

УДК 342.8:342.56:343.35:004.056(477)

DOI <https://doi.org/10.32689/3083-7359.2026.2.13>

АДМІНІСТРАТИВНО-ПРАВОВІ ГАРАНТІЇ ДОСТОВІРНОСТІ ЦИФРОВОЇ ІНФОРМАЦІЇ У СУДОВОМУ ЗАХИСТІ ВИБОРЧИХ ПРАВ І ПРОТИДІЇ КОРУПЦІЙНИМ РИЗИКАМ

О. І. Полотнянко, М. В. Сандига

ADMINISTRATIVE AND LEGAL GUARANTEES OF DIGITAL INFORMATION RELIABILITY IN JUDICIAL PROTECTION OF ELECTORAL RIGHTS AND COUNTERING CORRUPTION RISKS

Oksana Polotnianko, Maksym Sandyha

Анотація. У статті досліджено адміністративно-правові гарантії достовірності цифрової інформації у судовому захисті виборчих прав та протидії корупційним ризикам виборчого процесу України з урахуванням підготовки до виборів після припинення або скасування воєнного стану. Розмежовано чотири масиви інформації: офіційні виборчі дані; матеріали передвиборної агітації та політичної реклами; контент цифрових платформ; персональні дані виборців. Доведено, що поряд із належним адміністративним управлінням цими масивами необхідний процесуальний маршрут їх перетворення на електронні докази, придатні для своєчасного судового контролю.

Запропоновано модель подвійного контуру доказової довіри. Адміністративний контур охоплює автентифікацію джерела, журналювання, простежуваність фінансування політичної реклами, мінімізацію персональних даних і невідкладне збереження матеріалів. Судовий контур передбачає перевірку належності, допустимості, достовірності, цілісності та достатності електронних доказів із дотриманням рівності сторін і скорочених виборчих строків. Показано, що розбіжності у даних про оплату реклами, цифрові сліди підкупу виборців, зловживання адміністративними ресурсами чи маніпуляції реєстрами є сигналами для перевірки, але не автоматичним доказом корупційного або кримінального правопорушення. Наукова новизна полягає у цифровому доказовому маршруті від виникнення інформації до її судової оцінки.

Ключові слова: виборчий процес, судовий захист, електронні докази, цифрова інформація, достовірність, корупційні ризики, політичне фінансування, цифрові платформи, Центральна виборча комісія, післявоєнні вибори.

Abstract. The article examines administrative and legal guarantees of digital information reliability in judicial protection of electoral rights and in countering corruption risks in Ukraine's electoral process, with particular attention to elections after the termination or cancellation of martial law. Four information domains are distinguished: official electoral data; campaign and political advertising materials; digital-platform content; and voters' personal data. Effective administration of these domains must be complemented by a procedural route through which relevant records become electronic evidence suitable for timely judicial review.

A dual-loop model of evidentiary trust is proposed. The administrative loop covers source authentication, logging, traceability of political-advertising finance, data minimisation and prompt preservation. The judicial loop verifies relevance, admissibility, reliability, integrity and sufficiency while safeguarding equality of arms and expedited electoral deadlines. Discrepancies in advertising payments, digital traces of voter bribery, misuse of administrative resources or register manipulation constitute risk indicators requiring verification, not automatic proof of a corruption-related or criminal offence. The study's novelty is a digital evidentiary route from information creation to judicial assessment.

Key words: electoral process, judicial protection, electronic evidence, digital information, reliability, corruption risks, political finance, digital platforms, Central Election Commission, post-war elections.

1. Вступ. Цифрове середовище змінило не лише спосіб ведення передвиборної агітації, а й інфраструктуру захисту виборчих прав. Відомості про кандидатів, місце голосування, фінансування реклами, перебіг підрахунку та результати поширюються через різні системи й у разі спору можуть набути значення електронних доказів. Помилка, підrobка або видалення цифрового запису здатні поширитися швидше, ніж офіційне спростування чи судове забезпечення доказу. Порівняльний аналіз

підтверджує потребу поєднувати цифрові інновації з правозахисними і процесуальними гарантіями (Skorokhod, 2024).

Для України питання особливо актуальне з огляду на майбутнє відновлення виборчих процесів після припинення або скасування воєнного стану. Центральна виборча комісія у січні 2026 року схвалила пропозиції щодо законодавчого врегулювання особливостей загальнодержавних виборів у післявоєнний період. Складність полягатиме не тільки

в організації голосування для переміщених громадян і військовослужбовців, а й у відновленні актуальності реєстрів, захисті цифрових систем та забезпеченні однаково доступної інформації (Central Election Commission of Ukraine, 2026).

Конституційні права громадян брати участь в управлінні державними справами, вільно обирати, висловлювати погляди й захищати приватність доповнюються правом на ефективний судовий захист. Тому протидія інформаційним маніпуляціям і корупційним ризикам не може виправдовувати загальний контроль над політичною дискусією. Адміністративні заходи мають бути законними, необхідними, пропорційними, документованими та придатними до оперативного оскарження.

