

### Список використаних джерел:

1. Наказ МВС України від 26.04.2018 № 340, зареєстрований в Міністерстві юстиції України 10.06.2018 за № 801/32253 «Про затвердження Статуту дій у надзвичайних ситуаціях органів управління та підрозділів Оперативно-рятувальної служби цивільного захисту та Статуту дій органів управління та підрозділів Оперативно-рятувальної служби цивільного захисту під час гасіння пожеж». *{Із змінами, внесеними згідно з Наказами МВС № 50 від 26.01.2022 № 251 від 18.04.2024}*. URL: <https://zakon.rada.gov.ua/laws/show/z0801-18#Text>
2. Дегтярьова Л. М., Гроза П. М. Технології розробки програмного забезпечення : навч. посіб. Полтава : ПолтНТУ, 2017. 218 с.
3. Грицюк Ю. І. Аналіз вимог до програмного забезпечення. Львів : Львівська політехніка, 2018. 456 с.

DOI <https://doi.org/10.36059/978-966-397-502-3-58>

**Жданкевич М. О.,**

*аспірант 2 курсу за спеціальністю 081 – Право  
Таврійського національного університету імені В. І. Вернадського  
м. Київ, Україна*

### **УДОСКОНАЛЕННЯ ЗАКОНОДАВСТВА ПРО ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ УКРАЇНИ В УМОВАХ ВОЄННОГО СТАНУ**

В умовах воєнного стану питання захисту персональних даних та державної таємниці набувають особливої актуальності, оскільки інформаційна безпека стає ключовим елементом забезпечення національної безпеки та обороноздатності держави. Виклики, пов'язані з кібератаками, інформаційними диверсіями та витоками конфіденційної інформації, вимагають удосконалення правових механізмів регулювання цієї сфери. З одного боку, право на захист персональних даних є основоположним правом людини, гарантованим як національним законодавством, так і міжнародними договорами, такими як Конвенція Ради Європи № 108 [1] та Загальний регламент про захист даних (GDPR) [2].

В умовах воєнного стану виникає необхідність пошуку балансу між відкритістю державних процесів і забезпеченням конфіденційності інформації, що може впливати на безпеку держави та громадян. Дослідження правових гарантій захисту персональних даних дозволяє

оцінити ефективність чинних правових механізмів, виявити прогалини в законодавстві та сформулювати рекомендації щодо вдосконалення системи інформаційної безпеки в кризових умовах.

Питання захисту персональних даних урегульовано Законом України «Про захист персональних даних» [3], аналіз якого показує, що з початку введення в Україні у лютому 2022 року правового режиму воєнного стану якісь спеціальні механізми або гарантії захисту відповідних даних фактично не запроваджувалися, окрім, зокрема, встановлення особливих умов обміну деякими відомостями медичного характеру.

Разом з тим, як свідчить офіційна статистика, протягом 2023 року Уповноваженим було розглянуто 2205 звернень, пов'язаних із порушеннями у сфері захисту персональних даних. З них: 49 % – незаконна обробка персональних даних; 14 % – доступ до власних персональних даних; 16 % – організація обробки персональних даних на підприємствах, установах та організаціях; 21 % – отримання рекомендацій і роз'яснень [4].

Отже, проблема порушення права осіб на персональні дані в умовах воєнного часу тільки загострилася.

Деякі науковці з цього приводу звертають увагу на необхідність дотримання гарантій захисту персональних даних деяких категорій осіб, чий права у цій сфері є особливо вразливими у період воєнного стану. Зокрема, йдеться про військовозобов'язаних та інших осіб під час отримання, обробки та використання інструментами електронного реєстру [5, с. 414].

Погоджуючись з необхідністю удосконалення законодавства про захист персональних даних в умовах дії правового режиму воєнного стану з метою посилення захисту персональних даних, необхідно розглянути можливість щодо внесення таких змін та доповнень до Закону України «Про захист персональних даних»:

1) запровадження особливого режиму обробки персональних даних під час воєнного стану, а саме: визначити перелік категорій персональних даних, обробка яких має бути обмежена або заборонена під час воєнного стану (наприклад, місце проживання військовослужбовців, їхні сімейні зв'язки тощо); надати право державним органам тимчасово призупиняти доступ до персональних даних у випадку загрози кібератак або витоку інформації; встановити особливі вимоги до обробки персональних даних військовослужбовців, переселенців, осіб, що перебувають на тимчасово окупованих територіях;

