ПРОБЛЕМИ КРИМІНАЛЬНОГО ПРАВА ТА КРИМІНОЛОГІЇ

УДК 343.35:355.1(477)
DOI https://doi.org/10.32850/LB2414-4207.2026.43.24

НЕСАНКЦІОНОВАНА ЗМІНА ІНФОРМАЦІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ ОСОБОЮ, ЯКА МАЄ ПРАВО ДОСТУПУ, ЯК СПОСІБ ПОРУШЕННЯ ЗАКОНОДАВСТВА ПРО ОБОРОНУ, МОБІЛІЗАЦІЙНУ ПІДГОТОВКУ ТА МОБІЛІЗАЦІЮ

Григоращенко Олександр Вікторович,
orcid.org/0009-0006-8934-5401
доктор філософії у галузі знань з права

У статті здійснено науковий аналіз протиправної діяльності, пов'язаної з несанкціонованою зміною інформації, яка оброблюється в електронно-обчислювальних машинах, автоматизованих та інформаційно-комунікаційних системах, особою, яка має право доступу до такої інформації. Особливу увагу приділено випадкам, коли такі дії вчиняються у сфері ведення військового обліку, функціонування Єдиного державного реєстру призовників, військовозобов'язаних та резервістів, а також реалізації законодавства про оборону, мобілізаційну підготовку та мобілізацію. Обґрунтовано, що в умовах збройної агресії проти України та дії правового режиму воєнного стану достовірність відомостей у відповідних реєстрах набуває не лише адміністративно-організаційного, а й безпекового значення, оскільки безпосередньо впливає на облік мобілізаційних ресурсів, проведення мобілізаційних заходів і здатність держави належно реагувати на зовнішню загрозу.

Визначено, що несанкціонована зміна інформації в автоматизованих системах, вчинена уповноваженою особою з використанням персонального доступу, може створювати умови для ухилення військовозобов'язаних від виконання військового обов'язку, зокрема через внесення недостовірних відомостей про адміністративне правопорушення, проходження військово-лікарської комісії, перебування в розшуку або інші обставини, що мають юридичне значення. Доведено необхідність кримінально-правової оцінки таких діянь не лише як порушення правил обігу інформації, а й як посягання на встановлений порядок мобілізаційної підготовки, авторитет державних органів, службову дисципліну та довіру до цифрових реєстрів. Запропоновано розглядати ефективну протидію таким правопорушенням як комплексний процес, що охоплює належну правову кваліфікацію, документування цифрових слідів, внутрішній контроль у територіальних центрах комплектування та соціальної

© Григоращенко О. В., 2026
Стаття поширюється на умовах ліцензії відкритого доступу (CC BY 4.0)

підтримки, міжвідомчу взаємодію і персональну відповідальність осіб, які мають доступ до реєстрів.

Ключові слова: мобілізаційна підготовка та мобілізація, воєнний стан, військовий облік, Єдиний державний реєстр призовників, військовозобов'язаних та резервістів, АІТС «Оберіг», несанкціонована зміна інформації, автоматизована система, особа, яка має право доступу, територіальний центр комплектування та соціальної підтримки, кримінально-правова кваліфікація.

UNAUTHORIZED MODIFICATION OF INFORMATION IN AUTOMATED SYSTEMS BY A PERSON WITH ACCESS RIGHTS AS A METHOD OF VIOLATING LEGISLATION ON DEFENSE, MOBILIZATION TRAINING AND MOBILIZATION

Grigorashchenko Oleksandr Viktorovych,
orcid.org/0009-0006-8934-5401
Doctor of Philosophy in Law

The article provides a scientific analysis of illegal activity related to the unauthorized modification of information processed in electronic computers, automated systems and information-communication systems by a person who has lawful access to such information. Particular attention is paid to cases where such actions are committed in the field of military registration, the functioning of the Unified State Register of Conscripts, Persons Liable for Military Service and Reservists, and the implementation of legislation on defense, mobilization training and mobilization. The article substantiates that, under armed aggression against Ukraine and the legal regime of martial law, the reliability of data in the relevant registers acquires not only administrative and organizational but also security significance, because it directly affects the accounting of mobilization resources and the ability of the state to respond properly to external threats.