Виборчий кодекс України, закони про Центральну виборчу комісію, Державний реєстр виборців і захист персональних даних визначають базові правила створення та використання цифрової інформації. Кодекс адміністративного судочинства України регулює електронні докази і спеціальні строки у виборчих справах. Кримінальний кодекс та Закон України «Про запобігання корупції» формують окремий контур правової кваліфікації, коли цифрові матеріали вказують на підкуп виборців, незаконне фінансування, зловживання ресурсами або інші ознаки правопорушення. Водночас жодна технічна розбіжність сама по собі не встановлює складу правопорушення (Verkhovna Rada of Ukraine, 2019; 2005; 2001; 2014).

Європейські стандарти швидко розвиваються. Регламент ЄС 2024/900 встановлює правила прозорості та таргетування політичної реклами. Digital Services Act передбачає системні обов'язки великих платформ щодо ризиків, прозорості реклами і доступу дослідників до даних. Венеційська комісія у 2024 році розтлумачила Кодекс належної практики у виборчих справах стосовно цифрових технологій і штучного інтелекту, наголосивши на вільному формуванні волі, рівності, прозорості та дієвому незалежному контролі (Venice Commission, 2024).

Українські дослідження цифрового виборчого середовища пов'язують політичне мікротаргетування, синтетичний контент і приховане фінансування з ризиками непрозорого профілювання, дезінформації та нерівності політичної конкуренції. Дослідники електронних доказів додатково наголошують на значенні первинного джерела, метаданих, цілісності та належного збереження цифрового матеріалу. Отже, регу-

лювання має спиратися на доказувану шкоду й перевірений доказовий ланцюг, а не на припущення про автоматичний вплив будь-якого алгоритму (Riznyk, 2023; Zharovska, 2025; Afanasieva, 2026; Yosyfovych, 2024).

Невирішеною залишається проблема переходу від адміністративної фіксації цифрового інциденту до належного судового доказування, особливо коли порушення виборчих правил одночасно створює корупційний або кримінально-правовий ризик. Метою статті є розроблення адміністративно-правових гарантій достовірності цифрової інформації у судовому захисті виборчих прав і протидії корупційним ризикам. Завданнями є класифікувати інформаційні масиви, визначити їх доказовий статус, сформувати модель розподілу повноважень і запропонувати цифровий доказовий маршрут.

2. Матеріали і методи. Об'єктом дослідження є адміністративно-правові відносини у сфері інформаційного забезпечення виборів і судового захисту виборчих прав. Предметом – гарантії достовірності, збереження, простежуваності та судової оцінки цифрової інформації, що може свідчити про порушення виборчих прав або корупційні ризики. Джерельну базу становлять Конституція і законодавство України, офіційні матеріали ЦВК, акти ЄС, документи Венеційської комісії та Ради Європи, а також статті українських учених про цифрові вибори й електронні докази.

Застосовано формально-юридичний метод для аналізу компетенції органів і процесуальних вимог; системний – для побудови зв'язку між видами інформації та способами захисту; порівняльно-правовий – для зіставлення українського регулювання з європейськими стандартами; метод правового моделювання – для розроблення подвійного контуру доказової довіри; метод пропорційності – для оцінки втручання у свободу вираження, приватність і рівність учасників.

Дослідження не оцінює правдивість конкретних політичних висловлювань і не підміняє кримінально-правову кваліфікацію адміністративною оцінкою ризику. Межі аналізу охоплюють достовірність походження, прозорість фінансування й таргетування, законність обробки персональних даних, збереження електронних доказів і процедури їх подання та перевірки судом.

3. Результати та обговорення. Першим результатом є поділ цифрової інформації на чотири правові масиви та визначення їх потенційного доказового статусу. Офіційні виборчі дані створюються виборчими комісіями; політична реклама потребує прозорості

замовника, вартості й критеріїв таргетування; контент користувачів і медіа охороняється свободою вираження; дані виборців мають спеціальний режим приватності. У спорі кожен масив оцінюється не за назвою носія, а за походженням, способом отримання, цілісністю та зв'язком із предметом доказування.

Змішування цих масивів породжує дві крайності. Перша – вимога до виборчих органів встановлювати істинність усієї політичної дискусії. Друга – відмова від фіксації та збереження інформації навіть за підроблення рішення ЦВК, прихованої оплати реклами, цифрових ознак підкupu виборців або незаконного використання реєстру. Правова модель має відокремлювати сигнал ризику, адміністративне порушення, доказ у судовій справі та встановлений склад правопорушення.

Перша гарантія – автентифікація джерела. Кожне офіційне цифрове повідомлення про процедуру, реєстрацію, голосування або результати повинно мати перевірюваний канал походження, єдиний ідентифікатор, час публікації та доступний архів змін. Доцільним є використання кваліфікованого електронного підпису для машиночитаних наборів і відкритого реєстру офіційних повідомлень, який дозволяє швидко відрізнити справжній документ від підробки.

Друга гарантія – простежуваність політичної реклами. Користувач повинен бачити замовника, період розміщення, основні параметри аудиторії, джерело фінансування і те, чи застосовано синтетичне зображення або голос. Публічний репозитарій реклами має бути доступним спостерігачам, журналістам і дослідникам. Водночас розкриття параметрів не повинно дозволяти ідентифікувати конкретного виборця або відтворити його чутливий профіль.