2) посилення відповідальності за порушення вимог щодо захисту персональних даних, зокрема: запровадити кримінальну відповідальність за несанкціоноване розголошення або передачу персональних даних, що може завдати шкоди національній безпеці; підвищити штрафи для посадових осіб державних органів, підприємств та

приватних компаній, які допустили витік даних або неналежний рівень їх захисту;

3) удосконалення вимог до кібербезпеки та збереження даних: зобов'язати всі державні та приватні установи використовувати сертифіковані засоби шифрування для зберігання та передачі персональних даних; установити обов'язкове резервне копіювання критичних персональних даних у захищених державних дата-центрах; запровадити прискорену процедуру реагування на кібератаки та витоки даних, зокрема обов'язкове повідомлення Держспецзв'язку про інциденти;

4) обмеження доступу до персональних даних у критичних умовах: надати право органам державної влади тимчасово обмежувати доступ до державних реєстрів у разі загрози несанкціонованого втручання; впровадити багаторівневу систему аутентифікації для доступу до баз даних під час воєнного стану (наприклад, подвійна ідентифікація для державних службовців); визначити механізми швидкого видалення або приховування персональних даних осіб, що перебувають у зоні ризику (наприклад, військових, журналістів, волонтерів);

5) запровадження особливого режиму захисту персональних даних громадян на окупованих територіях: передбачити можливість зашифрованого зберігання персональних даних осіб, що перебувають в тимчасовій окупації, з метою унеможливлення їх використання ворогом; заборонити передавання персональних даних осіб із тимчасово окупованих територій будь-яким організаціям, крім державних структур України; встановити особливі процедури перевірки та підтвердження особи для тих, хто виїжджає з окупованих територій або отримує соціальну допомогу.

Запровадження цих змін дозволить підвищити рівень захисту персональних даних та запобігти їхньому несанкціонованому використанню в умовах війни.

Таким чином, правові гарантії захисту персональних даних в умовах воєнного стану є важливим інструментом забезпечення національної безпеки та захисту прав громадян. Воєнні загрози та активізація кібератак вимагають від держави ефективного регулювання обігу інформації, що включає як обмеження доступу до чутливих даних, так і запровадження механізмів контролю за їх використанням.

Дослідження показало, що правова система України передбачає широкий спектр норм щодо захисту персональних даних (Закон України «Про захист персональних даних»), однак у період воєнного стану виникає низка викликів, пов'язаних із адаптацією цих норм до нових загроз. Зокрема, актуальними залишаються питання запобігання витокам інформації, посилення контролю за її обробкою та забезпечення належного рівня кібербезпеки.

З огляду на це, доцільним є вдосконалення нормативної бази у сфері інформаційної безпеки, посилення відповідальності за незаконне

розголошення персональних даних і державної таємниці, а також впровадження сучасних технологічних рішень для захисту інформації. Важливим також є дотримання балансу між відкритістю державної інформації та необхідністю обмеження доступу до певних відомостей в інтересах національної безпеки.

Отже, правове забезпечення захисту персональних даних в умовах воєнного стану потребує подальшого розвитку, адаптації до сучасних загроз і впровадження найкращих міжнародних практик для ефективного функціонування державних інституцій та захисту громадян.

### **Список використаних джерел:**

1. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних: міжнародний документ від 28.01.1981. URL: [https://zakon.rada.gov.ua/laws/show/994\\_326#Text](https://zakon.rada.gov.ua/laws/show/994_326#Text)

2. 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. (GDPR): Міжнародний документ від 27.04.2016 № 2016/679. URL: [https://zakon.rada.gov.ua/laws/show/984\\_008-16#Text](https://zakon.rada.gov.ua/laws/show/984_008-16#Text)

3. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. URL : <https://zakon.rada.gov.ua/laws/show/2297-17#Text>

4. Проблеми захисту персональних даних в умовах воєнного стану обговорили за круглим столом: Національна асоціація адвокатів України. 2024. URL: <https://unba.org.ua/news/9369-problemi-zahistu-personal-nih-danih-v-umovah-voennogo-stanu-obgovorili-za-kruglim-stolom.html>

5. Бойко Б. В. Гарантії захисту персональних даних військово-зобов'язаних під час їх використання в державних реєстрах для військового обліку. *Електронне наукове видання «Аналітично-порівняльне правознавство»*. 2023. № 12. С. 410–415.