УДК 355.4:004.056:004.91

В. В. Карпусь, А. В. Колесник

КІБЕРБЕЗПЕКА ВІЙСЬКОВОГО ЗВ'ЯЗКУ ТА ЗАХИСТ ІНФОРМАЦІЇ В СИСТЕМІ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ (СЕДО) ЗБРОЙНИХ СИЛ УКРАЇНИ В УМОВАХ ВОЄННОГО СТАНУ

Анотація. *Досліджено нормативно-правові та організаційні засади кібербезпеки військового зв'язку і захисту інформації в системах електронного документообігу Збройних Сил України в умовах воєнного стану. Розмежовано загальні правила електронного документообігу та спеціальні режими оброблення інформації з обмеженим доступом. Визначено значення конфіденційності, цілісності, доступності, автентичності й безперервності управлінських процесів. Запропоновано напрями підвищення кіберстійкості на рівні правового регулювання, організації та підготовки персоналу.*

Ключові слова: *кібербезпека, військовий зв'язок, СЕДО, електронний документообіг, Збройні Сили України, воєнний стан, захист інформації.*

Abstract. *The paper examines the legal and organizational foundations of cybersecurity in military communications and information protection in electronic document management systems of the Armed Forces of Ukraine under martial law. It distinguishes general electronic document rules from special regimes governing restricted information. The study highlights confidentiality, integrity, availability, authenticity and continuity of military administration and proposes legal, organizational and training measures to improve cyber resilience.*

Keywords: *cybersecurity, military communications, electronic document management system, Armed Forces of Ukraine, martial law, information protection.*

Вступ

У сучасних умовах збройної агресії цифрові канали комунікації забезпечують обмін інформацією між органами військового управління, підрозділами та установами. Водночас електронне середовище створює ризики перехоплення повідомлень, несанкціонованого доступу, підміни службових документів і блокування інформаційних ресурсів. Тому захист військового зв'язку та електронного документообігу необхідно розглядати як взаємопов'язані елементи інформаційної стійкості оборонного сектору.

Актуальність дослідження полягає в необхідності узгодження оперативності електронного обміну з вимогами законності, режиму доступу та безперервності управління. Мета роботи — на основі відкритого законодавства визначити правові та організаційні особливості кіберзахисту військових комунікацій і СЕДО, а також сформулювати пропозиції щодо вдосконалення практик без розкриття внутрішніх механізмів захищених систем. Застосовано формально-юридичний, системний і порівняльно-аналітичний методи.

Основна частина

Військовий зв'язок забезпечує передавання повідомлень, тоді як СЕДО підтримує створення, погодження, реєстрацію, виконання й архівування документів. Ці функції перетинаються, але не є тотожними: захищений канал передавання не гарантує правильності змісту або повноважень підписанта, а коректно оформлений електронний документ не гарантує безпеки мережі. Отже, кібербезпека має охоплювати весь життєвий цикл інформації — від її створення до зберігання та правомірного знищення.

Для оборонної сфери особливо важливим є одночасне забезпечення конфіденційності, цілісності та доступності даних. Конфіденційність обмежує доступ сторонніх осіб, цілісність запобігає непомітній зміні змісту, а доступність підтримує своєчасне отримання документа уповноваженим адресатом. Додатково необхідні автентичність походження, простежуваність дій користувачів і юридично належне підтвердження отримання документа. Зазначені принципи не є описом конкретної архітектури СЕДО ЗСУ, а становлять загальні критерії оцінювання її правового та організаційного забезпечення.

Закон України «Про основні засади забезпечення кібербезпеки України» визначає засади державної політики, суб'єктів національної системи кібербезпеки та заходи реагування на кіберзагрози [1]. У чинній редакції законодавство підкреслює ризик-орієнтований підхід, міжвідомчу координацію та компетенцію Міністерства оборони України і Генерального штабу ЗСУ у сфері кібероборони. Загальні правила захисту інформації під час її оброблення в інформаційно-комунікаційних системах визначає Закон № 80/94-ВР [2].

Закон «Про електронні документи та електронний документообіг» установлює засади створення, передавання, одержання і зберігання електронних документів [3]. Однак юридична сила документа не вичерпується його електронною формою: мають значення обов'язкові реквізити, компетенція автора, встановлений порядок погодження й доведення до адресата. Закон № 2155-VIII регулює електронну ідентифікацію та довірчі послуги, проте прямо визначає винятки для систем, у яких обробляють службову інформацію та державну таємницю [4]. Отже, застосування загальнодоступних сервісів підпису до всіх військових документів без правового розмежування було б помилковим.