Третя гарантія – мінімізація персональних даних. Державний реєстр виборців містить дані, необхідні для реалізації виборчого права, але доступ до них не є ресурсом політичного профілювання. Партії, поставальники реклами й уповноважені органи повинні мати правову підставу для кожної операції, визначений строк зберігання та заборону несумісного повторного використання. Журнали доступу зберігаються так, щоб за потреби підтвердити або спростувати несанкціоноване втручання (Verkhovna Rada of Ukraine, 2007; 2010).

Четверта гарантія – швидке виправлення офіційної помилки. Виборчі органи повинні мати процедуру, за якою неправильне повідомлення не просто видаляється,

а позначається, виправляється і зберігається в журналі версій. Якщо помилка могла вплинути на реалізацію права, виправлення поширюється тим самим або еквівалентним каналом і містить практичне роз'яснення для виборця. Така процедура підвищує довіру більше, ніж спроба приховати факт виправлення.

П'ята гарантія – незалежне оскарження й своєчасне забезпечення доказів. Рішення про маркування, обмеження реклами, відмову в доступі до даних або вимогу надати інформацію мають бути мотивованими, повідомленими адресату й придатними до швидкого судового перегляду. Через скорочені виборчі строки суд повинен мати доступ до первинного цифрового об'єкта, метаданих і журналу його збереження, а учасники – рівну можливість перевірити ці матеріали (Yosyfovych, 2024).

На основі гарантій запропоновано модель подвійного контуру доказової довіри. Адміністративний контур включає визначення категорії даних, перевірку походження, фіксацію метаданих, оцінку ризику, збереження матеріалу, повідомлення адресата та передання за належною компетенцією. Судовий контур включає перевірку належності, допустимості, достовірності, цілісності й достатності доказів, застосування пропорційного способу захисту та можливість перегляду рішення.

Ризик-орієнтована реакція передбачає різні заходи. Для підробленого офіційного документа пріоритетом є спростування і збереження цифрового сліду; для немаркованої або приховано оплаченої реклами – розкриття замовника, фіксація даних про платіж і передання матеріалів компетентному органу; для дискусійного політичного твердження – перевага відповіді й плюралізму; для витоку даних – локалізація, документування та захист постраждалих. Подальша юридична кваліфікація залежить від сукупності доказів, суб'єкта, умислу та наслідків.

Синтетичний контент потребує окремої процедури. Заборона всіх матеріалів, створених із використанням ШІ, була б непропорційною, оскільки технологія може застосовуватися для перекладу, доступності або дизайну. Юридично значущим має бути введення в оману щодо особи, події чи офіційного джерела. Обов'язкове маркування, збереження даних про походження та швидка процедура реагування на шкідливі підробки є точнішими інструментами.

Венеційська комісія пов'язує цифрові технології з базовими принципами загального,

рівного, вільного, таємного і прямого виборчого права. Звідси випливає, що алгоритмічне таргетування не можна оцінювати лише як рекламну технологію. Якщо різні групи виборців отримують взаємовиключні обіцянки, приховані від публічного контролю, порушується прозорість політичного змагання, навіть коли кожне повідомлення окремо не є незаконним.

Центральна виборча комісія повинна координувати стандарти офіційної інформації, вести реєстр повідомлень, визначати машиночитані формати та зберігати журнали інцидентів. Вона не встановлює істинності політичних програм і не підміняє суд чи правоохоронний орган. Національна рада України з питань телебачення і радіомовлення діє в межах медійної компетенції, Уповноважений Верховної Ради України з прав людини контролює захист персональних даних, а НАЗК – передбачені законом аспекти політичного фінансування та запобігання корупції.

Кібербезпекові суб'єкти забезпечують захист реєстрів, обмін індикаторами атак і перевірку резервного відновлення. Політичні партії відповідають за походження матеріалів, законність коштів, даних і підрядників. Платформи забезпечують прозорість реклами, належне збереження записів і виконання законних вимог. Правоохоронні органи перевіряють ознаки правопорушень, а суд здійснює незалежну оцінку доказів і захист прав. Такий розподіл не допускає концентрації несумісних функцій.

Протокол має бути технічно нейтральним. Закон повинен визначати результат – перевірюване походження, прозорість і захист прав – а не закріплювати конкретну платформу або криптографічну технологію. Інакше норма швидко застаріє. Технічні стандарти можуть затверджуватися підзаконними актами після відкритого тестування, оцінки впливу на приватність і консультацій із виборчими органами та громадянським суспільством.

Післявоєнний контекст вимагає доступності інформації для громадян за кордоном, внутрішньо переміщених осіб, військовослужбовців і людей на територіях із пошкодженою інфраструктурою. Цифровий канал не може бути єдиним. Кожне критичне повідомлення повинно мати резервні способи поширення, зрозумілу мову й доступний формат. Інакше цифровізація формально підвищить швидкість, але поглибить нерівність участі.

