УДК 342.738:355.1:004.056

В. В. Карпусь

ПРАВОВЕ РЕГУЛЮВАННЯ ТА РОЗМЕЖУВАННЯ ДОСТУПУ ДО СЛУЖБОВИХ ДОКУМЕНТІВ У ЗБРОЙНИХ СИЛАХ УКРАЇНИ: МІЖНАРОДНИЙ ДОСВІД

Анотація. *Досліджено правові засади обмеження та розмежування доступу до службових документів у Збройних Силах України в умовах воєнного стану. Визначено відмінності між службовою інформацією, державною таємницею та відкритими відомостями, а також співвідношення формального допуску й потреби ознайомлення з конкретним документом. Порівняно відкриті підходи України, НАТО, Великої Британії та США до класифікації, авторизації та контролю доступу. Запропоновано правові й організаційні рекомендації для вдосконалення військового діловодства.*

Ключові слова: *службова інформація, військове діловодство, розмежування доступу, державна таємниця, need-to-know, Збройні Сили України, міжнародний досвід.*

Abstract. *The paper examines the legal framework governing access to official documents in the Armed Forces of Ukraine under martial law. It distinguishes official information, state secrets and publicly accessible information, and clarifies the difference between security clearance and authorization to access specific records. Publicly available approaches used in Ukraine, NATO, the United Kingdom and the United States are compared. Legal and organizational recommendations are proposed to improve military records management and accountability.*

Keywords: *official information, military records management, access control, classified information, need-to-know, Armed Forces of Ukraine, international experience.*

Вступ

В умовах повномасштабної збройної агресії проти України своєчасний обмін службовими документами є необхідною передумовою функціонування військового управління. Водночас надмірне поширення інформації, її неналежне маркування або безпідставне обмеження доступу створюють різні за характером правові ризики. Перший стосується розголошення чутливих відомостей і загрози безпеці персоналу; другий — порушення принципів законності, підзвітності та доступу до публічної інформації. Ці ризики не можна усунути одним лише запровадженням електронної системи документообігу.

Актуальність теми полягає у необхідності узгодити захист військової інформації із чіткими юридичними підставами обмеження доступу, службовою компетенцією користувачів та міжнародними принципами інформаційної безпеки. Мета роботи — дослідити нормативні критерії класифікації військових документів і повноважень щодо доступу до них, порівняти відкриті міжнародні моделі та визначити напрями вдосконалення правового регулювання в Україні. Застосовано формально-юридичний, порівняльно-правовий та системний методи. Дослідження обмежено відкритими правовими джерелами й не описує непублічні процедури ЗСУ.

Основна частина

Конституційні гарантії свободи інформації та право на захист національної безпеки вимагають диференційованого підходу до кожного документа. Закон України «Про інформацію» розмежовує відкриту інформацію та інформацію з обмеженим доступом; остання охоплює конфіденційну, таємну і службову інформацію [1]. Водночас назва документа, його військове походження або належність до внутрішнього листування не є самостійною достатньою підставою для автоматичного засекречування.

Закон «Про доступ до публічної інформації» передбачає перевірку обґрунтованості обмеження за сукупністю критеріїв: легітимна мета, істотна шкода відповідному інтересу від

розголошення та переважання цієї шкоди над суспільним інтересом в отриманні інформації [2]. Цей підхід особливо важливий для документів із позначкою «Для службового користування» (ДСК). Віднесення до службової інформації не тотожне віднесенню до державної таємниці, а рішення про обмеження повинне мати законну підставу.

Окремий правовий режим встановлено Законом України «Про державну таємницю» [3]. Він визначає ступені секретності, компетенцію державних експертів з питань таємниць, вимоги до матеріальних носіїв і спеціальний порядок допуску та доступу. Таким чином, під час організації військового діловодства необхідно розрізняти щонайменше три ситуації: відкритий документ, документ зі службовою інформацією та документ із відомостями, що становлять державну таємницю. Для кожної категорії застосовуються різні правові вимоги.