It is determined that unauthorized modification of information in automated systems by an authorized person using personal access credentials may create conditions for evasion of military duty by persons liable for military service, in particular through entering inaccurate data on administrative offenses, medical examination, search status or other legally significant circumstances. The necessity of criminal-law assessment of such acts is justified not only as a violation of the rules of information circulation, but also as an encroachment on the established procedure of mobilization preparation, the authority of state bodies, official discipline and trust in digital registers. Effective counteraction to such offenses should include proper legal qualification, documentation of digital traces, internal control in territorial recruitment and social support centers, interagency cooperation and personal liability of persons who have access to registers.

Key words: mobilization training and mobilization, martial law, military registration, Unified State Register of Conscripts, Persons Liable for Military Service and Reservists, AITS "Oberig", unauthorized modification of information, automated system, person with access rights, territorial recruitment and social support center, criminal-law qualification.

Постановка проблеми. Повномасштабна збройна агресія проти України зумовила суттєве зростання значення мобілізаційних ресурсів, стабільності військового обліку та належного функціонування органів, уповноважених на реалізацію заходів оборони, мобілізаційної підготовки і мобілізації. У таких умовах інформація про призовників, військовозобов'язаних та резервістів перестає бути лише обліково-адміністративним масивом даних. Вона набуває значення елементу оборонної спроможності держави, оскільки використовується для планування мобілізаційних заходів,

визначення правового статусу особи, організації виклику, проходження військово-лікарської комісії, взяття на військовий облік, зняття з нього або зміни відповідних облікових даних [1; 2; 11].

Особливу небезпеку становлять ситуації, коли особа, яка має правомірний доступ до автоматизованої системи, використовує його всупереч службовому призначенню і без належної документальної підстави змінює відомості у відповідному реєстрі. Такий спосіб протиправної поведінки складний для виявлення, оскільки зовні може мати вигляд звичайної службової операції, виконаної користувачем із належними повноваженнями. Проте фактичний зміст таких дій полягає у порушенні цілісності, достовірності та правового значення інформації, яка використовується державою для забезпечення військового обліку та проведення мобілізаційних заходів [10; 11; 16].

Проблема ускладнюється тим, що несанкціонована зміна інформації в Єдиному державному реєстрі призовників, військовозобов'язаних та резервістів або в пов'язаних із ним інформаційних системах може мати похідні правові наслідки: скасування або зміну відомостей про розшук у зв'язку з мобілізацією, створення уявних підстав для зміни статусу військовозобов'язаного, направлення на військово-лікарську комісію, уникнення притягнення до адміністративної відповідальності або інше фактичне сприяння ухиленню від виконання військового обов'язку. Саме тому такі діяння потребують не лише технічної перевірки дій користувача реєстру, а й комплексної кримінально-правової та криміналістичної оцінки [15; 16; 17; 18].

Актуальність теми також визначається корупційним і латентним потенціалом зазначених правопорушень. Доступ до реєстрів, службова обізнаність, знання процедур військового обліку і мобілізації створюють підвищені ризики використання службового становища для формування штучних підстав уникнення мобілізаційних заходів. У результаті шкода заподіюється не лише конкретним адміністративним або інформаційним відносинам, а й довірі до цифрових інструментів держави, дисципліні у системі військового управління, принципу рівності виконання військового обов'язку та загальній обороноздатності України.

Аналіз останніх досліджень і публікацій. Питання кримінально-правової охорони встановленого порядку несення військової служби, відповідальності за ухилення від військового обов'язку, службових правопорушень у сфері військового управління та захисту інформації в автоматизованих системах розглядалися у працях багатьох українських дослідників. У науковій літературі увага приділяється як загальним засадам кримінальної відповідальності за військові та службові кримінальні правопорушення, так і особливостям кваліфікації діянь, пов'язаних із підробленням документів, зловживанням повноваженнями та використанням цифрових систем у протиправних цілях.

З урахуванням предмета цієї статті особливе значення мають праці, у яких розглядаються конституційні засади військового обов'язку та заходи попередження ухилення від його реалізації [20, с. 83–88], а також поняття військової служби і заходи запобігання ухиленню від неї [21, с. 306–308].