До Виборчого кодексу доцільно включити поняття цифрової політичної реклами, син-

тетичного виборчого контенту, репозитарію реклами та протоколу автентичності офіційних даних. Окремо слід закріпити обов'язки щодо строків збереження цифрових записів, видачі завіреної технічної інформації, маркування, незалежного оскарження і захисту персональних даних. Процесуальні норми мають узгоджувати адміністративну фіксацію з вимогами до електронних доказів у суді.

Ефективність моделі слід оцінювати за часом підтвердження джерела, повнотою репозитарію реклами, строком збереження доказу, кількістю мотивованих і скасованих рішень, тривалістю судового розгляду, випадками неправомірного доступу до реєстру та часткою матеріалів, цілісність яких підтверджено. Кількість видалених повідомлень або переданих матеріалів не доводить сама по собі ефективність протидії корупційним ризикам.

Подальша конкретизація потребує розмежування достовірності, автентичності, законності, належності та достатності. Автентичний документ може містити помилку; достовірне повідомлення може бути поширене з порушенням правил агітації; розбіжність у фінансовій звітності може вимагати перевірки, але не доводити умисел. Адміністративний орган фіксує факт і реагує в межах компетенції, тоді як суд оцінює докази у сукупності та обирає спосіб захисту.

Для офіційної виборчої інформації пропонується протокол джерела. Кожне повідомлення Центральної виборчої комісії або іншого уповноваженого органу отримує постійний ідентифікатор, дату, версію, електронний підпис, історію виправлень і машинозчитуване посилання на першоджерело. Копія на платформі не повинна вважатися самостійним джерелом. Якщо текст змінено через технічну або змістовну помилку, попередня версія зберігається з позначкою, а користувач бачить сутність виправлення.

Резервування офіційних каналів має поєднувати доступність і контроль автентичності. Під час кібератаки або відключення основного сайту громадянин повинен заздалегідь знати альтернативні домени, телефонні лінії, мовників і територіальні канали. Перелік резервів оприлюднюється до початку процесу та підписується ЦВК. Створення нового каналу вже під час інциденту без можливості перевірки відкриває простір для підроблення.

Для даних Державного реєстру виборців основним є принцип функціонального розмежування. Персональні дані використовуються лише для визначених законом

завдань, а аналітичні потреби задовольняються агрегованими або знеособленими наборами. Працівник отримує доступ до мінімально необхідної функції, кожна операція журналюється, а нетипові запити перевіряються. Масове копіювання реєстру не може виправдовуватися зручністю адміністрування.

Якість реєстру потребує процедур виправлення, які є доступними до виборів і достатньо швидкими під час виборчого періоду. Виборець повинен мати можливість перевірити відомості, отримати зрозуміле пояснення, подати підтвердження й оскаржити відмову. Електронний канал доповнює, а не замінює фізичний. Для внутрішньо переміщених осіб, військовослужбовців і громадян за кордоном потрібні окремі інформаційні маршрути, але базові стандарти перевірки й захисту залишаються однаковими.

Політична реклама повинна мати видиме маркування без необхідності відкривати додаткове меню. Мінімальний набір включає замовника, платника, період показу, суму або діапазон витрат, критерії аудиторії, використання персональних даних і посилання на репозиторій. Регламент ЄС 2024/900 демонструє перехід від загальної вимоги прозорості до стандартизованих повідомлень. Для України важливо забезпечити однакове застосування до традиційних медіа, платформ та інших цифрових посередників.

Репозитарій реклами повинен бути придатним і для публічного контролю, і для судового доказування. Пошук за замовником, періодом, платформою, аудиторією та витратами має працювати без спеціального програмування; дані – завантажуватися у відкритому форматі; видалене оголошення – залишатися в архіві з часом і правовою підставою припинення показу. Строк зберігання має охоплювати строки оскарження, післявиборчого аудиту та, за законною вимогою, перевірки можливого правопорушення.

Окремої уваги потребує розмежування політичної реклами, агітації, журналістського матеріалу, особистого висловлювання та інформації органу влади. Критеріями можуть бути оплата, контроль над змістом, координація з учасником виборів, мета впливу й системність поширення. Один критерій не є достатнім. Невизначеність вирішується через мотивоване рішення, яке може бути швидко оскаржене, а не через автоматичне блокування.

Мікротаргетинг створює ризик фрагментації публічної дискусії. Різні групи можуть отримувати несумісні обіцянки,

а спостерігачі не бачать загальної кампанії. Мінімальною гарантією є доступність усіх варіантів оголошень і опису аудиторій. Використання чутливих даних або висновків про політичні погляди потребує особливо суворого обмеження. Згода, включена до загальних умов сервісу, не повинна автоматично вважатися достатньою для політичного профілювання.

Платформи мають виконувати процедурні, а не квазісудові функції. Вони забезпечують маркування, архів, приймання повідомлень, невідкладне збереження доказів і виконання законного рішення. Встановлення порушення, вини та санкції належить компетентним органам і суду. Після належного запиту платформа повинна зберегти первинний запис, історію редагувань, параметри показу й платежу, не розкриваючи надмірні персональні дані.

