НАПРЯМ 15. ЗАХИСТ ІНФОРМАЦІЙНИХ СИСТЕМ І КІБЕРБЕЗПЕКА ПІД ЧАС ВІЙНИ ТА У ПІСЛЯВОЄННИЙ ПЕРІОД

DOI https://doi.org/10.36059/978-966-397-570-2-94

Данькевич Ю. В.,
кандидат філологічних наук, доцент,
доцент кафедри комп'ютерних та інформаційних технологій
Таврійського національного університету імені В. І. Вернадського
м. Київ, Україна

ОСОБЛИВОСТІ ЗАХИСТУ ІНФОРМАЦІЙНИХ СИСТЕМ У СФЕРІ ДОКУМЕНТОЗНАВСТВА ПІД ЧАС ВІЙНИ ТА У ПІСЛЯВОЄННИЙ ПЕРІОД: ВИКЛИКИ ТА ПЕРСПЕКТИВИ

Сучасні умови воєнного стану в Україні актуалізували проблему кібербезпеки та захисту інформаційних систем, особливо у сфері документознавства, яка є важливим елементом державного управління, національної безпеки та інформаційної стійкості. Війна змінила не лише технологічні, а й організаційні підходи до збереження, обробки та захисту документної інформації. У контексті цифровізації суспільства документознавство стає не просто сферою фіксації інформації, а складовою кіберінфраструктури держави. Тому питання безпеки інформаційних систем виявилося життєво важливим для функціонування органів влади, бізнесу та суспільних інститутів.

Під інформаційною системою у сфері документознавства розуміють сукупність технічних, програмних і організаційних засобів, що забезпечують створення, обіг, збереження та використання документів в електронному середовищі. Починаючи з 2022 року, Україна переживає безпрецедентну хвилю кіберагресій, спрямованих на державні реєстри, архівні ресурси, електронні документообігові системи. Дослідники з Національного інституту стратегічних досліджень підкреслюють, що основна мета таких атак полягає не лише у знищенні чи спотворенні даних, а й у дестабілізації інформаційної політики держави, підриві довіри громадян до офіційних джерел інформації [1]. Кібербезпека документознавчої сфери є частиною загальної концепції інформаційної безпеки України, визначеної в Законі України «Про основні засади забезпечення кібербезпеки України» (2017 р.) [2]. Документ окреслює необхідність створення інтегрованої системи

кіберзахисту державних і приватних інформаційних ресурсів. Одним із ключових викликів війни стало питання збереження цифрових архівів. У багатьох установах спостерігалися випадки пошкодження серверів, втрати доступу до інформаційних систем через окупацію територій або фізичне знищення інфраструктури.

У свою чергу, використання хмарних технологій дозволило зменшити ризики знищення документів, але водночас створило нові загрози, пов'язані з контролем доступу до даних та залежністю від зарубіжних провайдерів [3]. Важливим напрямом безпеки стало впровадження системи електронної ідентифікації та електронного підпису. Закон України «Про електронну ідентифікацію та електронні довірчі послуги» (2017 р.) заклав нормативну основу для створення безпечних процедур автентифікації користувачів у документознавчих системах [4]. Саме це дало змогу під час війни забезпечити безперервність документообігу у державному секторі. Досвід останніх років показав, що навіть найсучасніші технічні засоби не є достатньою гарантією безпеки без належної культури інформаційної поведінки.

Державна служба спеціального зв'язку та захисту інформації України (ДССЗЗІ) ініціювала оновлення методик оцінки ризиків, а також створення рекомендацій для захисту електронних архівів [5]. Вони базуються на міжнародних стандартах ISO/IEC 27001 [6] та ISO 15489 – «Інформація та документація. Управління записами» [7]. У сфері документознавства особливої уваги заслуговує питання цілісності та автентичності документів. У воєнний час спроби фальсифікації, підробки або знищення електронних доказів можуть мати серйозні правові наслідки. Відповідно, системи повинні забезпечувати журналювання усіх змін у документах і зберігати цифрові сліди операцій.

Не менш актуальним є питання правового забезпечення кіберзахисту. Юридична доктрина ще не сформувала чітких критеріїв відповідальності за кібератаки чи за неналежний захист документів. У цьому контексті доцільно адаптувати підходи Європейського Союзу, зокрема положення Директиви NIS 2 та Регламенту AI Act, які вимагають створення внутрішніх політик кібербезпеки та технічної документації систем, що обробляють інформацію з високим рівнем ризику [8]. Варто відзначити і досвід військових інформаційних структур, які розробляють спеціальні алгоритми розподіленого зберігання даних, що мінімізують втрати у разі фізичного знищення серверів. Ці підходи можуть бути адаптовані й для цивільних інформаційних систем документознавства. Післявоєнна відбудова інформаційної інфраструктури передбачає не лише технічне відновлення, а й створення національної політики кіберстійкості документних систем.

