УДК 355.4:004.91:342.78

В. В. Карпусь

ОСОБЛИВОСТІ ПРАВОВОГО РЕГУЛЮВАННЯ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ В ЗСУ ПІД ЧАС ВОЄННОГО СТАНУ

Анотація. Проаналізовано нормативно-правові засади електронного документообігу у Збройних Силах України під час воєнного стану. Розмежовано загальний режим електронних документів і спеціальні вимоги до інформації з обмеженим доступом, визначено значення електронного підпису, реєстрації, зберігання, кіберзахисту та безперервності управління. Запропоновано організаційно-правові напрями вдосконалення військового діловодства.

Ключові слова: електронний документообіг, Збройні Сили України, воєнний стан, електронний підпис, захист інформації, військове управління.

Abstract. The paper examines the legal framework for electronic document management in the Armed Forces of Ukraine under martial law. It distinguishes the general legal regime for electronic documents from special rules applicable to restricted information and addresses electronic signatures, registration, retention, cybersecurity and continuity of command. Organizational and legal improvements to military records management are proposed.

Keywords: electronic document management, Armed Forces of Ukraine, martial law, electronic signature, information protection, military administration.

Вступ

Цифровізація управлінських процесів стала необхідною умовою своєчасного ухвалення рішень, обміну розпорядчими документами та забезпечення підзвітності державних органів. Для Збройних Сил України (ЗСУ) значення електронного документообігу посилюється в умовах воєнного стану, коли необхідно одночасно забезпечувати оперативність комунікацій, достовірність документів і збереження інформації. Однак перенесення паперових процедур в електронне середовище саме собою не усуває правових ризиків, пов’язаних із розмежуванням доступу, повноваженнями підписантів і зберіганням цифрових доказів.

Актуальність дослідження зумовлена поєднанням загальнодержавного курсу на цифровізацію з особливим правовим режимом функціонування військового управління. Метою роботи є систематизація відкритих норм законодавства України, що визначають юридичну силу електронних документів, особливості їх застосування у військовій сфері та вимоги до захисту інформації під час воєнного стану. Використано формально-юридичний, системний і порівняльно-правовий методи. Предметом дослідження є нормативні вимоги, а не внутрішня архітектура чи непублічні процедури інформаційних систем ЗСУ.

Основна частина

1. Загальні правові засади електронного документообігу.

Базовим актом є Закон України «Про електронні документи та електронний документообіг» № 851-IV, який визначає електронний документ, засади його створення, передавання, одержання та зберігання [1]. Законодавство виходить із того, що електронна форма сама по собі не може бути підставою для заперечення юридичної сили документа. Водночас правова придатність конкретного документа залежить від належного оформлення обов’язкових реквізитів, встановлення автора та виконання спеціальних вимог, передбачених для певної категорії документів.

Закон України «Про електронну ідентифікацію та електронні довірчі послуги» № 2155-VIII регулює механізми ідентифікації та електронного підписання [2]. Кваліфікований електронний

підпис є важливим засобом підтвердження авторства та цілісності документа в межах застосовного правового режиму. Проте наявність підпису не підтверджує автоматично службових повноважень особи, законності змісту наказу чи дотримання правил доступу. Отже, технічна автентифікація і юридична компетенція посадової особи мають перевірятися окремо.

Для військового діловодства важливі також реєстраційний індекс, дата, належність документа до конкретної справи, підтвердження отримання адресатом і можливість відтворити історію його опрацювання. Правила ведення діловодства мають узгоджуватися з актами, що регулюють діяльність відповідного органу, та спеціальними відомчими вимогами.

2. Особливості воєнного стану та компетенції військового управління.

Закон України «Про правовий режим воєнного стану» № 389-VIII визначає правові засади діяльності державних органів і військового командування в особливий період [3]. Введення воєнного стану не означає автоматичного скасування загальних вимог до документування управлінських рішень. Навпаки, підвищена швидкість обігу інформації потребує чіткого визначення компетенції посадових осіб, порядку доведення розпоряджень та відповідальності за їх виконання.

Закон України «Про оборону України» та Закон України «Про Збройні Сили України» встановлюють організаційні засади оборони і функціонування ЗСУ [4; 5]. У межах цих засад електронний документообіг може підтримувати управлінські процеси, але не підмінює передбачені законодавством форми військового керівництва. Правомірність електронного наказу або службового повідомлення залежить від його виду, компетенції автора, встановленого порядку оформлення та каналу доведення.

Особливої уваги потребує відмежування загальнодоступного адміністративного листування від документів, які містять відомості про бойові завдання, переміщення сил, озброєння чи інші чутливі дані. Сам факт існування електронної системи документообігу не означає, що в ній дозволено опрацьовувати будь-які категорії військової інформації.

3. Документи з обмеженим доступом і правові межі цифровізації.

Закон України «Про державну таємницю» встановлює особливий режим охорони секретної інформації [6]. Закон України «Про захист інформації в інформаційно-комунікаційних системах» визначає загальні засади її захисту під час автоматизованого оброблення [7]. Порядок роботи з документами, що містять державну таємницю або службову інформацію, повинен відповідати спеціальним вимогам і не може визначатися лише зручністю електронного обміну.

Принципове значення має стаття 2 Закону № 2155-VIII: дія цього Закону не поширюється на електронну ідентифікацію та надання електронних довірчих послуг у системах, де обробляють службову інформацію і державну таємницю, а також у визначених законом інших випадках [2]. Тому твердження про універсальну обов’язковість загальнодоступних сервісів електронного підпису для всіх військових документів було б юридично некоректним. Для таких систем застосовують спеціальні правові та організаційно-технічні механізми.