Ризик-орієнтований нагляд означає, що пріоритет отримують системні й масштабні порушення, приховане фінансування, цифрові ознаки підкупу виборців, використання чутливих даних, маніпуляції реєстром і підроблення офіційної інформації. Такі факти можуть стосуватися різних складів правопорушень, тому потребують перевірки за належною підслідністю та юрисдикцією, а не автоматичного віднесення кожного інциденту до корупційного злочину (Kuznietsov, 2024; Podoliaka et al., 2025).

Синтетичний контент потребує правила походження. Маркування потрібне тоді, коли матеріал істотно створений або змінений і може ввести виборця в оману щодо реальної особи, події чи висловлювання. Технічне покращення якості, корекція кольору або доступний переклад не повинні автоматично прирівнюватися до маніпуляції. Закон має визначити відповідального за маркування, спосіб подання та наслідки навмисного приховування.

Заборона синтетичного контенту як загальної категорії була б непропорційною. Законними можуть бути сатира, мистецьке висловлювання, реконструкція й очевидна ілюстрація. Ключовими є контекст, здатність створити помилкове уявлення, суспільний ризик і наявність чіткого повідомлення. Рішення про обмеження повинно бути індивідуальним, мотивованим та обмеженим у часі, а заявник – мати швидкий засіб захисту.

Оперативний протокол ЦВК пропонується поділити на три рівні. Перший охоплює спростування підробленої офіційної інформації; другий – координацію з платформами і кібербезпековими органами для збереження джерела, метаданих та ланцюга пере-

дання; третій – направлення матеріалів компетентному органу або надання їх суду. ЦВК захищає автентичність власних повідомлень, але не вирішує питання про винуватість чи остаточну правову кваліфікацію.

Стандарт електронного доказу повинен забезпечувати належність, допустимість, достовірність, цілісність і відтворюваність. Знімок екрана без адреси, дати, автора, параметрів аудиторії, історії редагувань або факту оплати часто не дає змоги перевірити походження. Тому цифровий доказовий маршрут включає первинний файл або запис, технічні метадані, опис способу отримання, контрольне значення, журнал доступу й передавання та можливість дослідження іншою стороною (Akhtyrskaya, 2023; Turov, 2024; Yosyfovych, 2024).

Швидкість розгляду є елементом ефективного судового захисту. Рішення після завершення голосування може не усунути вплив незаконної реклами чи перешкод у реалізації права. Доцільно визначити скорочені строки для реєстрації звернення, збереження доказу, первинної адміністративної оцінки, тимчасового заходу і судового перегляду. Тимчасове обмеження застосовується лише за очевидного ризику значної шкоди, є мотивованим і втрачає силу без своєчасного подальшого рішення.

Заходи реагування мають бути пропонує різними охопленням, повторності, умислу, прихованню та наслідкам. Окрім штрафу, можливі виправлення маркування, внесення до репозитарію, припинення обробки даних, спростування або передання матеріалів для перевірки. У судовому провадженні спосіб захисту не повинен підміняти встановлення складу адміністративного, кримінального чи корупційного правопорушення уповноваженим органом у визначеній законом процедурі.

Незалежність контролю потребує чіткого розподілу компетенцій. ЦВК забезпечує виборчий процес та офіційну інформацію; орган захисту даних – законність обробки; медіарегулятор – правила медіа; НАЗК – встановлені законом питання політичного фінансування і запобігання корупції; правоохоронні органи – ознаки правопорушень; суд – незалежний перегляд та оцінку доказів. Міжвідомчий протокол має визначати приймання, збереження, пересилання й відстеження матеріалів.

Післявоєнні вибори потребують окремої оцінки інформаційних ризиків. Велика кількість переміщених громадян, виборців за кордоном, військовослужбовців, пошкоджена інфраструктура й тривала дезінформація

створюють нерівний доступ. Інформаційна кампанія повинна починатися завчасно, пояснювати процедури зміни виборчої адреси, доступні канали й строки та не створювати враження, що цифровий інструмент є єдиним способом реалізації права.

Для громадян за кордоном необхідні узгоджені повідомлення ЦВК, дипломатичних установ та офіційних державних каналів. Різні формулювання щодо реєстрації, документів або місця голосування породжують помилки й відкривають простір для шахрайських сервісів. Єдиний протокол джерела дає змогу перевірити актуальність повідомлення, а багатомовні матеріали допомагають залучати приймаючі установи без втрати правової точності.

Цифрова доступність повинна оцінюватися як правова гарантія. Сайт, репозиторій і сервіс перевірки мають працювати на мобільних пристроях, із допоміжними технологіями, за повільного зв'язку та в простій мові. Для особи без електронної ідентифікації зберігається альтернативний канал. Недоступність не можна компенсувати лише загальним номером телефону, якщо він перевантажений або не надає письмового підтвердження.

Медіаграмотність є допоміжним, а не замінним інструментом. Держава повинна навчати перевіряти джерело, архів реклами й позначення синтетичного матеріалу, але не перекладати на виборця всю відповідальність за непрозору систему. Найкраща просвітницька кампанія не виправляє відсутність репозитарію, незаконне профілювання або неможливість оскарження. Тому освіта вбудовується в інституційні гарантії.

