Тетяна БЛАЩУК
ORCID: 0000-0002-0605-1920

ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ МЕДИЧНОЇ ІНФОРМАЦІЇ ПРИ НАДАННІ МЕДИЧНОЇ ДОПОМОГИ ВІЙСЬКОВОСЛУЖБОВЦЯМ ТА ВІЙСЬКОВОЗОБОВ'ЯЗАНИМ

УДК 347.1, 342.7

Постановка проблеми. Забезпечення конфіденційності медичної інформації, особливо у військовій сфері, є одним із ключових викликів сучасного державного управління. Медичні дані військовослужбовців є не лише приватною інформацією, але й важливим інструментом для ухвалення стратегічних рішень у сфері оборони, мобілізації, соціального забезпечення та планування. З розвитком цифрових технологій з'являються нові можливості для автоматизації процесів передачі та обробки таких даних, але разом із цим зростають і ризики, пов'язані з порушенням конфіденційності, несанкціонованим доступом та кіберзагрозами.

Проблема набуває особливої актуальності у зв'язку зі створенням Єдиного державного реєстру призовників, військовозобов'язаних та резервістів «Оберіг», який передбачає централізоване зберігання й обробку великого обсягу персональних, в тому числі медичних даних. Недостатня захищеність системи, відсутність чітких регламентів доступу, недостатній контроль за обробкою даних і слабка інтеграція із міжнародними стандартами конфіденційності можуть призвести до серйозних наслідків, зокрема до витоку інформації, зловживань або порушення прав громадян.

Аналіз останніх досліджень та публікацій. Проблематика захисту персональних даних в умовах війни є однією з ключових у сучасній юридичній науці. Останні дослідження демонструють різні аспекти та підходи до забезпечення конфіденційності інформації про військовослужбовців і військовозобов'язаних, що дозволяє окреслити основні виклики та запропонувати шляхи їх вирішення.

В. Пашинський та В. Цьоменко у статті «Забезпечення захисту персональних даних громадян органами публічної влади в умовах війни» (2022) акцентують увагу на особливій важливості захисту даних військовослужбовців в умовах широкомасштабної військової агресії [1]. Автори підкреслюють, що несанкціонований доступ до даних військовополонених може бути використаний противником для інформаційних атак, шантажу та поширення панічних настроїв. Запропоновано створення окремих реєстрів із різними рівнями верифікації доступу та розширення повноважень Координаційного штабу для ефективного управління інформацією у цій сфері.

П. В. Діхтієвський у статті «Адміністративно-правове забезпечення захисту персональних даних громадян в умовах воєнного стану» (2023) досліджує питання адаптації правового регулювання до умов воєнного стану [2]. Автор наголошує, що забезпечення захисту даних має ґрунтуватися на пропорційності заходів, швидкій адаптації до змін у суспільних відносинах та суворому дотриманні законодавства. Зокрема, адміністративно-правові механізми повинні спрямовуватися на мінімізацію ризиків втрати чи знищення даних та попередження несанкціонованого доступу.

Б. В. Бойко у статті «Гарантії захисту персональних даних військовозобов'язаних під час їх використання в державних реєстрах для військового обліку» (2023) розглядає специфіку використання даних у процесах мобілізаційної підготовки [3]. Автор наголошує на необхідності внесення змін до законодавства, які б чітко визначали перелік осіб із доступом до даних, мінімізували обмін інформацією між реєстрами та забезпечували високий рівень технічного захисту інформаційних систем. Запропоновано публічну сертифікацію програмних продуктів та посилення відповідальності за незаконні дії з даними.

Метою статті є аналіз існуючих нормативно-правових засад та практичних механізмів забезпечення конфіденційності медичної інформації у військовій сфері, зокрема в умовах автоматизації передачі даних до Єдиного державного реєстру призовників, військовозобов'язаних та резервістів. Особливу увагу приділено визначенню основних викликів, таких як захист від несанкціо-

нованого доступу, регулювання доступу до інформації та відповідність міжнародним стандартам. На основі дослідження запропоновано практичні рекомендації для впровадження технічних і правових заходів, які сприяють підвищенню ефективності роботи з даними, збереженню конфіденційності та зміцненню довіри громадян до державних систем управління інформацією.

Виклад основного матеріалу. Забезпечення конфіденційності медичної інформації є ключовим аспектом прав людини, що гарантує повагу до приватного життя та захист персональних даних. Для військовослужбовців це питання набуває особливого значення, оскільки їх медична інформація може бути пов'язана з професійною діяльністю, фізичною придатністю до служби та участю у бойових діях.

