, захист інформаційних систем і мереж, кібербезпеку та криптографічний захист даних, а також екстрені процедури реагування на інциденти [19].

Дослідження питань захисту персональних даних в умовах забезпечення національної безпеки, на думку Б. Фасія свідчить, що ці два аспекти не тільки тісно взаємопов'язані, але й потребують комплексного підходу для ефективного вирішення сучасних викликів. Водночас у своїй роботі науковець розглядає проблеми захисту персональних даних здебільшого крізь призму кібербезпеки та відповідних методів захисту персональних даних, таких як шифрування даних, багатофакторна автентифікація, регулярні кібербезпекові аудити та сертифікації, машинне навчання та штучний інтелект для моніторингу безпеки [20, с. 80].

Наведений літературний огляд дає підстави стверджувати, що захист персональних даних є актуальною проблематикою, яка викликає значний науковий інтерес, зокрема у контексті визначення правового режиму їхнього захисту в різних сферах суспільного життя. В Україні сформувався певний правовий прецедент щодо захисту персональних даних в умовах війни, досвід якого може становити цінність для міжнародної правничої спільноти. Саме тому зазначена тематика є важливою та потребує окремого ґрунтовного дослідження.

Метою статті є визначення особливостей досвіду захисту персональних даних громадян України в умовах війни у правовому та безпековому вимірах.

Виклад основного матеріалу. В умовах воєнного стану ідентифікація особи та збір, обробка персональних даних можуть мати певні особливості. Зокрема, в Україні у 2022 р. було створено Єдиний реєстр осіб, зниклих безвісти за особливих обставин. Реєстр створюється за допомогою засобів центральної підсистеми Єдиної інформаційної системи Міністерства внутрішніх справ України та містить відомості про зниклих безвісти, зокрема: їхні персональні дані, дату та обставини зникнення, дані про реєстрацію заяви, результати встановлення місця перебування чи поховання, інформацію про кримінальне провадження (номер, кваліфікація, орган досудового розслідування), відомості про орган поліції, що здійснює розшук, дати закриття справ, а також дані судових рішень про визнання особи безвісно відсутньою чи оголошення померлою [21].

Крім того, створено Єдиний реєстр осіб, стосовно яких встановлено факт позбавлення особистої свободи внаслідок збройної агресії проти України. Для забезпечення компенсацій громадянам було засновано Державний реєстр майна, пошкодженого та знищеного внаслідок бойових дій, терористичних актів і диверсій, спричинених збройною агресією російської федерації проти України [22]. Кожен із цих реєстрів містить відповідні персональні дані.

Наведені обставини засвідчують, що в умовах війни мета збору і обробки персональних даних здатна змінюватися. Український досвід демонструє істотне розширення сфер їх використання, зокрема, через діяльність пошукових ініціатив та обмін інформацією у соціальних менеджерах щодо зниклих осіб, гуманітарних потреб та евакуації. Такий неформальний обіг даних супроводжувався витоком інформації через недостатній рівень усвідомлення суспільством значення персональних даних як складника системи національної безпеки. З огляду на це, під час формування правового режиму збору та обробки персональних даних у воєнний період необхідно враховувати підвищені ризики та забезпечувати належний рівень захисту.

У своєму рішенні, у справі *Panteleyenko v. Ukraine* від 29 червня 2006 року Європейський суд з прав людини наголошував, що «як зберігання органами публічної влади інформації, що стосується приватного життя особи, так і її використання є втручанням у право на неприкосновенність приватного життя, захищене пунктом 1 статті 8 Конвенції про захист прав людини і основоположних свобод». За таких умов, головне питання полягає в тому, чи це втручання було виправданим за пунктом 2 статті 8 Конвенції про захист прав людини і основоположних свобод, зокрема чи воно було «відповідно до приписів права» (*«in accordance with the law»*) та «потрібним у демократичному суспільстві» щодо однієї з цілей, зазначених у цьому пункті» [23].