Для оцінки результативності пропонуються показники доступності офіційних каналів, часу виправлення помилки, повноти репозитарію, строку збереження електронного доказу, частки записів із підтвердженою цілісністю, строків судового розгляду, кількості скасованих рішень і випадків неправомірного доступу до реєстру. Кількість відкритих перевірок не може бути самостійним показником, оскільки не відображає якість доказів і кінцевий правовий результат.

Дорожня карта охоплює аудит чинних норм, стандартизацію офіційних повідомлень, визначення цифрової політичної реклами, створення репозитарію, протокол збереження доказів, форми міжвідомчого передання, оцінку впливу на захист даних, навчання органів, платформ і суддів, пілотне тестування та незалежний післявиборчий звіт. Кожний етап має бути завершений завчасно, щоб правила

не змінювалися під час активної кампанії без крайньої необхідності.

Обмеження моделі полягає в швидкій зміні технологій і неможливості передбачити всі формати впливу. Тому закон має бути технологічно нейтральним і зосередженим на функції, походженні, оплаті, даних та ризику. Технічні стандарти можуть оновлюватися підзаконно після відкритого тестування й консультацій, але основні права, компетенція та підстави обмеження визначаються законом. Це забезпечує адаптивність без втрати правової визначеності.

Громадські спостерігачі, дослідники й журналісти повинні мати рівний доступ до відкритих цифрових даних. Вибіркове надання інформації окремим організаціям створює нерівність контролю. Інтерфейс репозиторію доповнюється програмним доступом із захистом від зловживань, описом полів і стабільними ідентифікаторами. Обмеження швидкості може бути технічно необхідним, але не повинно унеможлилювати аналіз великих кампаній.

Прозорість реклами має бути пов'язана з контролем політичного фінансування. Дані про платника, суму, період, одержувача та параметри розміщення зіставляються зі звітністю суб'єкта виборчого процесу. Розбіжність формує документований сигнал для перевірки, але не є автоматичним доказом прихованого фінансування, корупційного правопорушення або вини конкретної особи. Доказове значення виникає після перевірки джерела коштів, зв'язку між суб'єктами, умислу й інших обставин.

Платформа повинна мати протокол значного виборчого інциденту. Він охоплює підроблення офіційного каналу, масове приховане фінансування, цифрові ознаки підкупу, витік виборчих даних або координане поширення оманливого синтетичного матеріалу. Протокол визначає контакт із ЦВК, фіксацію часу, невідкладне збереження первинних записів і метаданих, тимчасові заходи, законне передання матеріалів та післяінцидентний звіт (Sachko & Kuznietsov, 2024).

Незалежний аудит репозитарію перевіряє повноту, затримку внесення, правильність маркування, збереження видалених оголошень і доступність пошуку. Аудитор використовує контрольну вибірку з публічних показів та звітності, документує методику й контрольні значення. Виявлена прогалина має строк виправлення, а аудиторський висновок може бути поданий суду разом із первинними даними, але не замінює їх самостійної оцінки.

Норми щодо цифрової інформації потребують післявиборчого перегляду. ЦВК, орган захисту даних, медіарегулятор, НАЗК, правоохоронні органи та судова адміністрація мають готувати агрегований звіт про звернення, збереження доказів, строки, рішення і технічні проблеми без розкриття таємниці провадження чи надмірних персональних даних. Законодавчі зміни повинні спиратися на цей матеріал, судову практику та відкриті консультації.

Таким чином, адміністративно-правова гарантія достовірності є системою простежуваності, збереження і захисту, а не окремою забороною неправдивого контенту. Її ефективність визначається тим, чи може особа знайти першоджерело, побачити замовника, захистити дані, зафіксувати цифровий слід, перевірити ланцюг передання і своєчасно оскаржити рішення. Подвійний контур доказової довіри поєднує адміністративну фіксацію із незалежною судовою оцінкою.

4. Висновки. Достовірність цифрової інформації у виборчому процесі охоплює автентичність офіційних даних, прозорість політичної реклами, захист персональних даних, свободу політичної дискусії, збереження електронних доказів і дієвий судовий захист. Ці елементи мають регулюватися взаємопов'язано, але не підміняти один одного.

Запропоновано розмежувати чотири інформаційні масиви та чотири юридичні стани цифрового матеріалу: сигнал ризику, зафіксований адміністративний факт, електронний доказ і встановлене правопорушення. Таке розмежування дозволяє реагувати на приховане фінансування, підкуп, зловживання ресурсами або маніпуляції даними без презумпції винуватості й без перетворення ЦВК на орган політичної цензури.

Науковою новизною є модель подвійного контуру доказової довіри та цифровий доказовий маршрут. Адміністративний контур забезпечує автентифікацію, журналювання, збереження, оцінку ризику й передання за компетенцією; судовий – перевірку належності, допустимості, достовірності, цілісності і достатності матеріалів із дотриманням рівності сторін та пропорційності втручання.

Для післявоєнних виборів необхідно поєднати цифрові інструменти з резервними каналами, захистом реєстрів і скороченими процедурами забезпечення доказів. Законодавчі зміни мають завчасно визначити строки збереження записів, обов'язки платформ, міжвідомче передання, процесуальні гарантії та межі використання персональних даних.

