

УДК 342.5

DOI <https://doi.org/10.24144/2307-3322.2025.90.3.31>

ІНФОРМАЦІЙНА БЕЗПЕКА У МЕДИЧНІЙ СФЕРІ У ПЕРІОД ПРАВОВОГО РЕЖИМУ ВОЄННОГО СТАНУ

Кобрусева Є.А.,
*докторка юридичних наук, професор,
професор кафедри адміністративного і кримінального права
Дніпровського національного університету імені Олеся Гончара*

Кобрусева Є.А. Інформаційна безпека у медичній сфері у період правового режиму воєнного стану.

У статті окреслено особливості обміну та захисту медичної інформації між державними електронними інформаційними системами у період введення у країні правового режиму воєнного стану, розглянуто порядок дотримання вимог законодавчих норм при передачі медичної інформації між медичними закладами, військовими частинами, ТЦК та СП, телемедичними платформами. Проаналізовано ст. 24-2 Закону України «Основи законодавства про охорону здоров'я» у частині, що стосується взаємодії між електронними медичними системами та окремими державними реєстрами. Констатовано, що під час зазначеної взаємодії доступ до медичної інформації не допускається. Досліджено основні норми проєкту Закону України «Про внесення змін до Закону України «Про військовий обов'язок і військову службу» щодо створення та функціонування Єдиного державного реєстру військовослужбовців та до інших законів України щодо удосконалення порядку ведення військового обліку» щодо надання доступу до медичної інформації (про результати медичних оглядів, що проводяться з метою визначення придатності до виконання військового обов'язку) Міністерству оборони України для подальшого внесення до Єдиного державного реєстру призовників, військовозобов'язаних та резервістів з метою забезпечення національної безпеки та оборони. Розглянуто особливості надання інформації медичними закладами на запити військових частин, ТЦК. Констатовано, що надання медичної інформації про військовослужбовців медичним закладом можливе за умов наявності законних підстав та інформованої згоди. Визначено сутність поняття «інформована згода пацієнта» у вітчизняному та міжнародному законодавстві. Проаналізовано постанову Тернопільського апеляційного суду у справі № 607/17453/22 від 09.08.2023 щодо розголошення конфіденційної інформації про нього представниками клінічної лікарні у період дії в країні правового режиму воєнного стану. Розглянуто особливості захисту медичної інформації під час консультування, діагностики та надання медичної допомоги за допомогою телемедичних платформ. Теоретично обґрунтовано, що наразі проблемними залишаються питання щодо захисту інформації під час їх передачі між інформаційними та телемедичними системами, а також дотримання користувачами медичних інформаційних систем та телемедичних платформ законодавчих норм у частині щодо технічного захисту такого роду інформації.

Ключові слова: медична інформація, технічний захист, кібербезпека, електронні інформаційні системи, телемедичні платформи, захищені канали зв'язку.

Kobrusseva E.A. Information security in the medical sphere during the legal regime of martial state.

The article outlines the features of the exchange and protection of medical information between state electronic information systems during the period of the introduction of the legal regime of martial law in the country, considers the procedure for complying with the requirements of legislative norms when transferring medical information between medical institutions, military units, CCC and SP, telemedical platforms. Analyzes Art. 24-2 of the Law of Ukraine «Fundamentals of Healthcare Legislation» in the part that concerns the interaction between electronic medical systems and individual state registers. It is stated that during the specified interaction, access to medical information is not allowed. The main provisions of the draft Law of Ukraine “On Amendments to the Law of Ukraine “On Military Duty

and Military Service” regarding the creation and functioning of the Unified State Register of Military Personnel and other laws of Ukraine regarding the improvement of the procedure for maintaining military records” regarding the provision of access to medical information (on the results of medical examinations conducted to determine suitability for military duty) to the Ministry of Defense of Ukraine for further inclusion in the Unified State Register of Conscripts, Military Conscripts and Reservists in order to ensure national security and defense were examined. The features of the provision of information by medical institutions at the request of military units and the Central Military District were considered. It was theoretically substantiated that the provision of medical information about military personnel by a medical institution is possible provided that there are legal grounds and informed consent. The essence of the concept of “patient informed consent” in domestic and international legislation was determined. The resolution of the Ternopil Court of Appeal in case No. 607/17453/22 dated 09.08.2023 regarding the disclosure of confidential information about him by representatives of a clinical hospital during the period of martial law in the country has been analyzed. The features of protecting medical information during consultation, diagnostics and provision of medical care using telemedical platforms have been considered. It is theoretically substantiated that currently the issues of information protection during its transfer between information and telemedical systems, as well as compliance by users of medical information systems and telemedical platforms with legislative norms regarding the technical protection of this type of information, remain problematic.