В іншому рішенні, у справі *L.B. v. Hungary* від 9 березня 2023 року ЄСПЛ зазначив, що «втручання вважатимуть «потрібним у демократичному суспільстві» для досягнення правомірної мети, якщо воно слугує «нагальній суспільній потребі» і, зокрема, якщо підстави, що їх навели органи влади держави на виправдання, є «доречними та достатніми», і якщо воно є «домірним щодо поставленої правомірної мети» та «захист особових даних має істотне значення для здійснення особою свого права на неприкосновенність приватного і сімейного життя, гарантованого статтею 8 Конвенції про захист прав людини і основоположних свобод. Національне право має забезпечувати належні

гарантії, щоб запобігти будь-якому використанню особових даних, що є несумісним із гарантіями, установленими статтею 8 Конвенції про захист прав людини і основоположних свобод» [24].

У рішенні у справі «Азер Ахмадов проти Азербайджану» від 22 липня 2021 року суд визначив, що захист персональних даних має основоположне значення для реалізації особою свого права на повагу до приватного та сімейного життя, гарантованого статтею 8 Конвенції про захист прав людини і основоположних свобод та будь-яке втручання в права особи може бути виправданим за пунктом 2 статті 8 Конвенції про захист прав людини і основоположних свобод лише якщо воно здійснюється згідно із законом, переслідує одну або декілька законних цілей, наведених у цьому пункті, та є необхідним у демократичному суспільстві для досягнення будь-якої такої цілі [25].

Інформаційна безпека є складовою національної безпеки. Відповідно до ч. 4 ст. 3 Закону України «Про національну безпеку України» державна політика у сферах національної безпеки і оборони спрямовується, зокрема, на забезпечення інформаційної безпеки [26]. Інформаційна безпека є складним поняттям, що охоплює як діяльність держави щодо її забезпечення, так і діяльність окремої людини. Вона стосується як інформації, так і безпеки кіберпростору. Її складовою є і захист персональних даних. При цьому концепція національної безпеки варіюється залежно від конкретного періоду та підходу. В Україні в умовах війни інформаційна безпека стала одним із базових напрямів національної безпеки.

Також слід зазначити, що Законом України «Про критичну інфраструктуру» захист персональних даних віднесено до сфер, які функціонально пов'язані з національною системою захисту критичної інфраструктури (ч. 1 ст. 24 Закону). Відтак система захисту персональних даних має самостійний характер, перебуваючи у безпосередньому зв'язку з національною безпекою [27].

Задля забезпечення інформаційної безпеки 18 березня 2022 р. Рада національної безпеки і оборони України прийняла рішення «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану», яке було введено в дію Указом Президента України від 19 березня 2022 р. № 152/2022 [26]. У ньому визначалося, що в умовах воєнного стану реалізація єдиної інформаційної політики є пріоритетним питанням національної безпеки.

Правовий режим інформаційних систем, зокрема тих, що містять персональні дані, було визначено постановою Кабінету Міністрів України «Деякі питання забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану» від 12 березня 2022 р. № 263. На період дії воєнного стану держателі державних реєстрів (органи публічної влади, державні та комунальні підприємства, установи, організації) задля захисту інформації можуть вживати такі додаткові заходи: розміщувати державні інформаційні ресурси та публічні електронні реєстри на хмарних ресурсах та/або у центрах обробки даних, що розташовані за межами України; створювати додаткові резервні копії публічних електронних реєстрів; зупиняти або обмежувати роботу публічних електронних реєстрів [28].

У 2025 р. було прийнято постанову Кабінету Міністрів України «Деякі питання оперативно-технічного управління електронними комунікаційними мережами в умовах надзвичайної ситуації, надзвичайного або воєнного стану» від 24 січня 2025 р. № 75, в якій зазначено, що для системи оперативно-технічного управління мережами встановлено два режими функціонування: звичайний та надзвичайний (п. 8 Постанови) [29].