Закон «Про державну таємницю» визначає особливий режим охорони секретних відомостей [5]. Наявність СЕДО не створює універсального дозволу обробляти в ній документи будь-якої категорії. Для інформації з обмеженим доступом вирішальними є її правовий статус, допуск та повноваження користувача, встановлені правила оброблення і дозволене інформаційне середовище. Електронний документ, сканована копія та належно засвідчена копія також мають різні правові характеристики.

Воєнний стан не скасовує вимог до законності обігу документів. Закон № 389-VIII визначає особливий режим діяльності органів державної влади та військового командування [6]. У цьому контексті необхідно забезпечувати баланс між швидкістю управлінських рішень та належною фіксацією повноважень, змісту й часу доведення документа. Практика має спиратися на чинні відкриті нормативні акти і відповідні відомчі регламенти, зміст яких може бути обмеженим для публічного доступу.

До типових загроз електронному документообігу належать фішинг, компрометація облікових даних, шкідливе програмне забезпечення, неправомірна зміна документа, помилки адресування та порушення доступності сервісу. Ці ризики є загальновідомими для інформаційних систем і не свідчать про виявлені вразливості певної військової мережі. Їх зниження потребує чіткого розподілу повноважень, обмеження доступу відповідно до службових функцій, навчання користувачів та організованого реагування на інциденти.

Особливу роль відіграє людський чинник. Навіть технічно захищена система залишається вразливою до помилок користувачів: передавання документа неналежному адресату, необережного поводження з автентифікаційними засобами або використання недозволеного середовища обміну. Доцільно впроваджувати регулярні навчальні заходи з розпізнавання підозрілих повідомлень, перевірки повноважень адресата, дотримання режиму доступу та своєчасного інформування відповідальних осіб про можливий інцидент.

Здатність відновлювати документування після порушення роботи інформаційних ресурсів є важливою складовою організаційної стійкості. На рівні правового регулювання доцільно передбачати належні процедури фіксації рішень у разі тимчасової недоступності електронної

системи та подальшого відображення таких дій у встановленому порядку. При цьому резервні процедури не повинні призводити до необґрунтованого послаблення захисту інформації.

Доказове значення електронного документа залежить від можливості підтвердити його походження, цілісність, належність підпису, час і обставини створення та отримання. Для належного зберігання важливі реєстраційні дані, контроль версій, документування життєвого циклу і дотримання архівних вимог [3; 7]. Відтак кібербезпека СЕДО має не лише технічний, а й процесуальний вимір, пов'язаний із можливістю відтворити історію ухвалення управлінського рішення.

На основі нормативного аналізу запропоновано чотири взаємопов'язані напрями: узгодження внутрішніх правил документообігу з чинним законодавством; чітке розмежування категорій інформації та відповідних режимів її оброблення; систематична підготовка персоналу; правова регламентація дій у разі кіберінцидентів і тимчасової недоступності електронних ресурсів. Такі заходи мають бути пропорційними ризикам, перевірюваними та сумісними з вимогами збереження документів.

Окремої уваги потребує періодичний перегляд регламентів з урахуванням змін законодавства і досвіду реагування на інциденти. Доцільно розмежовувати оцінювання відповідності правовим вимогам і технічне тестування захищеності, оскільки позитивний результат одного з них не замінює іншого. Наведені пропозиції є авторським узагальненням відкритих нормативних вимог, а не описом чинних внутрішніх процедур ЗСУ.

Висновки

Кібербезпека військового зв'язку та захист інформації у СЕДО Збройних Сил України становлять взаємопов'язані напрями забезпечення безперервності військового управління. Надійність цифрового обміну визначається не лише захищеністю каналів, а й юридично коректним оформленням документів, перевіркою повноважень, дотриманням режимів доступу та збереженням доказової інформації.

Основна особливість правового регулювання під час воєнного стану полягає в одночасному застосуванні загального законодавства про електронні документи, спеціальних правил захисту інформації та норм оборонної сфери. Підвищення кіберстійкості потребує системної взаємодії правових, організаційних і освітніх заходів. Подальші дослідження доцільно спрямувати на відкриті критерії оцінювання організаційної стійкості електронного документообігу та вдосконалення підготовки персоналу.

Список використаних джерел:

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

2. 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.

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

4. 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.

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

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

7. 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.

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

9. Про електронні комунікації : Закон України від 16.12.2020 № 1089-IX. URL: https://zakon.rada.gov.ua/laws/show/1089-20.

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

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

Колесник Андрій Вікторович — викладач військової кафедри, Вінницький національний технічний університет, Вінниця; e-mail: andrey.enginer@gmail.com.

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

Kolesnyk Andrii Viktorovych — Lecturer at the Military Department, Vinnytsia National Technical University, Vinnytsia, Ukraine; e-mail: andrey.enginer@gmail.com.