Водночас сучасні умови воєнного стану актуалізували новий аспект цієї проблематики: використання автоматизованих систем військового обліку не як нейтрального технічного інструменту, а як потенційного способу прихованого впливу на мобілізаційний статус особи. Саме поєднання службового доступу, цифрової форми обліку, значного масиву персональних і службових даних та високої суспільної значущості мобілізаційних процедур створює нову площину для кримінально-правового аналізу. Попри наявність досліджень щодо ухилення від військової служби, службового підроблення та кіберзлочинності, питання несанкціонованої зміни даних у Реєстрі

«Оберіг» особою, яка має право доступу, потребує окремого наукового осмислення з урахуванням норм законодавства про оборону, мобілізацію, інформацію, персональні дані та кримінальну відповідальність.

Мета статті. Метою статті є науковий аналіз механізму вчинення протиправної діяльності, пов'язаної з несанкціонованою зміною інформації в автоматизованих системах особою, яка має право доступу до такої інформації, у контексті можливого порушення законодавства про оборону, мобілізаційну підготовку та мобілізацію, а також визначення кримінально-правових і криміналістичних орієнтирів для кваліфікації та документування відповідних діянь.

Виклад основного матеріалу. Правову основу аналізу становлять положення законодавства, яке визначає режим оборони держави, порядок запровадження та реалізації воєнного стану, виконання військового обов'язку, ведення військового обліку, функціонування інформаційних систем та відповідальність за несанкціоновані дії з інформацією. Відповідно до Закону України «Про оборону України» оборона держави охоплює систему політичних, економічних, соціальних, воєнних, наукових, інформаційних, правових та інших заходів щодо підготовки до збройного захисту і захисту України у разі збройної агресії або збройного конфлікту [1]. Закон України «Про правовий режим воєнного стану» визначає воєнний стан як особливий правовий режим, що вводиться у разі збройної агресії чи загрози нападу та передбачає надання відповідним органам додаткових повноважень, необхідних для відвернення загрози і забезпечення національної безпеки [2].

Запровадження воєнного стану в Україні Указом Президента України від 24 лютого 2022 року № 64/2022, затвердженим відповідним законом, створило правові передумови для особливого режиму реалізації низки конституційних прав і виконання обов'язку захисту Вітчизни [3; 4]. При цьому обмеження окремих прав у період воєнного стану не скасовує вимог законності, обґрунтованості, пропорційності та належної процедури. Це має принципове значення для оцінки дій посадових осіб, які працюють із реєстрами військового обліку: навіть за умов особливого періоду вони зобов'язані діяти виключно на підставі, у межах повноважень та у спосіб, визначені законом.

Закон України «Про військовий обов'язок і військову службу» та Закон України «Про мобілізаційну підготовку та мобілізацію» формують нормативну основу виконання громадянами військового обов'язку, організації військового обліку та проведення мобілізаційних заходів [5; 6]. Своєю чергою територіальні центри комплектування та соціальної підтримки відповідно до Положення, затвердженого постановою Кабінету Міністрів України від 23 лютого 2022 року № 154, є органами військового управління, на які покладається виконання законодавства з питань військового обов'язку і військової служби, мобілізаційної підготовки та мобілізації, керівництво військовим обліком і проведення відповідних заходів в особливий період [7].

У межах зазначеної системи особливого значення набуває достовірність інформації, що обробляється у цифрових реєстрах. Закон України «Про інформацію» визначає інформацію як будь-які відомості або дані, які можуть бути збережені на матеріальних носіях чи відображені в електронному вигляді, а також закріплює правовий режим інформації з обмеженим доступом [8]. Закон України «Про доступ до публічної інформації» конкретизує види інформації з обмеженим доступом та умови обмеження доступу до неї [9]. Для військового обліку ці положення мають прикладне значення, оскільки відповідні реєстри містять персональні та службові відомості, обробка яких допускається лише у визначених законом межах.

Закон України «Про захист інформації в інформаційно-комунікаційних системах» визначає інформаційну систему як організаційно-технічну систему, у якій

реалізується технологія обробки інформації з використанням технічних і програмних засобів, та встановлює відповідальність за порушення законодавства про захист інформації в таких системах [10]. Отже, правовий режим автоматизованих систем охоплює не лише технічні вимоги до захисту даних, а й юридичний обов'язок уповноважених користувачів забезпечувати цілісність, достовірність і законність обробки інформації.