Захист конфіденційності медичної інформації військовослужбовців регулюється комплексом національних і міжнародних правових актів. Національне законодавство закладає фундаментальні принципи та механізми, тоді як міжнародні норми встановлюють загальні стандарти та забезпечують інтеграцію національної правової системи в глобальний контекст.

В Україні захист конфіденційності медичної інформації військовослужбовців забезпечується Конституцією України (1996), яка у статті 32 гарантує кожній особі право на збереження конфіденційності особистої інформації, включаючи медичні дані [4].

Закон України «Основи законодавства України про охорону здоров'я» (1992) встановлює обов'язок медичних працівників зберігати лікарську таємницю, забороняючи розголошення інформації про стан здоров'я пацієнта без його згоди [5]. Водночас винятки, передбачені цим законом, дозволяють передавати такі дані в окремих випадках, зокрема для забезпечення національної безпеки. У зв'язку зі створенням Єдиного державного реєстру призовників, військовозобов'язаних та резервістів «Оберіг» такі винятки набули особливої актуальності. Автоматизація процесу передачі медичних даних до цього реєстру спрямована на підвищення ефективності мобілізаційних процесів і забезпечення точності інформації про стан здоров'я військовослужбовців.

Закон України «Про інформацію» (1992) визначає принципи захисту персональних даних, включаючи медичну інформацію

[6]. Він наголошує на балансі між суспільними потребами у використанні даних та забезпеченням їх конфіденційності. Автоматизована передача медичних даних до реєстру «Оберіг» вимагає додаткових заходів для запобігання несанкціонованому доступу та використанню інформації. Це передбачає впровадження таких технічних рішень, як шифрування даних, багаторівнева автентифікація та моніторинг доступу.

Закон України «Про соціальний і правовий захист військовослужбовців та членів їх сімей» (1991) передбачає використання медичних даних для надання військовослужбовцям пільг і компенсацій [7]. Автоматизація цього процесу через реєстр «Оберіг» спрощує роботу відповідних органів, але потребує чіткого регулювання доступу до інформації. Це має запобігти порушенням конфіденційності, особливо якщо до даних отримують доступ сторонні структури.

Наказ Міністерства оборони України «Про затвердження Порядку обробки і захисту персональних даних у Міністерстві оборони України» (2014) є ключовим нормативним документом, що регулює процеси збору, обробки, зберігання та передачі персональних даних, включаючи медичні, у структурі Міністерства оборони [8]. Він встановлює жорсткі вимоги до конфіденційності даних, визначає коло осіб, які мають право на доступ до них, та регламентує порядок їх передачі. Цей наказ, у поєднанні із законодавчими нормами, забезпечує нормативну основу для роботи з персональними даними військовослужбовців у нових умовах автоматизації.

Автоматизація передачі медичних даних через реєстр «Оберіг» сприяє ефективності управлінських процесів у військовій сфері, але водночас створює ризики порушення конфіденційності. Для їх мінімізації необхідно посилити технічний захист даних і впровадити механізми прозорого контролю за доступом до системи. Це дозволить забезпечити баланс між національною безпекою та правами громадян на конфіденційність.

Міжнародні норми захисту прав людини мають важливе значення для формування правового поля захисту конфіденційності медичної інформації. Конвенція про захист прав людини і осно-

воположних свобод (1950), зокрема її стаття 8, гарантує право на повагу до приватного і сімейного життя [9]. Це включає захист персональних даних, зокрема медичних, навіть у випадках, що стосуються державної безпеки або суспільних інтересів. Останні зміни у національному законодавстві України, зокрема автоматична передача медичних даних до реєстру «Оберіг», викликають необхідність забезпечення дотримання цих стандартів у межах нових умов.

Рішення Європейського суду з прав людини у справі «М.К. проти України» (2022) підтвердило, що захист персональних даних, включаючи медичну інформацію, є невід'ємною частиною права на повагу до приватного життя [10]. Суд зазначив, що навіть у випадках, коли розкриття інформації здійснюється в інтересах державної безпеки, це має бути пропорційним і супроводжуватись чіткими гарантіями. Важливо, що у цій справі підкреслено необхідність мінімізації втручання в особисте життя шляхом запровадження механізмів контролю за доступом до персональних даних та їх захистом від неправомірного використання.

Рішення у справі «Суріков проти України» (2017) розширило розуміння зобов'язань держави щодо забезпечення конфіденційності персональних даних, підкресливши, що наявності законодавства недостатньо для захисту даних [11]. Європейський суд з прав людини наголосив, що держава повинна гарантувати ефективне виконання законів через чітке регулювання доступу до інформації, контроль над її використанням і відповідність обробки визначеній меті. Це включає впровадження механізмів, які обмежують доступ до даних лише для уповноважених осіб та забезпечують прозорість усіх операцій з інформацією, зокрема зберігання, передачі та доступу.