У межах національної безпеки кожна країна може встановлювати спеціальні режими захисту персональних даних в умовах війни. В умовах збройного конфлікту зростає кількість кібератак на об'єкти критичної та військової інфраструктури, що може призвести до витоку інформації і, як наслідок, до втрати персональних даних та їх використання ворогом у своїх цілях [18].

Під станом захищеності персональних даних прийнято розуміти юридично забезпечений рівень безпеки персональної інформації, за якого гарантується її конфіденційність, цілісність, доступність, а також дотримання прав суб'єктів даних щодо їх збору, обробки, зберігання та передачі. Він передбачає застосування належних організаційних та технічних заходів, спрямованих на запобігання несанкціонованому доступу, розголошенню, модифікації або знищенню персональних даних відповідно до вимог чинного законодавства [30, с. 231].

У кожній державі розробляються власні системи захисту персональних даних, що залежать від рівня інформаційно-технічного забезпечення, стану законодавства, інформаційно-правової обізнаності населення та організаційних механізмів контролю. Такі системи можуть включати стандарти безпеки інформаційних технологій, процедури шифрування та обмеження доступу до персональних даних, а також механізми моніторингу й реагування на порушення конфіденційності.

У звичайних умовах сфера захисту персональних даних потребує постійного вдосконалення. Об'єктивна потреба у вдосконаленні захисту прав людини у цій сфері визначається поширенням неправомірних і несанкціонованих дій із персональними даними на міжнародному та національному рівнях [31, с. 44] Розширення використання цифрових технологій призводить до додаткового

використання персональних даних, зокрема під час реєстрації чи надання доступу до цифрового профілю людини. Така тенденція підкреслює необхідність посилення механізмів захисту конфіденційності та персональних даних у цифровому середовищі.

Водночас у надзвичайних умовах захист персональних даних має бути посиленим. Доцільною є розробка особливої системи захисту персональних даних, яка може включати такі елементи: роз'яснення населенню ризиків використання персональних даних; підвищення кваліфікації фахівців; створення спеціалізованих підрозділів для захисту персональних даних; розробку та впровадження стратегії кібербезпеки, а також міжнародне співробітництво й обмін досвідом [19]. Окремим напрямом є вдосконалення захисту персональних даних відповідно до європейських стандартів [33].

Введення надзвичайного правового режиму захисту персональних даних має бути завжди обґрунтованим. У світі ця проблематика постала внаслідок пандемії COVID-19, тоді як в Україні певні обмеження прав людини та процедури збору й обробки персональних даних набули особливостей у зв'язку з війною. У п. 46 Преамбули Директиви 95/46/ЄС до надзвичайних гуманітарних ситуацій віднесено, зокрема, стихійні лиха та антропогенні катастрофи. За цих обставин деякі типи опрацювання можуть ґрунтуватися на важливих підставах суспільного інтересу та життєво важливих інтересах суб'єкта даних. Наприклад, якщо опрацювання є необхідним для гуманітарних цілей, у тому числі для моніторингу епідемій та їх поширення [34].

Тобто опрацювання персональних даних на підставі життєво важливого інтересу можливе без згоди суб'єкта персональних даних. Крім того, ст. 6(1)(с) GDPR передбачає альтернативні підстави обробки персональних даних поряд із згодою суб'єкта. Це положення варто застосовувати з урахуванням п. 49 Преамбули (Recital) GDPR, де зазначено, що надзвичайно необхідна обробка персональних даних можлива для забезпечення мережевої та інформаційної безпеки, запобігання несанкціонованому доступу, поширенню шкідливого коду чи відмові в обслуговуванні (DoS-атаки). У такому випадку це визнається законним інтересом контролера і дає йому право на обробку персональних даних.