Key words: medical information, technical protection, cybersecurity, electronic information systems, telemedical platforms, protected communication channels.

Постановка проблеми. Наразі в Україні, з урахуванням перебування країни в умовах правового режиму воєнного стану, актуалізувалося питання щодо удосконалення системи інформаційної безпеки у медичній сфері. І це стосується як забезпечення конфіденційності даних пацієнтів, безпечного зв'язку між медичними закладами, військовими частинами, ТЦК та СП, так і захисту медичних систем від кібератак та інших загроз.

Тобто з одного боку необхідно забезпечити захист медичної інформації під час обміну даними для надання своєчасної та ефективної допомоги, з іншого – забезпечити захист персональних даних пацієнтів (військових) від несанкціонованого доступу, використання чи розголошення. Як бачимо, питання щодо передачі медичної інформації під час активних бойових дій у країні є досить актуальним і потребує дослідження.

Метою дослідження є аналіз особливостей обміну та захисту інформації між державними електронними інформаційними та телемедичними системами у період введення у країні правового режиму воєнного стану, законодавчих актів, які затверджено останнім часом, окреслення проблематики у даному напрямі.

Стан опрацювання проблематики. Питанням щодо захисту та особливостей обміну інформації між електронними системами у своїх наукових працях приділяли увагу Я. Бабенко, Г. Білінова, І. Котерлін, І. Пономаренко, Я. Сенюта, Р. Стефанчук, Х. Терешко, С. Тернова, О. Трофименко та інші. Проте повномасштабне вторгнення країни-агресора на територію України, активні бойові дії, мобілізація громадян внесли свої корективи у чинне законодавство, яке регламентує зазначений напрям, окреслили проблематику, яка потребує негайного вирішення та, з урахуванням, актуальності, удосконалення.

Виклад основного матеріалу. Повномасштабне вторгнення на Україну країни-агресора виявило проблематику щодо захисту медичної інформації. У першу чергу це стосується захисту електронних медичних систем від кібератак, а також взаємодії з іншими державними реєстрами.

Акценти на виявлення інформаційних загроз у медичній сфері в умовах активних бойових дій в Україні, – зазначає І.Б. Котерлін, – змінюються у напрямі звуження прав людини, керуючись необхідністю забезпечення впливу на потенційні та існуючі загрози [1]. Що стосується вимог, передбачених Законом України «Про захист інформації в інформаційно-комунікаційних системах», то під час введення в країні правового режиму воєнного стану, вони не змінюються.

Частиною 5 статті 24-2 Закону України «Основи законодавства про охорону здоров'я» від 19.11.1992 № 2801-ХІІ визначено, що взаємодія між електронними медичними системами, Єдиним державним демографічним реєстром, Державним реєстром актів цивільного стану громадян та Державним реєстром фізичних осіб-платників податків здійснюється у встановленому законом порядку, з використанням єдиної інформаційної системи МВС України, з дотриманням вимог

Закону України «Про захист персональних даних» [2]. Разом з тим, законом передбачено, що під час зазначеної взаємодії доступ до медичної інформації не допускається.

Слід зазначити, що у вересні 2024 року розроблено проєкт Закону України «Про внесення змін до Закону України «Про військовий обов'язок і військову службу» щодо створення та функціонування Єдиного державного реєстру військовослужбовців та до інших законів України щодо удосконалення порядку ведення військового обліку», яким запропоновано внести зміни до абзацу 11 статті 24-2 Закону України «Основи законодавства про охорону здоров'я» у частині щодо надання доступу до медичної інформації (про результати медичних оглядів, що проводяться з метою визначення придатності до виконання військового обов'язку) Міністерству оборони України для подальшого внесення до Єдиного державного реєстру призовників, військовозобов'язаних та резервістів з метою забезпечення національної безпеки та оборони [3]. Також надано пропозиції щодо розроблення функціоналу Електронної системи охорони здоров'я (ЕСОЗ), який надасть можливість взаємодіяти з Єдиним державним реєстром призовників, військовозобов'язаних та резервістів «Оберіг» (централізована система, яка зберігає та аналізує інформацію про стан здоров'я громадян України).

