

### Список використаних джерел

1. Про державний захист працівників суду і правоохоронних органів: Закон України № 3781-ХІІ від 23.12.1993. URL: <https://zakon.rada.gov.ua/laws/show/3781-12#Text>
2. Хлистік М. А. Визначення поняття правоохоронного органу в законодавстві України. *Адміністративне право і процес; фінансове право; інформаційне право*. DOI: <https://doi.org/10.32838/TNU-2707-0581/2021.4/09>
3. ДСТУ 4163:2020. Уніфікована система організаційно-розпорядчої документації. Вимоги до оформлення документів. Київ, 2020.
4. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 № 4651-VI.
5. Про оперативно-розшукову діяльність: Закон України від 18.02.1992 № 2135-ХІІ.
6. Інструкція з оформлення документів у системі Міністерства внутрішніх справ України: затв. наказом МВС України від 27.07.2012 № 650.
7. Інструкція з діловодства в системі Міністерства внутрішніх справ України: затв. наказом МВС України від 23.08.2012 № 747.
8. Перелік типових документів, що створюються в діяльності державних органів та органів місцевого самоврядування, інших установ, підприємств та організацій, із зазначенням строків зберігання: затв. наказом Мін'юсту України від 12.04.2012 № 578/5 (зі змінами).
9. Правила організації діловодства та архівного зберігання документів: затв. наказом Мін'юсту України від 18.06.2015 № 1000/5 (зі змінами, внесеними наказом від 16.03.2026 № 667/5).



УДК: 070(043.2)

**Тімченко Максим Сергійович**

*(наук. керівник – канд. філол. наук, доцент Литвинська С. В.)*  
**Національний університет біоресурсів і природокористування України,**  
**м. Київ**

## **МАНІПУЛЯЦІЯ ОФІЦІЙНИМИ ДОКУМЕНТАМИ ЯК ІНСТРУМЕНТ ІНФОРМАЦІЙНИХ ВОЄН**

*Анотація. У роботі проаналізовано методи створення і використання сфальсифікованих офіційних документів у сучасних інформаційних операціях. Розглянуто технології створення «фейкових» наказів та листів для дестабілізації державних інституцій. Визначено роль електронного документообігу в системі національної інформаційної безпеки та способи протидії документальним маніпуляціям.*

*Ключові слова: інформаційна війна, офіційний документ, маніпуляція, верифікація, цифрова фальсифікація.*

Сучасний етап розвитку суспільства характеризується стрімким поширенням інформаційних технологій, що суттєво впливає на способи ведення інформаційних воєн. Одним із найбільш небезпечних інструментів такого протистояння під час війни за Незалежність України є маніпуляція офіційними документами, що полягає у навмисному спотворенні, підробленні або вибіркового використанні документальної інформації з метою маніпулятивного впливу на громадську думку, дискредитації державних інституцій та дестабілізації суспільства [1; 2].

Інформаційна війна наразі виходить за межі поширення фейкових новин у соціальних мережах [3]. Особливу загрозу становлять спеціально сфальсифіко-

вані офіційні документи, які завдяки своїй формі викликають високий рівень довіри серед населення. Наявність державної символіки, підписів та печаток формує у громадян сприйняття достовірності, що активно використовується з маніпулятивною метою.

Сучасні цифрові технології значно спростили процес створення підроблених документів. Серед основних способів маніпуляції можна виокремити створення так званих «документів-привидів», тобто повністю вигаданих матеріалів, які імітують офіційні накази чи розпорядження. Такі документи швидко поширюються через соціальні мережі та месенджери, що може спровокувати паніку ще до моменту їх офіційного спростування.

Іншим поширеним методом є використання «напівправди», коли в автентичний документ спеціально внесено незначні зміни, наприклад, у числових даних або формулюваннях. Незважаючи на мінімальні правки, зміст документа буде істотно викривлений. Це призводить до невідповідного розуміння інформації.

Також поширеним є штучне виривання інформації з контексту, коли окремі фрагменти службових документів подають скорочено, що дає змогу формувати хибне уявлення про ситуацію.

В умовах цифровізації суттєво змінюється роль фахівців у документознавчій сфері. Сьогодні вони виконують не лише функції обліку та зберігання документів, але й забезпечують інформаційну безпеку. Особливо актуальною є проблема «візуальної довіри», коли користувачі сприймають зображення документа як доказ його автентичності, хоча в цифровому середовищі це лише графічний файл, який легко піддається редагуванню.