Суд також звернув увагу на важливість встановлення суворої відповідальності за порушення конфіденційності, що охоплює як державні, так і приватні установи, які обробляють персональні дані. Побудова довіри громадян до державних механізмів захисту конфіденційності залежить від відкритості процедур, чіткої регламентації процесів обробки інформації та можливості звернення до незалежних органів для вирішення спорів. Таким чином, ефек-

тивна система захисту даних має не лише відповідати національним і міжнародним стандартам, але й бути практичною та дієвою в забезпеченні прав людини.

Забезпечення конфіденційності медичної інформації у військовій сфері має свої специфічні особливості, зумовлені необхідністю поєднання захисту персональних даних із потребами національної безпеки. У цій сфері важливе значення мають нормативно-правове регулювання, чітка організація роботи з персональними даними та впровадження сучасних технологічних засобів захисту. Розгляд особливостей включає порядок обробки персональних даних у Міністерстві оборони України та передачу медичних даних до Єдиного державного реєстру призовників, військовозобов'язаних та резервістів.

У світі, де цифрові технології стають невід'ємною частиною державного управління, особливо важливою є розробка надійних систем захисту персональних даних. Це стосується і медичної інформації, яка потребує особливого рівня конфіденційності через її чутливість. Для цього необхідно впроваджувати сучасні технічні рішення, такі як шифрування, багаторівневий контроль доступу та захищені канали передачі даних.

Однак лише технічні заходи не є достатніми. Необхідно також забезпечити обмеження доступу до медичних даних певним колом осіб, які мають відповідну підготовку та повноваження. Такий підхід мінімізує ризик неправомірного використання інформації і гарантує, що дані залишатимуться доступними лише тим, хто безпосередньо відповідає за їх обробку.

Важливим елементом є впровадження регулярного аудиту систем обробки медичних даних. Це дозволить оперативно виявляти та усувати можливі вразливості, забезпечуючи дотримання як національних, так і міжнародних стандартів захисту. Прозорість процесів, включаючи чітку регламентацію відповідальності осіб, які мають доступ до даних, зміцнить довіру громадян і сприятиме підвищенню ефективності використання інформаційних систем.

Як вже було вказано порядок обробки персональних даних у структурі Міністерства оборони України регламентується Нака-

зом Міністерства оборони «Про затвердження Порядку обробки і захисту персональних даних у Міністерстві оборони України». Доступ до медичних даних має обмежене коло осіб, які наділені відповідними повноваженнями. Передача інформації здійснюється через захищені канали зв'язку, з обов'язковим впровадженням таких заходів, як шифрування даних і двофакторна автентифікація. Крім того, Наказ передбачає проведення регулярного аудиту систем зберігання і передачі даних для виявлення та усунення можливих загроз.

Особливої уваги потребує питання відповідальності за порушення правил обробки персональних даних. При розголошенні конфіденційної інформації передбачено дисциплінарну, адміністративну або кримінальну відповідальність, залежно від характеру порушення.

Починаючи з 01.01.2025, набудуть чинності зміни до законодавства, які регламентують впровадження нових механізмів захисту персональних даних. Передача медичних даних до Єдиного державного реєстру призовників, військовозобов'язаних та резервістів «Оберіг» є однією з ключових змін у законодавстві, спрямованих на підвищення ефективності мобілізаційних процесів. Автоматизація передачі даних дозволяє оперативно отримувати інформацію про стан здоров'я військовослужбовців, що є важливим для ухвалення управлінських рішень у сфері національної безпеки.

Цей процес регулюється положеннями законів України «Про інформацію», «Основи законодавства України про охорону здоров'я» та «Про соціальний і правовий захист військовослужбовців та членів їх сімей». Дані передаються через захищену інфраструктуру, яка включає багаторівневі системи доступу та моніторинг всіх операцій із використанням персональної інформації.

Автоматизація передачі медичних даних має низку переваг, серед яких швидкість обробки запитів, мінімізація людського фактору та інтеграція даних із іншими державними реєстрами. Як зазначено у статті «Основні виклики та рішення в розробці ПЗ для охорони здоров'я» (2024), автоматизація у сфері охорони

здоров'я не лише оптимізує процеси, але й забезпечує точність та узгодженість даних між різними структурами [12]. Вона також сприяє ефективній координації між медичними закладами та іншими державними установами, що є критично важливим для ухвалення оперативних рішень.