Отже, для визначення особливостей захисту персональних даних у надзвичайних обставинах необхідно застосовувати сукупність норм, зокрема ст. 6(1)(f) GDPR, п. 49 Преамбули GDPR та положення національного законодавства. Наприклад, у п. 6 ч. 1 ст. 11 Закону України «Про захист персональних даних» встановлено, що підставою для обробки персональних даних є необхідність захисту законних інтересів володільця персональних даних або третьої особи, якій передаються персональні дані, крім випадків, коли потреби захисту основоположних прав і свобод суб'єкта даних у зв'язку з обробкою його даних переважають такі інтереси [7].

Водночас українське законодавство щодо обробки персональних даних у надзвичайних обставинах перебуває у процесі адаптації до європейських стандартів. Аналогічні обмеження під час надзвичайних ситуацій існують у праві США. Так, у ст. 1135 Закону про соціальне забезпечення США (42 U.S.C. § 1320b–5) передбачено тимчасове скасування певних вимог під час національних надзвичайних ситуацій. У випадках пандемій або природних катастроф Секретар Міністерства охорони здоров'я та соціальних служб США (HHS) має право тимчасово скасовувати або змінювати застосування окремих положень HIPAA відповідно до зазначеного Закону. Це дозволяє медичним установам більш гнучко реагувати на надзвичайні ситуації, зокрема щодо обміну інформацією, необхідної для надання медичної допомоги [35].

Виходячи з наведеного, можна стверджувати, що надзвичайний правовий режим захисту персональних даних може мати такі ознаки: 1) вводиться нормативно-правовим актом; 2) має законе підґрунтя запровадження; 3) має тимчасовий характер і застосовується лише на період дії надзвичайної ситуації або воєнного стану; 4) характеризується підвищеним технічним рівнем захисту інформаційних систем, що містять персональні дані, включаючи впровадження додаткових механізмів контролю доступу, шифрування та моніторингу інформаційних потоків; 5) передбачає посилений контроль за обробкою персональних даних; 6) може супроводжуватися спеціальними заходами щодо забезпечення безпеки передачі даних, резервного копіювання та відновлення інформації у разі загрози її втрати або несанкціонованого доступу.

В Україні надзвичайний правовий режим захисту персональних даних так і не був запроваджений. Це створює певні ризики для безпеки інформації, особливо в умовах воєнного стану та активного використання цифрових технологій. Відсутність спеціального режиму ускладнює координацію заходів із захисту персональних даних між державними органами, юридичними особами та громадянами.

Законом України «Про захист персональних даних» визначено, що персональні дані – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована (абз. 10 ч. 1 ст. 2 Закону) [7]. Європейське законодавство також містить визна-

чення цих даних. Так, п. 1 ст. 4 Регламенту Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року «Про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних та про скасування Директиви 95/46/ЄС» (Загальний регламент про захист даних, GDPR) закріплює, що «персональні дані» означають будь-яку інформацію, що стосується фізичної особи, яку ідентифіковано чи можна ідентифікувати («суб'єкт даних»). Фізична особа, яку можна ідентифікувати, – це особа, яку можна ідентифікувати прямо чи опосередковано, зокрема за такими ідентифікаторами, як ім'я, ідентифікаційний номер, дані про місцеперебування, онлайн-ідентифікатор або за одним чи декількома факторами, що є визначальними для фізичної, фізіологічної, генетичної, розумової, економічної, культурної чи соціальної ідентичності такої фізичної особи [36].

Виходячи зі змісту статті зазначеного Регламенту, можна визначити:

- 1) персональні дані становлять окремий вид інформації;
- 2) персональні дані зазвичай фіксуються у документах, що надаються особою;
- 3) основною метою персональних даних є ідентифікація фізичної особи.

Якщо зіставити закріплені поняття в українському та європейському законодавстві, то з порівняльного аналізу випливає, що українське законодавство визначає персональні дані у більш загальних рисах, зосереджуючись на ключовому елементі – можливості ідентифікації особи. Натомість європейський підхід є значно ширшим і конкретизованим: він не лише фіксує сам факт можливості ідентифікації, але й деталізує способи та ознаки, за якими вона здійснюється.