Зазначимо, що ЕСОЗ – багатокомпонентна система, яка має атестат відповідності КСЗІ, до якої залучається кілька сторін та учасників (пацієнти, медичні заклади, медичні інформаційні системи). Архітектуру ЕСОЗ розроблено таким чином, що медична інформація про пацієнта зберігається відокремлено у різних кластерах ЦБД (забезпечено підвищені вимоги до кібербезпеки – обмежено доступ, спеціалізована система захисту, посилання на пацієнта деперсоніфіковане, передача відомостей здійснюється у зашифрованому виді згідно з нормами законів з криптографічного та технічного захисту інформації), що сприяє мінімізації витоку інформації [4].

Слід зазначити, що 18 червня 2025 року Верховною Радою України цей проєкт було ухвалено, відповідно після набуття його чинності, суттєво спроститься процес доступу державних органів (ТЦК) до відомостей про медичний стан населення, що передбачає автоматичну оцінку придатності громадян до військової служби. Медична інформація (результати обстежень, дані про хронічні захворювання, перенесені травми, інші медичні показники), які можуть впливати на придатність до військової служби про стан здоров'я осіб автоматично передаватиметься з медичних установ до реєстру. Процес передачі даних передбачає автоматичну інтеграцію з базами даних медичних установ. Інформація передаватиметься за наступним алгоритмом: медичні організації підключаються до системи, забезпечуючи передачу даних про пацієнтів у цифровому форматі; на основі зібраних даних система автоматично класифікує громадян, визначаючи їх стан здоров'я та можливість проходження служби. Слід зазначити, що доступ реєстру буде надаватися виключно уповноваженим органам.

Крім того, медична інформація про результати медичних оглядів, що проводяться з метою визначення придатності до виконання військового обов'язку, передаватиметься з реєстрів ЕСОЗ до «Оберіг» через національну систему електронної взаємодії між державними інформаційними ресурсами, електронними реєстрами, інформаційними системами «Трембіта» (сучасне організаційно-технічне рішення щодо забезпечення безпечної інформаційної міжвідомчої взаємодії між органами державної влади, органами місцевого самоврядування та суб'єктами господарювання через інтернет шляхом обміну електронними повідомленнями між їх інформаційними системами. Основу даної системи становить удосконалена естонська платформа обміну даними X-ROAD, яка є фундаментом естонського цифрового суспільства) [5].

Разом з тим, ухвалення зазначеного Закону викликало як позитивні (завдяки цифровізації спроститься процедура), так і негативні (потенційне зловживання медичними даними, витік інформації) відгуки. Як зазначають експерти з інформаційної безпеки, успіх нової системи залежить від прозорості її впровадження та суворого дотримання норм законодавства щодо захисту персональних даних.

Наступним актуальним наразі є питання щодо надання інформації медичними закладами на запити військових частин. Військові частини наразі мають обмежений доступ до медичної інформації, так як вона є конфіденційною, і її заборонено надавати без згоди пацієнта, проте в окремих випадках (необхідно для забезпечення безпеки, бойової готовності або виконання військових обов'язків), військове командування може отримати до неї доступ. Тобто у разі, якщо військова частина вимагає медичну інформацію про військовослужбовця, медичний заклад повинен перевірити, чи є законні підстави для надання такої інформації та чи отримана згода пацієнта.

Звертаючись до поняття «інформована згода пацієнта» зазначимо, що воно передбачене Конституцією України «Жодна людина без її вільної згоди не може бути піддана медичним дослідженням [6]», Цивільним кодексом України – медична допомога надається за умови згоди пацієнта [7], Законом України «Основи законодавства про охорону здоров'я» – «для застосування методів діагностики, профілактики та лікування необхідна згода інформованого пацієнта. Інформування включає надання достовірних відомостей про стан здоров'я, ознайомлення з медичними документами, що стосуються його здоров'я [2].

Крім того, статтею 5 глави II Конвенції про захист прав і гідності людини щодо застосування біології та медицини (Конвенція Ов'єдо) – будь-яке втручання у сферу здоров'я здійснюється лише за умови її добровільної та свідомої згоди або ж у разі надзвичайної ситуації [8]. Статтею 8 зазначеної вище Конвенції визначено, що до надзвичайних ситуацій відносять стихійні лиха, за яких лікар не має об'єктивної можливості отримати належної згоди у пацієнта; неможливість поінформувати законного представника, який мав би дозволити термінове втручання; перебування пацієнта у комі та інші. Особі завчасно сповіщають про мету втручання, наслідки та ризики. Крім того, зазначену згоду особа може відкликати у будь-який час [8].