Подальші дослідження доцільно спрямувати на апробацію цифрового доказового маршруту в модельних виборчих спорах, визначення стандартів судового витребування даних у платформ, оцінку доказового значення реєстрів політичної реклами та розмежування виборчих, адміністративних, кримінальних і корупційних правопорушень у цифровому середовищі.

Конфлікт інтересів. Автори декларують відсутність конфлікту інтересів щодо цього дослідження, зокрема фінансового, особистого, авторського чи іншого характеру, який міг би вплинути на його результати.

Фінансування. Дослідження проведено без фінансової підтримки.

Доступність даних. Рукопис не має пов'язаного набору дослідницьких даних.

Використання засобів штучного інтелекту. Під час підготовки робочої редакції використано засоби штучного інтелекту для структурування матеріалу та мовного редагування. Усі висновки, нормативні посилання й бібліографічні відомості мають бути остаточно перевірені та схвалені авторами перед поданням до редакції.

Внесок авторів. Полотнянко Оксана Іванівна: концептуалізація дослідження, аналіз виборчого та інформаційного законодавства, європейські стандарти, підготовка основного тексту. Сандига Максим Вікторович: аналіз адміністративно-правових засад цифровізації судового захисту, електронних доказів і корупційних ризиків, розроблення моделі подвійного контуру доказової довіри. Обидва автори: методологія, редагування, формулювання висновків і відповідальність за остаточний зміст.

REFERENCES

1. Verkhovna Rada of Ukraine. (1996). Konstytutsiia Ukrainy vid 28.06.1996 No. 254k/96-VR [Constitution of Ukraine]. <https://zakon.rada.gov.ua/go/254%D0%BA/96-%D0%B2%D1%80>
2. Verkhovna Rada of Ukraine. (2019). Vyborchyi kodeks Ukrainy vid 19.12.2019 No. 396-IX [Electoral Code of Ukraine]. <https://zakon.rada.gov.ua/go/396-20>
3. Verkhovna Rada of Ukraine. (2004). Pro Tsentralnu vyborchu komisiiu: Zakon Ukrainy vid 30.06.2004 No. 1932-IV [On the Central Election Commission]. <https://zakon.rada.gov.ua/go/1932-15>
4. Verkhovna Rada of Ukraine. (2007). Pro Derzhavnyi reiestr vybortsiv: Zakon Ukrainy vid 22.02.2007 No. 698-V [On the State Voter Register]. <https://zakon.rada.gov.ua/go/698-16>
5. Verkhovna Rada of Ukraine. (2010). Pro zakhyst personalnykh danykh: Zakon Ukrainy vid 01.06.2010 No. 2297-VI [On Personal Data Protection]. <https://zakon.rada.gov.ua/go/2297-17>
6. Verkhovna Rada of Ukraine. (2005). Kodeks administratyvnoho sudochynstva Ukrainy vid 06.07.2005 No. 2747-IV [Code of Administrative Proceedings of Ukraine]. <https://zakon.rada.gov.ua/laws/show/2747-15>
7. Verkhovna Rada of Ukraine. (2001). Kryminalnyi kodeks Ukrainy vid 05.04.2001 No. 2341-III [Criminal Code of Ukraine]. <https://zakon.rada.gov.ua/go/2341-14>
8. Verkhovna Rada of Ukraine. (2014). Pro zapobihannia koruptsii: Zakon Ukrainy vid 14.10.2014 No. 1700-VII [On Prevention of Corruption]. <https://zakon.rada.gov.ua/laws/show/1700-18>
9. Central Election Commission of Ukraine. (2026). Komisiia napratsiuvala propozyzii shchodo zakonodavchoho vrehuliuvannia vyboriv pislia prypynennia chy skasuvannia voiennoho stanu [CEC proposals on regulating post-war elections]. <https://www.cvk.gov.ua/novini/komisiya-napratsyuvala-propozitsii-shchodo-zakonodavchogo-vregulyuvannya-vyboriv-v-ukraini-pislya-pripinennya-chi-skasuvannya-voiennoho-stanu.html>
10. European Parliament and Council. (2024). Regulation (EU) 2024/900 on the transparency and targeting of political advertising. <https://eur-lex.europa.eu/eli/reg/2024/900/oj/eng>
11. European Parliament and Council. (2022). Regulation (EU) 2022/2065 on a Single Market for Digital Services (Digital Services Act). <https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng>
12. Venice Commission. (2024). Interpretative Declaration of the Code of Good Practice in Electoral Matters as concerns digital technologies and artificial intelligence (CDL-AD(2024)044). <https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD%282024%29044-e>
13. Council of Europe. (2019). Guidelines of the Committee of Ministers of the Council of Europe on electronic evidence in civil and administrative proceedings. <https://search.coe.int/cm?i=0900001680902e0c>
14. Riznyk, V. A. (2023). Prottydiia dezinformatsii v politychnii reklamii: pravovyi aspekt [Countering disinformation in political advertising: a legal aspect]. *Visnyk Lvivskoho torhovelno-ekonomichnoho universytetu. Yurydychni nauky*, (13). <https://doi.org/10.32782/2616-7611-2023-13-07>
15. Skorokhod, O. P. (2024). Svitovyi dosvid vprovadzhennia ta vykorystannia tsyfrovyykh tekhnolohii u vyborchomu protsesi [Global experience in implementing and using digital technologies in the electoral process]. *Politychne zhyttia*, (2), 124–130 <https://doi.org/10.31558/2519-2949.2024.2.16> [in Ukrainian].
16. Zharovska, I. M. (2025). Vykylyky shchnohoho intelektu dlia pravovykh standartiv chesnykh vyboriv: problemy hlobalistyky [Challenges of artificial intelligence for legal standards of fair elections: problems of global studies]. *Analitychno-porivnialne pravoznnavstvo*, (6, part 1), 65–69. <https://doi.org/10.24144/2788-6018.2025.06.1.9>