В українському законодавстві поняття персональних даних також закріплено в ч. 1 ст. 11 Закону України «Про інформацію»: «інформація про фізичну особу (персональні дані) – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована». При цьому у ч. 2 ст. 11 цього Закону встановлено, що до конфіденційної інформації про фізичну особу належать, зокрема, дані про її національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адреса, дата і місце народження. Частиною 2 ст. 21 визначено, що конфіденційною є інформація про фізичну особу, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, а також інформація, визнана такою на підставі закону [37]. Виходячи з цього, варто розмежовувати персональні дані та конфіденційну інформацію про особу. Слід звернути увагу, що конфіденційна інформація, як і персональні дані, – це інформація про фізичну особу, зокрема її національність, дату та місце народження, освіту тощо. Водночас до конфіденційної інформації може належати, наприклад, інформація статистичного характеру або відомості про результати перевірки контролюючим органом. У ч. 3 ст. 10¹ Закону України «Про доступ до публічної інформації» встановлено, що публічна інформація, яка містить персональні дані фізичної особи, оприлюднюється та надається на запит у формі відкритих даних у разі дотримання однієї з таких умов: персональні дані знеособлені та захищені відповідно до Закону України «Про захист персональних даних»; фізичні особи (суб'єкти даних), персональні дані яких містяться в інформації у формі відкритих даних, надали свою згоду на поширення таких даних [38].

Персональні дані фіксуються у відповідній базі даних. В.І. Теремецький справедливо зазначає, що базу персональних даних можна розглядати у широкому розумінні (будь-яка база даних, що містить персональні дані) та у вузькому розумінні (збірка персональних даних з метою формування локальної бази персональних даних) [39]. Отже, персональні дані мають таку ознаку, як обов'язковість їх фіксації.

Можна стверджувати, що персональні дані – це особливий вид інформації про особу, яка може бути ідентифікована, зокрема відомості про її дату народження, місце народження, наявність спеціального соціального захисту та інші дані, щодо яких особа надала згоду на їх обробку. Для цих даних характерний режим відкритості, що встановлюється людиною в момент надання згоди на обробку персональних даних. Персональним даним громадян властиві такі ознаки, як: інформаційний зміст; ідентифікаційна властивість; фіксована форма та відображення у певному джерелі (носії даних); невичерпність. Крім того, вони набувають правового режиму персональних даних із початком їх обробки, тобто будь-якої дії або сукупності дій, таких як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення персональних даних, у тому числі з використанням інформаційних (автоматизованих) систем [40].

Щодо класифікації персональних даних, то М.В. Різак пропонує поділяти їх на: загальні персональні дані (прізвище, ім'я, дата народження, а також інші дані, які за згодою суб'єкта розміщені в загальнодоступних базах персональних даних); вразливі персональні дані (відомості про расове або етнічне походження, політичні, релігійні або світоглядні переконання, а також дані, що стосуються здоров'я чи статевого життя); спеціальні персональні дані – дані, межі обігу яких

визначаються суб'єктом [41, с.91]. Слід підкреслити, що у Регламенті Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року «Про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних та про скасування Директиви 95/46/ЄС» виокремлено звичайні та чутливі персональні дані, зокрема дані про стан здоров'я, генетичні та біометричні дані (ст. 4) [36].