Важливим є розмежування понять «допуск до державної таємниці» та «доступ до державної таємниці». За законом допуск означає оформлення права громадянина працювати із секретною інформацією, тоді як доступ пов'язаний із дозволом ознайомлюватися з конкретною інформацією відповідно до службової потреби [3]. Наявність оформленого допуску не створює необмеженого права переглядати всі документи певного ступеня секретності. Відповідні рішення повинні прийматися уповноваженими посадовими особами.

Для службових документів доцільно використовувати принцип мінімально необхідного доступу: посадова особа отримує саме ті відомості, які об'єктивно потрібні для виконання визначеного завдання. Принцип має організаційний зміст і не може замінити спеціальних норм про режим секретності. Правомірне розмежування доступу повинно враховувати посадові функції, мету використання документа, строк актуальності дозволу та контроль його перегляду після зміни службових повноважень.

В умовах воєнного стану інтенсивність кадрових переміщень і оперативність управлінських рішень можуть зростати, проте це не усуває потреби документувати підстави доступу. Закон «Про правовий режим воєнного стану» визначає особливий порядок діяльності державних органів та військового командування, але не є загальним дозволом на довільне обмеження інформаційних прав [4].

Постанова Кабінету Міністрів України № 736 затверджує Типову інструкцію щодо обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію [5]. Її положення формують загальну основу організації роботи з такими документами; застосування у військових органах повинне враховувати належні спеціальні нормативні акти та межі їх дії. Важливо уникати змішування грифів ДСК і ступенів секретності державної таємниці.

Електронний формат не змінює змісту правового режиму відомостей. Створення цифрової копії, її пересилання чи завантаження до інформаційної системи мають оцінюватися з огляду на правомірність доступу та допустимість відповідного середовища оброблення. Закон «Про захист інформації в інформаційно-комунікаційних системах» встановлює загальні засади охорони інформації в таких системах [6]. Отже, технічна можливість відкрити файл не дорівнює юридичному праву ознайомитися з його змістом.

Для правової визначеності доцільно розрізняти автора документа, його власника або розпорядника в установленому законом значенні, особу, яка ухвалює рішення про доступ, та користувача, якому доступ надано. Такий поділ допомагає встановити відповідальність за неправомірне поширення відомостей і водночас запобігати необґрунтованим відмовам.

У відкритих документах політики безпеки НАТО важливе місце займає принцип need-to-know — доступ до захищеної інформації має бути зумовлений службовою необхідністю, а не лише формальним статусом особи [7]. При цьому правила НАТО стосуються визначених категорій інформації Альянсу та не можуть автоматично підміняти національне законодавство України. Їх практична цінність полягає в розмежуванні класифікації відомостей, перевірки особи та конкретного рішення про надання доступу.

У Великій Британії Government Security Classifications Policy (оновлена у 2024 році) застосовує три основні рівні класифікації: OFFICIAL, SECRET і TOP SECRET [8]. Захисні заходи

співвідносяться з імовірними наслідками компрометації та характером загроз. Важливим елементом є не лише маркування документа, а й правила поводження з ним протягом усього життєвого циклу. Британська модель демонструє ризик-орієнтований підхід, однак її рівні класифікації не є прямими юридичними еквівалентами українських категорій.

У США Executive Order 13526 регламентує систему класифікації інформації національної безпеки, передбачає критерії її засекречування, перегляду та розсекречування [9]. Доступ до класифікованої інформації, за загальним правилом, пов'язується з належним статусом особи, виконанням службових функцій і необхідністю ознайомлення. Для українського контексту важливо не механічно копіювати іноземні процедури, а використовувати порівняльний аналіз для підвищення визначеності критеріїв і підзвітності рішень.