У міжнародному контексті варто враховувати стандарти ISO 22301 (Business Continuity Management Systems), які визначають вимоги

до планування безперервності бізнес-процесів, у тому числі документознавчих [9]. Це особливо актуально для післявоєнного етапу, коли потрібно гарантувати доступність інформації навіть у разі технічних збоїв. Важливо також розглядати етичний аспект кібербезпеки, адже захист інформаційних систем не повинен обмежувати права людини на доступ до інформації.

Війна стала каталізатором переосмислення концепції інформаційного суверенітету. Захист національних інформаційних ресурсів, зокрема документних баз, є питанням державної безпеки. Після війни необхідно створити умови для розвитку власних дата-центрів, національних репозиторіїв і програмних платформ. Особливу роль у відновленні систем відіграють кадрові ресурси. Підготовка фахівців з кіберзахисту у документознавчій сфері повинна стати пріоритетом освітньої політики. Важливим етапом стане інтеграція українських інформаційних систем у європейський цифровий простір. Це дозволить не лише забезпечити додатковий рівень кіберзахисту, а й гарантувати визнання електронних документів на міжнародному рівні. Крім того, необхідно продовжувати розвиток систем моніторингу кібератак, аналітичних платформ для прогнозування загроз і створення резервних копій даних у географічно розподілених зонах. Такий підхід відповідає концепції «цифрової стійкості» (digital resilience), яку активно розвивають у ЄС.

Отже, досвід воєнного часу показав, що кібербезпека документознавчої сфери є фундаментом інформаційної незалежності держави. Захист документів – це не лише технічна, а й стратегічна категорія, що охоплює етичні, правові, управлінські й освітні аспекти. В умовах війни забезпечення безпеки документних систем стало критично важливим для функціонування державного управління, науки, освіти та бізнесу. Після завершення війни пріоритетом стане створення адаптивної, гнучкої та стійкої цифрової інфраструктури, побудованої на принципах національного контролю, європейських стандартів і міжнародного партнерства. Українська документознавча наука має потенціал стати одним із центрів інновацій у сфері інформаційної безпеки.

Список використаних джерел:

1. Огляд російських кібератак проти України. URL: https://niss.gov.ua/news/komentari-ekspertiv/ohlyad-rosiyskykh-kiberatak-proty-ukrayiny (дата звернення: 10.10.2025).

2. Закон України «Про основні засади забезпечення кібербезпеки України». Документ 2163-VIII, чинний, поточна редакція – редакція від 20.04.2025, підстава – 4336-IX. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 10.10.2025).

3. Що таке хмарні технології? URL: https://ucloud.ua/hmarni-tehnologiyi-shho-cze-take/#:~: (дата звернення: 11.10.2025).

4. Закон України «Про електронну ідентифікацію та електронні довірчі послуги». Документ 2155-VIII, чинний, поточна редакція – редакція від 18.12.2024, підстава – 3911-IX. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text (дата звернення: 11.10.2025).

5. Державна служба спеціального зв'язку та захисту інформації України. URL: https://cip.gov.ua/ua (дата звернення: 11.10.2025).

6. Сертифікація ISO/IEC 27001 – Методи та засоби забезпечення інформаційної безпеки. URL: https://imcert.ua/ua/service/iso-iec-27001#:~:text (дата звернення: 10.10.2025)

7. ISO 15489 – «Інформація та документація. Управління записами». URL: https://zakon.isu.net.ua/sites/default/files/normdocs/dstu_iso_15489-1_2018.pdf (дата звернення: 10.10.2025).

8. Artificial Intelligence Act: MEPs adopt landmark law. URL: https://www.europarl.europa.eu/news/en/press-room/20240308IPR19015/artificial-intelligence-act-meps-adopt-landmark-law (дата звернення: 10.10.2025).

9. Business Continuity Solutions. URL: https://gigacloud.ua/solutions/business-continuity-solutions/?utm_source=googleads&utm_medium=cpc&utm_campaign=BCS_max_clicks_additional&utm_content=183406610876&utm_term= (дата звернення: 11.10.2025).