Загалом персональні дані можуть класифікуватися залежно від:

1) сфери використання: звичайні персональні дані; персональні дані працівників; персональні дані публічних осіб; персональні дані військовослужбовців та осіб, що беруть участь у збройному конфлікті (зокрема волонтерів); персональні дані призовників, військовозобов'язаних та резервістів; медичні персональні дані (про стан здоров'я, генетичні дані); персональні дані, що використовуються у цифровому середовищі;

2) можливості поширення: відкриті персональні дані та конфіденційні персональні дані;

3) відношення до приватності особи: звичайні персональні дані та чутливі персональні дані;

4) в залежності від правових режимів їх захисту: персональні дані в звичайному, надзвичайному та воєнному станах;

5) в залежності від підстав їх обробки: персональні дані обробка яких здійснена за згодою суб'єкта персональних даних та персональні дані обробка яких здійснена без його згоди (зокрема, але не виключно, відповідно до вимог закону);

6) в залежності від мети обробки: персональні дані в цілях охорони здоров'я; персональні дані в цілях забезпечення ведення військового обліку призовників, військовозобов'язаних та резервістів; персональні дані для захисту життєво важливих інтересів суб'єкта персональних даних або іншої особи у разі недієздатності або обмеження цивільної дієздатності суб'єкта персональних даних тощо.

Висновки. Проведене дослідження дозволяє дійти висновку, що персональні дані як правова категорія характеризуються подвійністю підходів до їхнього розуміння: у вітчизняному праві вони визначаються насамперед через можливість ідентифікації особи, тоді як європейський підхід є більш конкретизованим та охоплює способи, ознаки та контексти такої ідентифікації. Ця різниця зумовлює різну глибину правового регулювання та ступінь захищеності інформації про фізичних осіб.

Умови воєнного стану посилюють потребу у застосуванні спеціальних технічних і правових механізмів захисту персональних даних, оскільки стандартні політики конфіденційності, характерні для звичайного режиму функціонування цифрових сервісів, не забезпечують належного рівня безпеки в умовах надзвичайного чи воєнного стану.

Захист персональних даних становить невід'ємну складову інформаційно та, відповідно, національної безпеки держави, адже забезпечує конфіденційність, цілісність і доступність інформації про фізичних осіб, знижує ризики несанкціонованого доступу та витоку даних. Під час воєнного стану ці вимоги набувають особливої ваги, коли виникає потреба у запровадженні посилених, надзвичайних механізмів захисту персональних даних.

Системи захисту персональних даних формуються з урахуванням рівня технічного оснащення інформаційних систем, особливостей національного законодавства, правової обізнаності громадян та дієвості механізмів контролю. Реалізація захисту персональних даних може відбуватися у звичайному і надзвичайному правовому режимі. Перспективним напрямом розвитку законодавства є удосконалення підходів до захисту персональних даних саме в умовах надзвичайного і воєнного станів. Подальшого наукового опрацювання потребує також концептуалізація персональних даних як об'єкта національної безпеки та складника приватності особи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»: Указ Президента України від 28 грудня 2021 року № 685/2021. URL: <https://zakon.rada.gov.ua/laws/show/685/2021#Text>.
2. Загальна декларація прав людини від 10 грудня 1948 р. URL: https://zakon.rada.gov.ua/laws/show/995_015#Text.
3. Конвенція про захист прав людини і основоположних свобод від 04 листопада 1950 р. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text.
4. Міжнародний пакт про громадянські і політичні права від 16 грудня 1966 року. URL: https://zakon.rada.gov.ua/laws/show/995_043#Text.
5. Загальний регламент ЄС про захист даних (GDPR) від 27 квітня 2016 р. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text.
6. Конвенція ЄС 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#Text.