Як бачимо, законодавчо норми щодо інформованої згоди пацієнта чітко окреслено як вітчизняними, так міжнародними актами. Разом з тим, не завжди їх можна застосувати у час активних бойових дій – під час евакуації поранених, надання допомоги у стабілізаційних центрах, ургентних випадках у госпіталях, де окремі вимоги законодавства, з метою збереження життя військового, переходять на «другий план». Адже поранені не завжди перебувають у стані свідомості, практично відсутня можливість також отримати згоду їх рідних.

У даному випадку, якщо Конвенцією допускається втручання у приватність на підставі норм закону, то вітчизняним законодавством передбачено «наявність ознак загрози життю», «невідкладні випадки». Це дещо спрощує ситуацію, проте відсутність їх чіткого переліку надає можливість їх різностороннього трактування, як наслідок, це може призвести до порушення прав людини.

Продовжуючи аналіз, зазначимо, що статтею 3 Указу Президента України «Про введення воєнного стану в Україні» визначено, що із введенням в Україні воєнного стану тимчасово, можуть бути обмежені конституційні права (статті 30, 34, 38, 39, 41 44, 53 Конституції України) та, у межах та обсязі, законні інтереси осіб, необхідні для забезпечення та здійснення заходів правового режиму воєнного стану (ч. 1 ст. 8 Закону України «Про правовий режим воєнного стану») [9; 10].

Розглянемо, як приклад, постанову Тернопільського апеляційного суду у справі № 607/17453/22 від 09.08.2023. Позивач звернувся за фактом розголошення конфіденційної інформації про нього представниками клінічної лікарні. За результатами розгляду матеріалів встановлено, що позивач звернувся до реєстратури Клінічної лікарні з метою отримання консультації у лікаря-гематолога. Завідуюча лікарні, керуючись наказом Департаменту охорони здоров'я ТОВА від 10.03.2022 № 339/11-06, яким передбачено, що у період введення воєнного стану проведення планової госпіталізації військовозобов'язаних чоловічої статі віком від 18 до 60 років здійснюється виключно за направленням районних (міських) ТЦК та СП та їх відділів, а в ургентних випадках з обов'язковим негайним інформуванням по телефону чергових районних (міських) ТЦК та СП та їх відділів та документальним підтвердженням протягом доби, проінформувала голову ВЛК обласного ЦК та СП про факт звернення позивача [11].

Судом першої інстанції позовні вимоги були задоволені частково з посиланням на те, що факт звернення Позивача за медичною допомогою відноситься до конфіденційної інформації про нього, відповідно, не допускається її розкриття (поширення) без його згоди. Дії посадових осіб неправомірними.

Суд апеляційної інстанції за результатами розгляду матеріалів дійшов висновку, що у період воєнного стану таке втручання Відповідача у право Позивача на нерозголошення таємниці про факт його звернення за медичною допомогою і повідомлення працівником відповідача про це голову ВЛК обласного ЦК та СП відповідало законній меті та необхідне, так як спрямоване на захист інтересів національної безпеки України та здійснено згідно із вимогами статей 32, 64 Конституції України, ст. 1 Закону України «Про правовий режим воєнного стану», ст. 3 Указу Президента України «Про введення воєнного стану в Україні» [11].

Наступним питанням, яке потребує розгляду, є захист медичної інформації під час консультування, діагностики та надання медичної допомоги за допомогою телемедичних платформ, адже у

воєнний час вони відіграють важливу роль у наданні медичної допомоги, особливо у віддалених районах або в умовах обмеженого доступу до лікарів. Дана процедура передбачена наказами МОЗ України «Про затвердження нормативних документів щодо застосування телемедицини у сфері охорони здоров'я» від 19.10.2015 № 681 та «Про організацію надання медичної допомоги із застосуванням телемедицини в умовах воєнного стану» від 20.06.2022 № 1062. З часу повномасштабного вторгнення країни-агресора на територію України, реалізовано 7 гуманітарних проєктів, до якого залучено 304 медичні заклади, 1024 медики пройшли відповідну підготовку. Разом з тим, для того, щоб лікарю оперативно надати консультацію, провести діагностику та лікування необхідно забезпечити швидкий доступ та, у разі необхідності, обмін інформацією, що передбачає відповідний її технічний захист від несанкціонованого доступу при використанні телекомунікаційних мереж. З метою запобігання витоку та несанкціонованого доступу до такого роду інформації, розробниками передбачено: доступ до неї лише уповноважених осіб, шифрування, передача захищеними каналами зв'язку, застосування телемедичних платформ, які відповідним чином сертифіковані.