Правовий режим документа визначається не носієм, а змістом відомостей, підставами обмеження доступу та встановленими правилами роботи. Цифрова копія паперового документа також не завжди набуває статусу оригіналу лише через сканування. Потрібно розрізняти електронний оригінал, належно засвідчену копію та інформаційний образ документа.

4. Автентичність, зберігання та доказове значення.

Важливою умовою юридичної надійності електронного документообігу є можливість встановити автора, час створення, факт підписання, зміну версій та факт надходження документа адресату. Окреме значення мають метадані, журнали подій і правила доступу до них. Застосування електронних позначок часу та інших довірчих механізмів здійснюється у випадках, визначених відповідним правовим режимом [1; 2].

Питання зберігання електронних документів має охоплювати не тільки фізичну наявність файлу, а й збереження придатності його прочитання, перевірки підпису та підтвердження

цілісності протягом установленого строку. Архівування потребує врахування Закону України «Про Національний архівний фонд та архівні установи» і чинних правил діловодства [8]. Перехід на нове програмне забезпечення не повинен спричиняти втрату реквізитів, реєстраційних даних або зв’язку між документом і справою.

У разі службового розслідування чи судового спору електронний документ може мати доказове значення за умови встановлення його походження та цілісності. Саме тому доцільно документувати життєвий цикл електронного документа: від створення й погодження до виконання, завершення діловодства та передання на зберігання.

5. Кібербезпека та безперервність документообігу.

Воєнний стан загострює ризики несанкціонованого доступу, підміни документів, втрати даних та недоступності інформаційних ресурсів. Закон України «Про основні засади забезпечення кібербезпеки України» встановлює загальну правову основу відповідних заходів [9]. При цьому конкретні технічні рішення для військових систем повинні визначатися уповноваженими органами та внутрішніми регламентами, а не публічними універсальними схемами.

У нормативному аспекті ключовими є принципи мінімально необхідного доступу, персональної відповідальності користувачів, обліку операцій і контролю правомірності передавання інформації. Окремо слід передбачати правомірні процедури роботи за умов тимчасової недоступності електронної системи, а також подальше належне документування дій. Такі процедури мають забезпечувати безперервність управління без порушення вимог щодо захисту інформації.

Законодавчо врегульована електронна взаємодія має поєднувати швидкість передавання повідомлень з можливістю їх перевірки, належним розподілом повноважень і збереженням службової таємниці. Це особливо важливо для багаторівневої системи військового управління.

6. Напрями вдосконалення правового забезпечення.

За результатами аналізу пропонується диференційований підхід до електронного документообігу: для документів загального адміністративного характеру — застосування передбачених законом електронних інструментів; для інформації з обмеженим доступом — дотримання спеціальних правил і дозволених середовищ оброблення. Така диференціація дозволяє уникнути помилкового ототожнення електронного документа з документом, придатним для передавання будь-яким цифровим каналом.

Другим напрямом є узгодження відомчих регламентів із чинними законами щодо реквізитів, строків зберігання, обліку дій користувачів, передачі повноважень і відповідальності. Третім — систематична підготовка персоналу з питань електронного підпису, інформаційної безпеки, класифікації документів та правил роботи з копіями. Четвертим — правова оцінка процедур відновлення документообігу після технічних збоїв.

Запропоновані напрями є авторськими узагальненнями, сформульованими на підставі відкритого законодавства. Вони не свідчать про наявність чи відсутність конкретних непублічних інформаційних систем або внутрішніх регламентів ЗСУ.

Висновки

Електронний документообіг у ЗСУ під час воєнного стану регулюється поєднанням загальних норм щодо електронних документів і спеціального законодавства у сфері оборони, державної таємниці та захисту інформації. Юридична сила документа залежить не лише від електронної форми чи підпису, а й від повноважень автора, дотримання процедури та належного режиму доступу.

Найсуттєвішою особливістю військового документообігу є необхідність розмежовувати відкриті адміністративні документи та інформацію з обмеженим доступом. Для останньої не можна беззастережно застосовувати загальні інструменти електронної ідентифікації та обміну. Подальше

вдосконалення має спрямовуватися на нормативну узгодженість, простежуваність документів, збереження цифрових доказів, кіберстійкість і підготовку персоналу.

Список використаних джерел:

1. Про електронні документи та електронний документообіг : Закон України від 22.05.2003 № 851-IV. URL: https://zakon.rada.gov.ua/laws/show/851-15.

2. Про електронну ідентифікацію та електронні довірчі послуги : Закон України від 05.10.2017 № 2155-VIII. URL: https://zakon.rada.gov.ua/laws/show/2155-19

3. Про правовий режим воєнного стану : Закон України від 12.05.2015 № 389-VIII. URL: https://zakon.rada.gov.ua/laws/show/389-19.

4. Про оборону України : Закон України від 06.12.1991 № 1932-XII. URL: https://zakon.rada.gov.ua/laws/show/1932-12.

5. Про Збройні Сили України : Закон України від 06.12.1991 № 1934-XII. URL: https://zakon.rada.gov.ua/laws/show/1934-12.

6. Про державну таємницю : Закон України від 21.01.1994 № 3855-XII. URL: https://zakon.rada.gov.ua/laws/show/3855-12.

7. 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

8. Про Національний архівний фонд та архівні установи : Закон України від 24.12.1993 № 3814-XII. URL: https://zakon.rada.gov.ua/laws/show/3814-12.

9. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19.

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.