7. Про захист персональних даних : Закон України від 1 червня 2010 р. № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>.
8. Рішення Конституційного Суду України від 20 січня 2012 року N 2-пп/2012. URL: <https://zakon.rada.gov.ua/laws/show/v002p710-12#Text>.
9. Рішення Конституційного Суду України від 11 жовтня 2018 року N 7-п/2018. URL: <https://zakon.rada.gov.ua/laws/show/v007p710-18#Text>.
10. Рішення Конституційного Суду України від 22 березня 2023 року N 3-п(II)/2023. URL: <https://zakon.rada.gov.ua/laws/show/va01p710-24#Text>.
11. Тимошенко О.А. Захист персональних даних в цивільних правовідносинах: вітчизняне правове забезпечення крізь призму практики європейського суду з прав людини. *Аналітично-порівняльне правознавство*. 2023. № 4. С. 165-172. DOI <https://doi.org/10.24144/2788-6018.2023.04.27>.
12. Полонська О.І. Правова регламентація правомірного обмеження права на недоторканність приватного життя в умовах правового режиму воєнного стану. *Електронне наукове видання «Аналітично-порівняльне правознавство»*. 2023. Вип.3 ч. 1 с.323-328. DOI <https://doi.org/10.24144/2788-6018.2025.03.1.48>.
13. Попович Т.П. Право особи на захист персональних даних в Інтернеті: теоретико-правові аспекти. *Аналітично-порівняльне правознавство*. 2021. № 2. С. 51-54. DOI <https://doi.org/10.24144/2788-6018.2021.02.9>.
14. Михайлик А.С. До питання нормативно-правового регулювання захисту персональних даних працівників в Україні. *Науковий вісник Ужгородського Національного Університету*, Серія ПРАВО. 2022. Вип. 72: частина 2. С. 82-87. DOI <https://doi.org/10.24144/2307-3322.2022.72.46>.
15. Малюга Л.Ю., Шкрібляк К.П. Особливості захисту персональних даних у процесі цифровізації трудових відносин в Україні: теоретико-правовий аналіз. *Науковий вісник Ужгородського національного університету*. Серія Право. 2025. № 91. ч.4. с. 398-418. DOI: <https://doi.org/10.24144/2307-3322.2025.91.2.14>.
16. Спіцина Г., Гуцу С. Захист особистої інформації працівників, отриманої у процесі відеоспостереження на робочому місці. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2023. № 2 (123). С. 171-178. DOI: <https://doi.org/10.31733/2078-3566-2023-2-171-178>.
17. Брижко В.М., Пилипчук В.Г. Приватність, конфіденційність та безпека персональних даних. *Інформація і право*. № 1(32)/2020. С. 33-46. URL: http://nbuv.gov.ua/UJRN/Infpr_2020_1_5.
18. Кірієнко В.М. Захист персональних даних як аспекту національної безпеки в умовах збройного конфлікту. *Юридичний науковий електронний журнал*. 2024. № 1. С. 398-400. С. 399. DOI <https://doi.org/10.32782/2524-0374/2024-1/90>.
19. Світличний В.А. Захист персональних даних в умовах воєнного стану в Україні. *Право і безпека – Law and Safety*. 2023. № 3 (90). С. 226-235 DOI: <https://doi.org/10.32631/pb.2023.3.19>.
20. Фасій Б. Національна безпека та захист персональних даних в епоху цифрових технологій. *Управління національною безпекою*. № 6 (6) 2024. С. 76-82. URL: http://lsej.org.ua/6_2024/6_2024.pdf
21. Про затвердження Положення про Єдиний реєстр осіб, зниклих безвісти за особливих обставин: наказ Міністерства внутрішніх справ України від 29 серпня 2022 р. № 535. URL: <https://zakon.rada.gov.ua/laws/show/z0998-22#Text>.
22. Деякі питання забезпечення функціонування Державного реєстру майна, пошкодженого та знищеного внаслідок бойових дій, терористичних актів, диверсій, спричинених збройною агресією Російської Федерації проти України: постанова Кабінету Міністрів України від 13 червня 2023 р. № 624. URL: <https://zakon.rada.gov.ua/laws/show/624-2023-%D0%BF#Text>.
23. Рішення Європейського суду з прав людини у справі «Пантелеєнко проти України» (Panteleyenko v. Ukraine) від 29 червня 2006 р. від 29 червня 2006 року. URL: https://zakon.rada.gov.ua/laws/show/974_274#Text.
24. Рішення Європейського суду з прав людини у справі «L.B. v. Hungary» від 9 березня 2023 року. URL: https://zakon-pro.ligazakon.net/document/ES074933?utm_source=oldproduct&utm_medium=baner_ID&utm_campaign=LIGA360_new&land=UA&context=UA.
25. Рішення Європейського суду з прав людини у справі «Азер Ахмадов проти Азербайджану» (Azer Ahmadov v. Azerbaijan) від 22 липня 2021 року. URL: <https://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=001-220392&filename=CASE%20OF%20AZER%20AHMADOV%20v.%20AZERBAIJAN%20-%20%5BUkrainian%20Translation%5D%20by%20ECHR%20Ukrainian%20Aspect.pdf>.

