

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-

зації управлінських процесів, де питання захисту інформації безпосередньо пов'язане з довірою до результатів голосування.

Особливої уваги потребує дотримання встановленої процедури таємного голосування, оскільки саме вона є ключовою гарантією забезпечення анонімності волевиявлення. На рівні держави закріплено відповідні нормативно-правові акти, які регламентують порядок організації голосування, вимоги до приміщень, використання виборчих бюлетенів і забезпечення умов, що унеможливають ідентифікацію виборця [1]. Такі вимоги мають не формальний, а принциповий характер, адже навіть незначне відхилення від процедури може створити передумови для порушення таємності голосування. У цьому контексті дотримання регламентованих норм треба розглядати як елемент системи інформаційної безпеки, що забезпечує захист результатів голосування від прямої та непрямой деанонізації.

Базові вимоги до організації таємного голосування передбачають створення умов, за яких виборець здійснює волевиявлення без стороннього контролю та можливості ідентифікації його вибору. Зокрема, обов'язковим є використання спеціально обладнаних кабін або кімнат для таємного голосування, що виключають присутність інших осіб під час заповнення бюлетеня. Виборчі скриньки мають бути опломбованими та розміщеними так, щоб унеможливити відстеження порядку вкидання бюлетенів. Процедура видачі бюлетенів здійснюється індивідуально після ідентифікації виборця, причому забороняється будь-яке маркування, яке може розкрити його вибір. Окремо встановлюється заборона фотографування та відеофіксації заповненого бюлетеня, передачі його третім особам або демонстрації змісту волевиявлення. Сукупність цих вимог формує процедурну основу, яка має забезпечувати реальну, а не декларативну таємність голосування.

Додатково варто зазначити, що регламентні процедури проведення таємного голосування на рівні парламенту деталізують механізми реалізації цих вимог та підкреслюють їх обов'язковість саме для народних депутатів України. Відповідно до положень Регламенту Верховної Ради України, таємне голосування здійснюється народними депутатами особисто у спеціально обладнаних кабінах шляхом заповнення бюлетеня з подальшим опусканням його до виборчої скриньки. Видача бюлетенів відбувається індивідуально з обов'язковою фіксацією їх отримання, що забезпечує контроль за участю у голосуванні без розкриття змісту волевиявлення. Отже, регламентні норми поєднують персоніфікований доступ до процедури голосування з повною деперсоналізацією його результату, що підтверджує визначальну роль процедурної дисципліни у забезпеченні таємності голосування [2].

Таємність голосування є базовим принципом демократичних процедур, що традиційно розглядається як відсутність прямої ідентифікації особи у бюлетені. Проте в сучасних умовах цього підходу недостатньо, оскільки технічні та документальні аспекти організації голосування створюють нові ризики деанонізації. Аналіз чинного законодавства показує, що нормативне регулювання здебільшого зосереджене на процедурних вимогах [1] і відповідальності за порушення [3; 5; 6], тоді як конкретні ознаки компрометації бюлетеня залишаються недостатньо визначеними [4].

Під час дослідження виявлено три ключові групи вразливостей (рис. 1). Перша пов'язана з можливістю використання індивідуальних маркерів у бюлетенях. Відмінності у відтінках чорнила, характері натиску, згинах паперу або навмисних позначках можуть використовуватися для подальшої ідентифікації виборця. Друга група стосується процедурних аспектів організації голосування. Лінійна видача бюлетенів і відсутність перемішування створюють можливість встановлення зв'язку між порядком голосування та конкретним бюлетенем, особливо в умовах невеликої кількості учасників. Третя група пов'язана з біометричними та фізичними характеристиками документів. Паперові носії здатні зберігати відбитки пальців, ДНК-сліди та інші фізичні маркери, що потенційно можуть бути використані для деанонімізації.



Рисунок 1 – Вразливості процедури голосування за чинними вимогами

Для мінімізації зазначених ризиків запропоновано комплекс заходів. Технічна стандартизація передбачає використання уніфікованих матеріалів і засобів заповнення бюлетенів, що унеможлиблює індивідуалізацію почерку. Процесуальна хаотизація включає застосування кількох скриньок для голосування та обов'язкове перемішування бюлетенів перед підрахунком. Біометрична нейтралізація полягає у використанні одноразових рукавичок усіма учасниками процесу для усунення фізичних слідів.