Важливу роль у протидії маніпуляціям відіграють сучасні інформаційні технології та системи електронного документообігу. Використання кваліфікованого електронного підпису забезпечує автентичність і цілісність документів, а впровадження електронних реєстрів дає змогу перевіряти їх походження. Додатковим інструментом є застосування QR-кодів, які надають можливість швидко перевіряти документи через офіційні джерела. Використання криптографічних методів захисту та автоматизованих систем верифікації значно знижує ризики підроблення документів.

Особливо значущим є розвиток критичного мислення в суспільстві. Громадяни повинні усвідомлювати необхідність перевіряти інформацію через офіційні ресурси та не довіряти неперевіреному джерелам в інтернет-мережі. Допомогають їм у цьому не лише документознавці, криміналісти, але й медійники, які верифікують, дешифрують і легітимізують документи в інфопросторі. Українські й зарубіжні журналісти стали не лише ретрансляторами офіційних повідомлень, а й «фільтром» їх автентичності – виявляють документальні маніпуляції, цифрові фальсифікації (дипфейки, підроблені реєстри тощо) [4]. Сучасні репортери з OSINT та з розслідувального напрямку ефективно ідентифікують різні документальні фальсифікації: витoki секретних даних (Leaks), штучні вкиди дезінформаційних документів тощо. Якщо журналіст вводить документ в інформаційне поле, то несе особисту відповідальність і ризикує іміджем видання, в якому він працює. Медійник повинен не лише виявити документ, а й фахово його проаналізувати, відсікти спроби ворожих інфооперацій.

Отже, маніпуляція офіційними документами є потужним інструментом інформаційних воєн, що здатен суттєво впливати на стабільність держави. Ефективна протидія цьому явищу можлива лише за умови поєднання сучасних інформаційних технологій, надійних систем електронного документообігу, високого рівня інформаційної культури суспільства, спільних зусиль фахівців з документознавства та медіажурналістики.

#### Список використаних джерел

1. Бадер А., Вовк С. Маніпулятивний вплив друкованих та електронних джерел у реалізації інформаційного складника сучасного збройного насилля. *Літопис Волині*. 2023. № 29. С. 133–141.
2. Ларіончева Н. Маніпуляція як ключовий інструмент інформаційної війни в епоху ЗМІ та соціальних мереж. *Науково-теоретичний альманах «Грані»*. 2025. Т. 28, № 1. С. 176–181.
3. Литвинська С. В. Роль журналістики в умовах інформаційної війни: досвід України. *Наукові праці Міжрегіональної Академії управління персоналом. Філологія*. 2025. Вип. 3(17). С. 127–134. URL: <https://journals.maup.com.ua/index.php/philology/article/view/5205>
4. Литвинська С. В., Герасимович А. В., Герасимович М. В. Журналістика в епоху цифровізації: трансформація форматів і стилів. *Вчені записки ТНУ імені В. І. Вернадського. Серія: Філологія. Журналістика*. 2025. Т. 36(75), № 5, ч. 2. С. 238–244. URL: [https://philol.vernadsky-journals.in.ua/journals/2025/5\\_2025/part\\_2/38.pdf](https://philol.vernadsky-journals.in.ua/journals/2025/5_2025/part_2/38.pdf)



УДК: 004.056:342.8

**Черняк Яків Сергійович**

*(наук. керівник – д-р екон. наук, професор Анісімова О. М.)*

*Донецький національний університет імені Василя Стуса, м. Вінниця*

### **ВРАЗЛИВОСТІ ЗАБЕЗПЕЧЕННЯ ТАЄМНОСТІ ГОЛОСУВАННЯ В ДОКУМЕНТАЦІЙНОМУ ТА ТЕХНІЧНОМУ ВИМІРАХ**

*Анотація. У роботі досліджено проблеми забезпечення таємності голосування крізь призму документаційних, фізичних і технічних вразливостей. Виявлено основні механізми потенційної деанонізації результатів голосування, зокрема через особливості оформлення бюлетенів, процедурні недоліки організації голосування та можливість біометричної ідентифікації. Запропоновано комплекс заходів щодо мінімізації ризиків, зокрема технічну стандартизацію, процедурну хаотизацію та впровадження біометричних бар'єрів.*

*Ключові слова: таємниця голосування, документаційне забезпечення, деанонізація, технічний захист інформації, електронне голосування, біометричні сліди.*

Актуальність дослідження зумовлена зростанням ролі інформаційних технологій і цифрових комунікацій у процесах організації голосування, що супроводжується появою нових ризиків порушення його таємності. Традиційне розуміння анонімності як відсутності прямої ідентифікації особи вже не є достатнім, оскільки сучасні технічні, біометричні та документаційні чинники створюють додаткові можливості для деанонізації результатів волевиявлення. Особливої ваги це набуває в умовах впровадження електронного голосування та цифрові-