26. Про національну безпеку України: Закон України від 21 червня 2018 р. № 2469-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2469-19#Text>.
27. Про критичну інфраструктуру: Закон України від 16.11.2021 № 1882-IX. URL: <https://zakon.rada.gov.ua/laws/show/1882-20#Text>.
28. Щодо реалізації єдиної інформаційної політики в умовах воєнного стану: рішення Ради Національної безпеки і оборони України від 18 березня 2022 р. URL: <https://zakon.rada.gov.ua/laws/show/n0004525-22#Text>.
29. Деякі питання забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану: постанова Кабінету Міністрів України від 12 березня 2022 р. № 263. URL: <https://zakon.rada.gov.ua/laws/show/263-2022-%D0%BF#Text>.
30. Деякі питання оперативно-технічного управління електронними комунікаційними мережами в умовах надзвичайної ситуації, надзвичайного або воєнного стану: постанова Кабінету Міністрів України від 24 січня 2025 р. № 75. URL: <https://zakon.rada.gov.ua/laws/show/75-2025-%D0%BF#top>.
31. Дяковський О.С. Характерні риси прояву захисту персональних даних. *Юридичний науковий електронний журнал*. 2025. № 2. С. 230-232. URL: http://lsej.org.ua/2_2025/55.pdf.
32. Пилипчук В.Г., Брижко В.М. Трансформація системи захисту персональних даних та приватності в контексті євроінтеграції України. *Вісник Національної академії правових наук України*. 2017. № 3 (90). С. 36-50. URL: http://nbuv.gov.ua/UJRN/vapny_2017_3_5.
33. Яворська, О. С. (2024). Захист персональних даних у цифровому середовищі: досвід ЄС. *Юридичний науковий електронний журнал*. 2024. № 9 С. 117-119. DOI <https://doi.org/10.32782/2524-0374/2024-9/26>.
34. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних). URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text.
35. U.S. Social Security Administration. (n.d.). Section 1135: Authority to waive requirements during national emergencies. Retrieved August 27, 2025 https://www.ssa.gov/OP_Home/ssact/title11/1135.htm.
36. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних). URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text.
37. Про інформацію Закон України від 2 жовтня 1992 р. № 2657-XII. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#top>.
38. Про доступ до публічної інформації: Закон України від 13 січня 2011 р. № 2939-VI. URL: <https://zakon.rada.gov.ua/laws/show/2939-17#Text>.
39. Теремецький В.І. Загальна характеристика охорони бази персональних даних за законодавством України. *Підприємництво, господарство і право*. 2015. № 11. С. 3-5. URL: http://prp-journal.kiev.ua/archive/2015/10_2015.pdf.
40. Цюменко, А. Персональні дані громадян та їхня класифікація в сучасній доктрині адміністративного права. *Вісник Київського національного університету імені Тараса Шевченка*. 2023. № 1 (53). С. 41-45. DOI: <https://doi.org/10.17721/1728-2217.2023.53.41-45>.
41. Різак М.В. Класифікація персональних даних як необхідний елемент введення ефективної комунікації в суспільстві. *Науковий вісник Міжнародного гуманітарного університету*. Серія: Юриспруденція. 2013. Вип. 6-3(1). С. 90-94. URL: <https://www.vestnik-pravo.mgu.od.ua/archive/juspradenc6-3-1/23.pdf>.