Порівняння показує спільну логіку трьох підходів: класифікація має бути обґрунтованою; право доступу є обмеженим службовою потребою; правила поводження з документами повинні супроводжувати їх від створення до зберігання або законного зняття обмежень. Водночас юридична природа інформаційних категорій, повноваження органів і механізми контролю відрізняються.

На підставі аналізу пропонується удосконалювати локальні правила документообігу за чотирма напрямами. Перший — забезпечення однозначного розмежування відкритих, службових і секретних відомостей із посиланням на відповідні правові підстави. Другий — формалізація службової необхідності доступу, щоб наявність посади або загального допуску не підміняла рішення щодо конкретних категорій документів. Третій — систематичний перегляд повноважень користувачів після кадрових і функціональних змін. Четвертий — підвищення правової грамотності персоналу щодо маркування, копіювання, передавання та архівування документів.

Доцільно також забезпечувати простежуваність управлінських рішень про надання, зміну й припинення доступу та можливість їх перевірки уповноваженими органами. Конкретні технологічні механізми повинні визначатися компетентними структурами відповідно до чинних вимог захисту інформації. У відкритій науковій публікації недоцільно деталізувати внутрішню архітектуру військових систем, непублічні процедури авторизації або відомості, розголошення яких може створити загрозу безпеці.

Окремий напрям — протидія необґрунтованому обмеженню доступу. Наявність законної мети захисту інформації не звільняє розпорядника від обов'язку належно обґрунтувати застосоване обмеження, якщо до правовідносин застосовуються правила доступу до публічної інформації. Отже, вдосконалення режиму захисту має супроводжуватися гарантіями законності та належними механізмами перегляду рішень.

Висновки

Правове регулювання доступу до службових документів у Збройних Силах України ґрунтується на поєднанні загальних гарантій інформаційних прав, норм щодо службової інформації та спеціального законодавства про державну таємницю. Визначальним є відокремлення юридичного статусу інформації від технічної можливості її отримання. Допуск до державної таємниці не тотожний дозволу ознайомитися з конкретним документом, а позначка ДСК не є ступенем секретності.

Порівняльний аналіз відкритих практик НАТО, Великої Британії та США підтверджує значення принципу службової необхідності, пропорційного захисту й документованого контролю повноважень. Запропоновано вдосконалювати критерії класифікації, розподіл відповідальності, правову підготовку персоналу та процедури перегляду доступу. Ці рекомендації мають концептуальний характер і потребують адаптації до чинних українських нормативних актів та законно встановлених відомчих процедур.

Список використаних джерел:

1. Про інформацію : Закон України від 02.10.1992 № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12.
2. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI. URL: https://zakon.rada.gov.ua/laws/show/2939-17.
3. Про державну таємницю : Закон України від 21.01.1994 № 3855-XII. URL: https://zakon.rada.gov.ua/laws/show/3855-12.
4. Про правовий режим воєнного стану : Закон України від 12.05.2015 № 389-VIII. URL: https://zakon.rada.gov.ua/laws/show/389-19.
5. Про затвердження Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію : постанова КМУ від 19.10.2016 № 736. URL: https://zakon.rada.gov.ua/laws/show/736-2016-%D0%BF.
6. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80.
7. NATO. Security within the North Atlantic Treaty Organization. C-M(2002)49 (publicly available policy framework). URL: https://www.nato.int/cps/en/natohq/official_texts_17120.htm.
8. UK Cabinet Office. Government Security Classifications Policy. Updated 5 August 2024. URL: https://www.gov.uk/government/publications/government-security-classifications/government-security-classifications-policy-html.
9. Executive Order 13526 of December 29, 2009. Classified National Security Information. Federal Register. URL: https://www.archives.gov/isoo/policy-documents/cnsi-eo.html.

Карпусь Віталій Володимирович – помічник військового капелана ЗСУ, Вінниця; e-mail: karpus-v-v@ukr.net.

Karpus Vitalii – Assistant to a Military Chaplain of the Armed Forces of Ukraine; e-mail: karpus-v-v@ukr.net.