Центральне місце у сфері військового обліку посідає Єдиний державний реєстр призовників, військовозобов'язаних та резервістів. Відповідний закон визначає його як інформаційно-комунікаційну систему, призначену для збирання, зберігання, обробки і використання даних про призовників, військовозобов'язаних та резервістів з метою забезпечення військового обліку громадян України [11]. Основними засадами ведення Реєстру є обов'язковість і своєчасність внесення відомостей, повнота та актуалізація даних, захищеність від несанкціонованого доступу, зловживання доступом, незаконного використання відомостей і порушення цілісності бази даних. Саме ці засади визначають межі правомірної поведінки користувача системи.

Важливо підкреслити, що наявність у службової особи формального права доступу до Реєстру не означає наявності права довільно змінювати відомості у ньому. Правомірність кожної дії користувача має оцінюватися не лише через факт автентифікації або використання персонального ключа доступу, а й через наявність належної службової підстави, відповідність змісту внесеної інформації підтверджуючим документам, дотримання процедури та службової мети обробки даних. Якщо інформація змінюється без документального підтвердження, з порушенням встановленого порядку або з метою створення неправдивих юридичних наслідків, така дія втрачає службовий характер і набуває ознак протиправності [10; 11; 12].

З погляду службової дисципліни така поведінка також суперечить обов'язкам військовослужбовців та інших службових осіб, які діють у сфері військового управління. Статут внутрішньої служби Збройних Сил України і Дисциплінарний статут Збройних Сил України закріплюють вимоги сумлінного виконання службових обов'язків, дотримання законності, дисципліни, наказів командирів і правил службової поведінки [13; 14]. Тому несанкціоновані зміни відомостей у Реєстрі «Оберіг» можуть мати не лише кримінально-правовий, а й дисциплінарний та службово-організаційний вимір.

Порядок проведення призову громадян на військову службу під час мобілізації, на особливий період, затверджений постановою Кабінету Міністрів України від 16 травня 2024 року № 560, деталізує процедури організації мобілізаційних заходів, взаємодію суб'єктів та оформлення відповідних рішень [15]. Порядок організації та ведення військового обліку призовників, військовозобов'язаних та резервістів, затверджений постановою Кабінету Міністрів України від 30 грудня 2022 року № 1487, визначає, що військовий облік здійснюється з використанням даних Реєстру, а районні та міські територіальні центри комплектування та соціальної підтримки виконують функції з ведення такого обліку, актуалізації персональних і службових даних, а також внесення змін до відповідних відомостей [16].

Зазначені положення дозволяють зробити висновок, що внесення відомостей до Реєстру «Оберіг» має бути похідним від реальної юридичної події або належного документа. Наприклад, відомості про складення адміністративного протоколу, проходження військово-лікарської комісії, зміну місця проживання, взяття на облік чи зняття з нього мають ґрунтуватися на перевірених даних і відповідних документах. Внесення недостовірної інформації, навіть користувачем із законним доступом, порушує логіку функціонування Реєстру, адже створює помилковий правовий стан, на підставі якого інші посадові особи можуть ухвалювати наступні рішення.

Особливу увагу слід приділити адміністративно-правовому контексту. Стаття 210-1 Кодексу України про адміністративні правопорушення передбачає відповідальність за порушення законодавства про оборону, мобілізаційну підготовку та мобілізацію, зокрема за відповідні діяння, вчинені в особливий період [17]. Якщо в Реєстрі відображається інформація про складення адміністративного протоколу за відсутності фактичного оформлення такого документа уповноваженими посадовими особами, це створює викривлення юридичної реальності. Така зміна може спричинити автоматичне або подальше службове рішення, яке не відповідатиме фактичним обставинам.

Ілюстративною є ситуація, коли оператор відділення обліку мобілізаційної роботи районного територіального центру комплектування та соціальної підтримки, маючи доступ до Реєстру «Оберіг» і використовуючи персональний ключ доступу, без належних підтверджуючих документів вносить відомості про те, що щодо конкретного військовозобов'язаного нібито складено адміністративний протокол за порушення законодавства про оборону, мобілізаційну підготовку та мобілізацію. Унаслідок такої дії система або інший уповноважений користувач може скасувати розшук військовозобов'язаного у зв'язку з мобілізацією або створити передумови для подальшого ухилення від виконання військового обов'язку.