Проте, цей підхід створює і певні виклики. Основним з них є необхідність забезпечення повної конфіденційності та виключення ризику несанкціонованого доступу до даних. Як сказано раніше, вирішення цих проблем потребує впровадження таких заходів, як багатофакторна автентифікація, шифрування даних на всіх етапах обробки та автоматичний моніторинг безпеки системи. У цьому контексті важливим є забезпечення постійного контролю за функціонуванням інформаційних систем, що дозволяє виявляти потенційні загрози та вчасно їх усувати.

Питання етичності автоматизації обробки медичних даних також набуває актуальності. Важливо, щоб усі зміни відповідали не лише законодавству України, але й міжнародним стандартам, таким як Конвенція про захист прав людини і основоположних свобод. Дотримання прав громадян на конфіденційність у рамках роботи з реєстром «Оберіг» має бути інтегроване у всі етапи цього процесу.

Висновки. Україна зараз має унікальну можливість стати прикладом для інших країн у поєднанні інтересів національної безпеки та дотримання прав людини. Забезпечення конфіденційності медичної інформації, особливо у військовій сфері, є важливим викликом, що потребує комплексного підходу. Аналіз нормативно-правової бази, технологічних рішень і міжнародних стандартів демонструє, що впровадження сучасних систем захисту може суттєво підвищити ефективність роботи з персональними даними.

Важливо не лише впровадити технічні засоби захисту, такі як шифрування, багаторівневий доступ і моніторинг безпеки, але й забезпечити регулярний аудит систем обробки медичних даних. Це дозволить вчасно виявляти потенційні вразливості та усувати ризики несанкціонованого доступу. Одночасно необхідно регламентувати доступ до інформації, обмеживши його лише упов-

новаженими особами з відповідною підготовкою. Прозорість процедур і довіра громадян до процесу є ключовими факторами успішної реалізації таких реформ.

У контексті автоматизації обробки медичних даних Україна стоїть на порозі нової ери управління персональною інформацією. Забезпечення чіткого балансу між потребами держави та правами громадян сприятиме зміцненню правової системи, підвищенню ефективності державного управління та закріпленню репутації України як партнера, що дотримується найкращих міжнародних стандартів. Інтеграція сучасних технологій у державне управління дозволить уникнути втрати ключових демократичних цінностей та забезпечить відповідність системи вимогам як національного, так і міжнародного законодавства.

1. *Пашинський, В., & Цьоменко, В. (2023). Забезпечення захисту персональних даних громадян органами публічної влади в умовах війни. Вісник Київського національного університету імені Тараса Шевченка. Військово-спеціальні науки, 52 (4 (52), 50–53. https://doi.org/10.17721/1728-2217.2022.52.50-53*
2. *Діхтієвський, П. В. (2023). Адміністративно-правове забезпечення захисту персональних даних громадян в умовах воєнного стану. Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування, (10). https://doi.org/10.54929/2786-5746-2023-10-01-15*
3. *Boyko B. V. Guarantees of protection of personal data of conscripts during their use in state registers for military registration. Analytical and comparative jurisprudence. 2023. No. 6. P. 410–415. URL:https://doi.org/10.24144/2788-6018.2023.06.69 (date of access: 23.11.2024).*
4. *Конституція України : Закон України від 28 червня 1996 р. № 254к/96-ВР. URL:https://zakon.rada.gov.ua/go/254к/96-вр (дата звернення: 23.11.2024).*
5. *Основи законодавства України про охорону здоров'я : Закон України від 19 листопада 1992 р. № 2801-XII. URL: https://zakon.rada.gov.ua/laws/show/2801-12/ed20250101#Text (дата звернення: 23.12.2024).*
6. *Про інформацію : Закон України від 2 жовтня 1992 р. № 2657-XII. URL:https://zakon.rada.gov.ua/go/2657-12 (дата звернення: 23.11.2024).*