17. Afanasieva, M. V. (2026). Heneratyvnyi shtuchnyi intelekt ta peredvyborna ahitatsiia: vyklyky ta perspektyvy rehuliuвання [Generative AI and election campaigning: challenges and regulatory prospects]. *Suchasna doktryna prava*, (4/98), 145–153. <https://doi.org/10.25313/3083-7774-2026-4-16>
18. Yosyfovych, N.-L. D. (2024). Kryterii otsinky elektronnykh dokaziv v administratyvnomu sudochynstvi [Criteria for evaluating electronic evidence in administrative proceedings]. *Naukovyi visnyk Uzhhorodskoho Natsionalnoho Universytetu*. Serii: Pravo, 85(2), 341–346. <https://doi.org/10.24144/2307-3322.2024.85.2.51>
19. Turov, V. D. (2024). Vykorystannia informatsiinykh tekhnolohii na etapi dokazuvannia v administratyvnomu sudochynstvi Ukrainy [Use of information technologies at the evidence stage in administrative proceedings of Ukraine]. *Naukovyi visnyk Uzhhorodskoho Natsionalnoho Universytetu*. Serii: Pravo, 82(2), 278–283. <https://doi.org/10.24144/2307-3322.2024.82.2.44>
20. Akhtyrskaya, N. M. (2023). Pravova rehlementatsiia elektronnykh dokaziv ta praktyka yikh vykorystannia v sudochynstvi Ukrainy [Legal regulation of electronic evidence and its use in Ukrainian judicial proceedings]. *Naukovyi visnyk Uzhhorodskoho Natsionalnoho Universytetu*. Serii: Pravo, 75(2), 141–150. <https://doi.org/10.24144/2307-3322.2022.75.2.23>
21. Podoliaka, A. M., Kurbatova, I. S., Simonovych, D. V., & Zarosylo, V. O. (2025). Okremi zminy v kryminalno-protsesualnykh normatyvnykh aktakh, yaki stosuutsia rozsliduvannia kryminalnykh pravoporushen u sferi vyborchykh prav hromadian [Selected changes in criminal procedural acts concerning investigation of criminal offences against citizens' electoral rights]. *Pravo i suspilstvo*, (2), 692–702. <https://doi.org/10.32842/2078-3736/2025.2.94>
22. Kuznietsov, M. H. (2024). Pravove zabezpechennia vyborchykh prav: problemy kryminalnoi vidpovidalnosti ta koruptsiinykh pravoporushen [Legal protection of electoral rights: issues of criminal liability and corruption offences]. *Prykarpatskyi yurydychnyi visnyk*, 6(59), 96–100. <https://doi.org/10.32782/pyuv.v6.2024.18>
23. Sachko, O. V., & Kuznietsov, M. H. (2024). Kryminalistychnyi analiz zlochyniv proty vyborchykh prav hromadian iz vykorystanniam informatsiinykh tekhnolohii [Forensic analysis of crimes against citizens' electoral rights involving information technologies]. *Kyivskyi chasopys prava*, (4), 144–150. <https://doi.org/10.32782/klj/2024.4.20>

ВІДОМОСТІ ПРО АВТОРІВ

Oksana Polotnyanko

Candidate of Economic Sciences, Associate Professor in the Department of Administrative, Financial, and Banking Law, Prince Volodymyr the Great Educational and Research Institute of Law, doctoral candidate at PJSC “Higher Educational Institution “Interregional Academy of Personnel Management”
e-mail: ksenijapolo21@gmail.com
ORCID: <https://orcid.org/0009-0008-7319-421X>

Maksym Sandyha

Postgraduate Student,
Interregional Academy of Personnel Management
ORCID: <https://orcid.org/0009-0008-5370-0293>

Полотнянко Оксана Іванівна

кандидат економічних наук, доцент кафедри адміністративного, фінансового та банківського права, Навчально-науковий інститут права імені князя Володимира Великого, докторант ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом»
e-mail: ksenijapolo21@gmail.com
ORCID: <https://orcid.org/0009-0008-7319-421X>

Сандига Максим Вікторович

аспірант,
ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом»
ORCID: <https://orcid.org/0009-0008-5370-0293>

Дата надходження статті: 19.05.2026

Дата надходження виправленої версії статті: 05.06.2026

Дата прийняття статті: 15.06.2026

Дата публікації статті: 05.10.2026