Науково коректною у такій ситуації є не автоматична презумпція наявності кримінального правопорушення, а послідовне встановлення всіх його ознак. Необхідно з'ясувати: чи мала особа право доступу до відповідної автоматизованої системи; які саме дії вона виконала; чи були ці дії дозволені її службовими повноваженнями; чи існували документи, що підтверджували правомірність зміни; який правовий наслідок спричинила зміна; чи усвідомлювала особа неправомірність своїх дій; чи був причинний зв'язок між зміною інформації та можливістю ухилення від мобілізаційних заходів.

Кримінально-правова кваліфікація подібних діянь передусім має здійснюватися з урахуванням статті 362 Кримінального кодексу України, яка передбачає відповідальність за несанкціоновані дії з інформацією, що оброблюється в електронно-обчислювальних машинах, автоматизованих системах або комп'ютерних мережах, вчинені особою, яка має право доступу до неї [18]. У цьому складі ключовим є саме поєднання двох обставин: наявність у суб'єкта права доступу і вихід за межі правомірного використання такого доступу. Отже, протиправність полягає не в самому факті входу до системи, а в несанкціонованому характері зміни, знищення, блокування, перекручення або іншого впливу на інформацію.

Водночас кваліфікація не повинна зводитися до формального посилання на статтю 362 КК України без аналізу фактичних обставин. Якщо несанкціонована зміна інформації супроводжується складанням або використанням неправдивого документа, зловживанням службовим становищем, одержанням неправомірної вигоди або умисним сприянням ухиленню від військового обов'язку, може постати питання про додаткову кримінально-правову оцінку за іншими нормами Кримінального кодексу України. При цьому конкуренція норм має вирішуватися з урахуванням безпосереднього об'єкта посягання, способу вчинення, форми вини, службового статусу особи та фактичного результату діяння [18].

Суб'єктивна сторона аналізованих діянь потребує особливої доказової уваги. У практичних ситуаціях може йтися як про прямий умисел, коли особа усвідомлює незаконність внесення даних і прагне створити неправдивий статус військовозобов'язаного, так і про злочинну самовпевненість або службову недбалість, якщо особа передбачає можливість настання шкідливих наслідків, але легковажно розраховує на їх відвернення або не перевіряє належним чином документальні підстави зміни.

Відмежування цих форм вини має вирішальне значення для правильної кваліфікації та індивідуалізації відповідальності.

Доказування у таких кримінальних провадженнях має поєднувати традиційні та цифрові джерела доказової інформації. До традиційних належать посадові інструкції, накази, журнали чергувань, документи військового обліку, матеріали адміністративного провадження, протоколи, направлення на військово-лікарську комісію, пояснення службових осіб і військовозобов'язаних. До цифрових джерел належать журнали доступу до Реєстру, електронні сліди авторизації, час і зміст змін, ідентифікатор користувача, IP-адреси, технічні логи, відомості про використання персонального ключа доступу, а також інформація про наступні автоматичні або ручні дії інших користувачів системи. Такі дані мають збиратися та перевірятися відповідно до вимог кримінального процесуального законодавства [19].

Криміналістично значущим є встановлення не лише факту зміни інформації, а й її функціонального значення для мобілізаційної процедури. Якщо внесена інформація фактично скасувала розшук, змінила статус особи, відкрила можливість проходження певної процедури або створила перешкоди для притягнення до відповідальності, така зміна має розглядатися як юридично значуща. Саме ця обставина відмежовує технічну помилку або несуттєве редагування від діяння, яке реально впливає на порядок мобілізаційної підготовки та мобілізації.

У практичному вимірі важливим є й те, що такі правопорушення можуть мати мережевий або груповий характер. Посадова особа, яка має доступ до системи, може діяти не ізольовано, а в інтересах конкретного військовозобов'язаного, посередника або іншої зацікавленої особи. Тому під час досудового розслідування доцільно перевіряти комунікації, фінансові операції, повторюваність аналогічних змін, зв'язки між користувачами, кількість однотипних випадків, час внесення відомостей, обставини чергування та інші поведінкові індикатори. Особливої уваги потребують ситуації, коли одна й та сама посадова особа неодноразово змінювала статуси різних військовозобов'язаних без належних документальних підстав.