7. *Про соціальний і правовий захист військовослужбовців та членів їх сімей : Закон України від 20 грудня 1991 р. № 2011-XII. URL:https://zakon.rada.gov.ua/go/2011-12 (дата звернення: 23.11.2024).*
8. *Про затвердження Порядку обробки і захисту персональних даних у Міністерстві оборони України : Наказ Міністерства оборони України від 26 грудня 2014 р. № 926. URL:https://zakon.rada.gov.ua/go/z0071-15 (дата звернення: 23.11.2024).*
9. *Конвенція про захист прав людини і основоположних свобод : Конвенція Ради Європи від 4 листопада 1950 р. URL:https://zakon.rada.gov.ua/go/995_004 (дата звернення: 23.11.2024).*
10. *Рішення Європейського суду з прав людини у справі «М.К. проти України» від 15 грудня 2022 р. URL:https://hudoc.echr.coe.int/eng?i=001-219198 (дата звернення: 23.11.2024).*
11. *Рішення Європейського суду з прав людини у справі «Суріков проти України» від 26 квітня 2017 р. URL: https://hudoc.echr.coe.int/fre?i=001-192315 (дата звернення: 23.11.2024).*
12. *Топ виклики та рішення в розробці ПЗ для охорони здоров'я |Stfalcon. Custom Software Development Company | Stfalcon.com. URL:https://stfalcon.com/uk/blog/post/key-challenges-in-healthcare?utm_source=chatgpt.com (дата звернення: 23.11.2024).*

Тетяна БЛАЩУК. Забезпечення конфіденційності медичної інформації при наданні медичної допомоги військовослужбовцям та військовозобов'язаним

Стаття присвячена дослідженню питань забезпечення конфіденційності медичної інформації військовослужбовців у контексті автоматизації процесів обробки персональних даних. Метою роботи є аналіз нормативно-правових засад, визначення ключових викликів і розробка практичних рекомендацій для вдосконалення захисту медичних даних в умовах сучасних технологічних змін. Методологія дослідження базується на комплексному підході, який включає аналіз національного законодавства, міжнародних стандартів, практики використання автоматизованих систем і відповідних судових рішень.

Особлива увага приділена викликам, що виникають під час впровадження автоматизованих систем, таких як Єдиний державний реєстр призовників, військовозобов'язаних та резервістів «Оберіг». Серед основних проблем — ризики несанкціонованого доступу, порушення конфіденційності та можливі кіберзагрози. Досліджено роль сучасних технологій, таких як шифрування, багаторівнева автентифікація, захищені канали передачі даних і автоматичний моніторинг систем, у забезпеченні безпеки інформації.

На основі отриманих результатів запропоновано рекомендації щодо обмеження доступу до даних лише уповноваженим особам, впровадження регулярного аудиту систем обробки даних і посилення відповідальності за порушення

конфіденційності. Підкреслено важливість прозорості процедур обробки даних та інтеграції механізмів громадського контролю для зміцнення довіри громадян.

Результати дослідження акцентують на необхідності забезпечення балансу між національною безпекою та правами громадян на конфіденційність. Інтеграція сучасних технологій у систему державного управління дозволить ефективно вирішувати сучасні виклики, зберігаючи демократичні цінності. Запропоновані заходи є основою для подальшого вдосконалення підходів до захисту персональних даних у військовій сфері.

Ключові слова: права людини, повага до приватного життя, конфіденційність медичної інформації, автоматизація обробки даних, військовослужбовці, захист персональних даних, інформаційна безпека, шифрування, багаторівнева автентифікація, моніторинг, прозорість процедур, кіберзагрози.

Tetiana BLASHCHUK. Ensuring the confidentiality of medical information in providing medical care to military personnel and conscripts

The article focuses on the issues of ensuring the confidentiality of medical information for military personnel in the context of automated personal data processing. The purpose of the study is to analyze the legal framework, identify key challenges, and develop practical recommendations for improving the protection of medical data amidst modern technological advancements. The research methodology is based on a comprehensive approach that includes an analysis of national legislation, international standards, the practical use of automated systems, and relevant court decisions.

Special attention is given to the challenges arising from the implementation of automated systems, such as the Unified State Register of Conscripts, Reservists, and Military Obligated Persons «Oberig.» Key issues include risks of unauthorized access, breaches of confidentiality, and potential cybersecurity threats. The study explores the role of modern technologies, such as encryption, multi-factor authentication, secure data transmission channels, and automatic system monitoring, in ensuring information security.

Based on the findings, the article proposes recommendations for limiting data access to authorized personnel, implementing regular audits of data processing systems, and enhancing accountability for breaches of confidentiality. The importance of transparent data processing procedures and the integration of public oversight mechanisms is emphasized to strengthen citizens' trust.

The research results highlight the need to balance national security interests with citizens' rights to confidentiality. The integration of modern technologies into state governance systems will effectively address current challenges while preserving democratic values. The proposed measures provide a foundation for further improvement of approaches to protecting personal data in the military sector.

Keywords: human rights, respect for privacy, confidentiality of medical information, automated data processing, military personnel, personal data protection, information security, encryption, multi-factor authentication, monitoring, transparency of procedures, cybersecurity threats.