Висновок. Підсумовуючи, зазначимо, що незважаючи на те, що Україна наразі перебуває в умовах правового режиму воєнного стану, у законодавство своєчасно вносяться зміни щодо удосконалення механізму захисту медичної інформації в електронних медичних системах, порядку взаємодії між медичними інформаційними системами та державними реєстрами, військовими частинами, ТЦК та СП, а також медичними закладами (удосконалено ст. 24-2 Закону України «Основи законодавства про охорону здоров'я», функціонал Електронної системи охорони здоров'я, ухвалено проєкт Закону України «Про внесення змін до Закону України «Про військовий обов'язок і військову службу», яким передбачено автоматичну інтеграцію з базами даних медичних установ та «Оберегом»).

Разом з тим, проблемними залишаються питання щодо: захисту інформації під час її передачі між інформаційними та телемедичними системами; отримання інформованої згоди пацієнта на доступ до медичної інформації (якщо Конвенцією про захист прав і гідності людини щодо застосування біології та медицини допускається втручання у приватність на підставі норм закону, то вітчизняним законодавством це можливо лише за умови наявності ознак загрози життю людини чи у невідкладних випадках, чіткий перелік яких відсутній, що надає можливість їх різностороннього трактування, як наслідок, це може призвести до порушення прав людини); захист медичної інформації під час консультування, діагностики та надання медичної допомоги за допомогою телемедичних платформ, а також дотримання користувачами медичних інформаційних систем законодавчих норм щодо технічного захисту такого роду інформації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Котерлін І.Б. Інформаційна безпека в умовах воєнного стану у аспекті забезпечення інформаційних прав та свобод. *Актуальні проблеми вітчизняної юриспруденції*. 2022. № 1. С. 150.
2. Основи законодавства про охорону здоров'я: Закон України від 19.11.1992 № 2801-XII. URL: https://zakon.rada.gov.ua/laws/show/2801-12?find=1&text=інформаційна+взаємодія+між+електронною#w4_1.
3. Про внесення змін до Закону України «Про військовий обов'язок і військову службу щодо створення та функціонування Єдиного державного реєстру військовослужбовців та до інших законів України щодо удосконалення порядку ведення військового обліку»: проєкт Закону України від 24.09.2024 № 12066. URL: [blob:https://itd.rada.gov.ua/609c87f0-9369-4370-815e-ca5457eda812](https://itd.rada.gov.ua/609c87f0-9369-4370-815e-ca5457eda812).
4. Тернова С. Безпека даних в ECO3: ризики під час війни та як їх усунути. URL: <https://thepharma.media/uk/business/35453-bezpeka-danix-v-esoz-riziki-pid-cas-viini-ta-yak-yix-uniknuti-01082024>.
5. Система електронної взаємодії державних електронних інформаційних ресурсів <https://se.dii.gov.ua/trembita>.
6. Конституція України від 28 червня 1996 року. *Відомості Верховної Ради України*. 1996. № 30. Ст. 43. URL: <http://zakon3.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80>.
7. Цивільний кодекс України: Закон України від 16.01.2003 р. № 435-IV (у редакції від 30.01.2024). *Відомості Верховної Ради України*. 2003. № 40. Ст. 356.

8. Конвенція про захист прав і гідності людини щодо застосування біології та медицини від 04.04.1997. URL: https://zakon.rada.gov.ua/laws/show/994_334#Text.
9. Про введення воєнного стану в Україні: Указ Президента України від 24.02.2022 № 62/2022. URL: <https://www.president.gov.ua/documents/642022-41397>.
10. Про правовий режим воєнного стану: Закон України від 12.05.2015 № 389-VIII. URL: zakon.rada.gov.ua/laws/show/389-19.
11. Бабенко Я. Втручання у право пацієнта на нерозголошення таємниці про факт його звернення за медичною допомогою. URL: <https://www.hsa.org.ua/blog/vtrucannia-u-pravo-pacijenta-na-nerozgolosennia-tajemnici-pro-fakt-iogo-zvernennia-za-medicinoiu-dopomogoiu>.