Окремим напрямом протидії є внутрішній адміністративний контроль. Ефективна система запобігання таким правопорушенням має передбачати розмежування прав доступу, обов'язкову фіксацію кожної зміни, автоматичне збереження попереднього значення, періодичний аудит дій користувачів, перевірку відповідності електронної операції матеріальному документу, службове реагування на атипові зміни, а також персональну відповідальність за використання ключів доступу. У сфері мобілізаційного обліку цифровий контроль не повинен підміняти службову дисципліну, однак має створювати умови для швидкого виявлення недобросовісних або необережних дій.

Не менш важливо забезпечити узгоджену міжвідомчу взаємодію. Територіальні центри комплектування та соціальної підтримки, правоохоронні органи, органи досудового розслідування, адміністратори інформаційних систем і органи військового управління мають діяти в межах єдиного підходу до перевірки цифрових змін. Виявлення недостовірних даних у Реєстрі повинно супроводжуватися не лише виправленням запису, а й з'ясуванням підстав його внесення, кола причетних осіб, можливих наслідків для мобілізаційного процесу та наявності ознак кримінального правопорушення.

Водночас необхідно уникати надмірної криміналізації службових помилок. Не кожне некоректне внесення інформації до автоматизованої системи є кримінальним правопорушенням. Помилка, що виникла внаслідок технічного збою, неоднозначності

документів, несвоєчасного оновлення відомостей або відсутності належного навчання користувача, має оцінюватися з урахуванням фактичної вини, характеру наслідків і можливості її виправлення. Кримінально-правовий вплив має застосовуватися тоді, коли встановлено суспільно небезпечний характер діяння, його несанкціонованість, причинний зв'язок із шкідливими наслідками або реальним ризиком їх настання та відповідну форму вини.

Таким чином, несанкціонована зміна інформації в Реєстрі «Оберіг» або інших автоматизованих системах у сфері військового обліку є багатовимірним правовим явищем. Воно поєднує інформаційно-правовий, військово-адміністративний, службово-дисциплінарний, антикорупційний і кримінально-правовий аспекти. Саме тому протидія таким діянням повинна бути не фрагментарною, а системною: від належного нормативного регулювання і контролю доступу до якісного документування цифрових слідів та правильної кваліфікації у кримінальному провадженні.

Висновки. Протиправна діяльність, пов'язана з несанкціонованою зміною інформації в автоматизованих системах особою, яка має право доступу до неї, у сфері мобілізаційної підготовки та мобілізації становить підвищену суспільну небезпеку в умовах воєнного стану. Її небезпека полягає не лише у порушенні правил обробки інформації, а й у потенційному впливі на військовий облік, мобілізаційні процедури, дисципліну в органах військового управління та обороноздатність держави.

По-перше, достовірність відомостей у Єдиному державному реєстрі призовників, військовозобов'язаних та резервістів має розглядатися як важлива гарантія належного функціонування системи мобілізаційної підготовки. Будь-яке внесення змін до таких відомостей повинно ґрунтуватися на законній підставі, підтверджуватися відповідними документами та відповідати службовій меті обробки інформації.

По-друге, наявність у посадової особи права доступу до автоматизованої системи не легітимізує довільну зміну даних. Вихід за межі службових повноважень, внесення недостовірних відомостей або використання доступу для створення уявних підстав зміни мобілізаційного статусу особи може утворювати ознаки кримінального правопорушення, передбаченого статтею 362 КК України, а за наявності додаткових обставин – потребувати оцінки за сукупністю інших кримінально-правових норм.

По-третє, ефективне розслідування таких діянь неможливе без належного документування цифрових слідів. Вирішальне значення мають журнали доступу, час і зміст змін, ідентифікатор користувача, підстави внесення запису, наявність або відсутність первинних документів, а також зв'язок між цифровою зміною і подальшим правовим результатом для військовозобов'язаного.

По-четверте, запобігання таким правопорушенням має охоплювати посилення внутрішнього контролю в територіальних центрах комплектування та соціальної підтримки, регулярний аудит дій користувачів, розмежування прав доступу, технічну неможливість безпідставної зміни ключових статусів без підтверджуючих документів, підвищення службової дисципліни та персональну відповідальність посадових осіб за використання власного доступу до реєстрів.