Використання цих методів має і психологічний ефект, що збільшує рівень довіри учасників голосування. Це прибирає страх перед можливими переслідуваннями, особливо у малих колективах або колективах із тиранічним керівництвом.

Окремим напрямом є використання електронного голосування, яке дає змогу усунути фізичні маркери та автоматизувати процес підрахунку. Водночас та-

ка форма має власні ризики, зокрема можливість ідентифікації за часом входу користувача, залежність від технічної інфраструктури та обмежений контроль над системою. Додатковим викликом є використання технологій штучного інтелекту, які можуть застосовуватися як для підвищення ефективності обробки результатів і виявлення аномалій, так і потенційно для аналізу поведінкових або технічних патернів користувачів з метою їх непрямой ідентифікації [7].

**Висновки.** Забезпечення таємності голосування потребує комплексного підходу, що поєднує правові, документаційні та технічні механізми і є динамічною системою із багатьма змінними. Лише за умови системного контролю кожного етапу голосування можна гарантувати реальну анонімність волевиявлення.

### Список використаних джерел

1. Про вимоги до приміщень виборчих комісій та приміщень для голосування, нормативи облаштування приміщень дільничних виборчих комісій і приміщень для голосування, перелік та норми забезпечення виборчих комісій транспортними засобами, засобами зв'язку, обладнанням, інвентарем, іншими матеріальними цінностями. Офіційний вебпортал парламенту України. URL: <https://zakon.rada.gov.ua/laws/show/v0164359-20#n22> (дата звернення: 29.03.2026).
2. Про Регламент Верховної Ради України Стаття 39. Організація таємного голосування та встановлення його результатів. Головна – Законодавство України 2019 рік. URL: [https://kodeksy.com.ua/pro\\_reglament\\_verhovnoyi\\_radi\\_ukrayini/39.htm](https://kodeksy.com.ua/pro_reglament_verhovnoyi_radi_ukrayini/39.htm) (дата звернення: 29.03.2026).
3. Стаття 158. Надання неправдивих відомостей до органу ведення Державного реєстру виборців або інше несанкціоноване втручання в роботу Державного реєстру виборців – Кримінальний кодекс України | Protocol. Безкоштовний сервіс для вирішення Юридичних питань № 1 в Україні! URL: [https://protocol.ua/ua/kriminalniy\\_kodeks\\_ukraini\\_stattya\\_158/](https://protocol.ua/ua/kriminalniy_kodeks_ukraini_stattya_158/) (дата звернення: 29.03.2026).
4. Стаття 158-1. Незаконне використання виборчого бюлетеня, бюлетеня для голосування на референдумі, голосування виборцем, учасником референдуму більше одного разу, викрадення, пошкодження, приховування або знищення виборчого бюлетеня, бюлетеня для голосування на референдумі – Кримінальний кодекс України | Protocol. Безкоштовний сервіс для вирішення Юридичних питань № 1 в Україні! URL: [https://protocol.ua/ua/kriminalniy\\_kodeks\\_ukraini\\_stattya\\_158\\_1/](https://protocol.ua/ua/kriminalniy_kodeks_ukraini_stattya_158_1/) (дата звернення: 29.03.2026).
5. Стаття 158-2. Незаконне знищення або пошкодження виборчої документації або документації референдуму – Кримінальний кодекс України | Protocol. Безкоштовний сервіс для вирішення Юридичних питань № 1 в Україні. URL: [https://protocol.ua/ua/kriminalniy\\_kodeks\\_ukraini\\_stattya\\_158\\_2/](https://protocol.ua/ua/kriminalniy_kodeks_ukraini_stattya_158_2/) (дата звернення: 29.03.2026).
6. Стаття 159. Порушення таємниці голосування: Кримінальний кодекс України | Protocol. Безкоштовний сервіс для вирішення Юридичних питань № 1 в Україні! URL: [https://protocol.ua/ua/kriminalniy\\_kodeks\\_ukraini\\_stattya\\_159/](https://protocol.ua/ua/kriminalniy_kodeks_ukraini_stattya_159/) (дата звернення: 29.03.2026).
7. Анісімова О. М. Еволюція інформаційних технологій: від автоматизації процесів до штучного інтелекту. *Інформація та соціум*. 2025. С. 8–11. URL: <https://jias.donnu.edu.ua/article/view/18819> (дата звернення: 29.03.2026).