Отже, в умовах триваючої збройної агресії проти України забезпечення невідворотності відповідальності за несанкціоновані зміни інформації в системах військового обліку є необхідною передумовою зміцнення правопорядку, підвищення довіри до державних інституцій, протидії корупційним практикам і належного забезпечення обороноздатності держави.

Список використаних джерел:

1. Про оборону України : Закон України від 06.12.1991 № 1932-XII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/1932-12 (дата звернення: 27.08.2026).

2. Про правовий режим воєнного стану : Закон України від 12.05.2015 № 389-VIII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/389-19 (дата звернення: 27.08.2026).

3. Про введення воєнного стану в Україні : Указ Президента України від 24.02.2022 № 64/2022 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/64/2022 (дата звернення: 27.08.2026).

4. Конституція України : Конституція України від 28.06.1996 № 254к/96-ВР // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/254%D0%BA/96-%D0%B2%D1%80 (дата звернення: 27.08.2026).

5. Про військовий обов'язок і військову службу : Закон України від 25.03.1992 № 2232-XII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2232-12 (дата звернення: 27.08.2026).

6. Про мобілізаційну підготовку та мобілізацію : Закон України від 21.10.1993 № 3543-XII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/3543-12 (дата звернення: 27.08.2026).

7. Про затвердження Положення про територіальні центри комплектування та соціальної підтримки : Постанова Кабінету Міністрів України від 23.02.2022 № 154 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/154-2022-%D0%BF (дата звернення: 27.08.2026).

8. Про інформацію : Закон України від 02.10.1992 № 2657-XII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2657-12 (дата звернення: 27.08.2026).

9. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2939-17 (дата звернення: 27.08.2026).

10. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/80/94-%D0%B2%D1%80 (дата звернення: 27.08.2026).

11. Про Єдиний державний реєстр призовників, військовозобов'язаних та резервістів : Закон України від 16.03.2017 № 1951-VIII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/1951-19 (дата звернення: 27.08.2026).

12. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2297-17 (дата звернення: 27.08.2026).

13. Про Статут внутрішньої служби Збройних Сил України : Закон України від 24.03.1999 № 548-XIV // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/548-14 (дата звернення: 27.08.2026).

14. Про Дисциплінарний статут Збройних Сил України : Закон України від 24.03.1999 № 551-XIV // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/551-14 (дата звернення: 27.08.2026).

15. Питання проведення призову громадян на військову службу під час мобілізації, на особливий період : Постанова Кабінету Міністрів України; Порядок від 16.05.2024 № 560 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/560-2024-%D0%BF (дата звернення: 27.08.2026).

16. Про затвердження Порядку організації та ведення військового обліку призовників, військовозобов'язаних та резервістів : Постанова Кабінету Міністрів України від 30.12.2022 № 1487 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/1487-2022-%D0%BF (дата звернення: 27.08.2026).

17. Кодекс України про адміністративні правопорушення : Кодекс України; Закон від 07.12.1984 № 8073-X // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/80731-10 (дата звернення: 27.08.2026).

18. Кримінальний кодекс України : Кодекс України; Закон від 05.04.2001 № 2341-III // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2341-14 (дата звернення: 27.08.2026).

19. Кримінальний процесуальний кодекс України : Кодекс України; Закон від 13.04.2012 № 4651-VI // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/4651-17 (дата звернення: 27.08.2026).

20. Градецька Н. М. Конституційні засади військового обов'язку та заходи попередження ухилення від його реалізації. Прикарпатський юридичний вісник. 2023. Вип. 1 (48). С. 83–88.

21. Колб Л. Г., Бусел А. О., Третяк Є. Г. Військова служба в Україні: поняття, сутність і заходи щодо запобігання від її ухилення. *Юридичний електронний журнал*. 2024. № 3. С. 306–308. DOI https://doi.org/10.32782/2524-0374/2024-3/71

Дата першого надходження статті до видання: 19.06.2026
Дата прийняття статті до друку після рецензування: 14.07.2026
Дата публікації (оприлюднення) статті: 30.09.2026