

А. О. Романюк

здобувачка, асистентка кафедри онлайн-медіа  
e-mail: aliona.romaniuk@knu.ua, ORCID: 0009-0008-8127-8675  
Київський національний університет імені Тараса Шевченка  
вул. Володимирська, 64/13, м. Київ, Україна, 01601

## ФЕЙКОВІ «ОФІЦІЙНІ» ДОКУМЕНТИ ЯК ІНСТРУМЕНТ ДЕЗІНФОРМАЦІЇ: МАРКЕРИ ПІДРОБКИ ТА ВЕРИФІКАЦІЯ

**Мета дослідження** – виявлення та систематизація маркерів підробки фейкових «офіційних» документів як специфічного формату дезінформаційного контенту, а також розробка алгоритму їх верифікації на основі емпіричного аналізу кейсів російських інформаційно-психологічних операцій у російсько-українській війні.

**Методологія дослідження** базується на комплексі якісних і порівняльних методів: контент-аналізі, кейс-аналізі, порівняльному аналізі підроблених документів з автентичними зразками офіційного діловодства та операціоналізації виявлених характеристик. Емпіричну базу становить авторський корпус із десяти верифікованих псевдоофіційних документів, поширених в інформаційному просторі України у 2022–2025 рр.

**Результати.** Виокремлено вісім типів маркерів підробки: формулярно-структурні, реквізитно-реєстраційні, інституційно-компетентнісні, мовно-стилістичні, логіко-юридичні та процедурні, візуально-технічні, реквізитно-часові, а також маркери циркуляції в межах наративу та «легенди». Встановлено, що у 100% досліджених кейсів зафіксовано маркери щонайменше трьох різних типів; найнадійнішими індикаторами є реквізитно-реєстраційні та інституційно-компетентнісні. Запропоновано функціональну типологію фейкових документів (документи деморалізації, паніки, делегітимації партнерства, шахрайські документи) та восьмикроковий алгоритм верифікації.

**Новизна** полягає у введенні концепції документної мімікрії – стратегії запозичення інституційної легітимності через відтворення формальних атрибутів офіційного документа – та у створенні першої систематизованої матриці маркерів підробки для псевдоофіційних документів в українському контексті.

**Практичне значення.** Матриця маркерів і верифікаційний алгоритм є придатними для використання в редакційній практиці медіа, освітніх програмах із журналістики, медіаграмотності та інформаційної гігієни, а також у підготовці державних службовців до розпізнавання цілеспрямованих дезінформаційних атак.

**Ключові слова:** дезінформація, фейкові документи, документна мімікрія, верифікація, інформаційно-психологічні операції, російсько-українська війна, соціальні мережі, фактчекінг.

### I. Вступ

У 2022 р. основним джерелом новин для українців став Telegram [9], який почали активно використовувати як канал комунікації державні органи, медіа, публічні особи. Передувало цьому явищу стрімке поширення анонімних телеграм-каналів, які позиціонують себе як новинні, мімікуючи під українські медіа та інституційні джерела, а також надаючи нібито інсайдерську інформацію. Через такі телеграм-канали, а також закриті спільноти й чати в різних месенджерах упродовж усього періоду російсько-української війни регулярно поширюються псевдоофіційні документи (листи, накази, довідки, скріншоти указів), які стилістично та візуально імітують офіційне листування державних інституцій та діячів. Такі матеріали є інструментом стратегічних дезінформаційних операцій у межах гібридної агресії РФ, спрямованих на розхитування ситуації всередині країни, дискредитацію органів влади, підірив довіри до армії та інституцій, деморалізацію населення, провокування панічних настроїв і конспірологічних переконань.

На проблему системного поширення фейкових документів регулярно звертають увагу аналітики Центру протидії дезінформації, Центру стратегічних комунікацій та інформаційної безпеки, фактчекери таких проєктів, як НотаСнота, Детектор медіа, StopFake, Gwara media, VoxCheck, Центру демократії і верховенства права та інших, які фіксують їх як окремий тип дезінформаційних повідомлень. На відміну від чуток, постів або скріншотів повідомлень, навіть підроблений документ має підвищену переконливість, оскільки відтворює атрибути формальної легітимності: бланк установи, реквізити, підпис, печатку, гриф обмеження доступу [1]. Унаслідок цього фейк у вигляді документа перетворюється на «матеріальний доказ», який підтверджує емоційні та політичні інтерпретації кризових подій.

Ефективність вірусного поширення фейкових документів у месенджерах і соціальних мережах посилюється специфікою функціонування сучасних медіаплатформ (Telegram, TikTok), де

висока швидкість споживання контенту в поєднанні з емоційною напруженістю воєнного часу нівелиює механізми раціональної перевірки процедурної та візуальної відповідності документа.

Відтак, систематизація маркерів підробки та розробка алгоритмів верифікації є науково й практично значущими для розвитку теорії соціальних комунікацій, удосконалення журналістських стандартів та зміцнення когнітивної стійкості суспільства.

Теоретичним підґрунтям дослідження слугує концепція інформаційного безладу, яку запропонували К. Уордл та Г. Дерахшан у доповіді для Ради Європи [20]. Автори розмежовують три типи інформації залежно від мети її поширення: місінформація (помилкова інформація без наміру нашкодити), дезінформація (свідомо сфабриковані повідомлення, неповна або спотворена інформація, яка створюється і поширюється з метою завдати шкоди) та малінформація (достовірна інформація, яку використовують з метою нашкодити). Фейкові «офіційні» документи належать до категорії дезінформації, оскільки їх створюють цілеспрямовано для маніпуляції, дискредитації інституцій та просування ворожих наративів.

Так, Г. Пеннікук та Д. Ренд вивчили когнітивні механізми, які пояснюють, чому аудиторія некритично сприймає фейки, включно з фейковими документами [15]. Автори доводять, що вразливість до фейків пояснюється передусім браком аналітичного мислення, а не партійною упередженістю. У контексті цього дослідження можна констатувати, що формальні атрибути офіційності, такі як бланк, реквізити, підпис, печатка, виступають для аудиторії «когнітивним ярликом», що активує периферійне опрацювання інформації та знижує рівень критичної перевірки. Показово, що навіть просте привернення уваги до точності інформації (наприклад, через запит «чи є це достовірним?») знижує поширення фейків на 51% [15]. Спираючись на це, можна стверджувати, що алгоритми верифікації мають практичну цінність як у режимі реального часу, так і у вибудовуванні довгострокової стратегії протидії дезінформації.

Огляд сучасних досліджень дезінформації та фейкових новин у соціальних мережах у своїй статті описують Е. Аймер, С. Амрі та Ж. Брассар [13]. Проаналізувавши понад 500 досліджень, автори наголошують, що жодна автоматизована система виявлення фейків досі не демонструє достатньої надійності. Цей висновок фактично підтверджує актуальність розробки людиноорієнтованих верифікаційних алгоритмів, у тому числі для формату фейкових документів.

Безпосереднім контекстом цього дослідження є російська дезінформаційна кампанія проти України під час повномасштабного вторгнення з 2022 р. Звіт Організації економічного співробітництва та розвитку (ОЕСР) [18] детально аналізує дезінформацію, яку використовує російська федерація як зброю проти України: від наративної підготовки до вторгнення до спроб дискредитувати Україну на міжнародній арені. Серед ключових інструментів автори виокремлюють і підробку «офіційних» або «секретних» документів, що мають на меті створення ілюзії достовірності та інституційної легітимності маніпулятивних повідомлень.

Порівняльний аналіз дезінформації під час пандемії COVID-19 та російсько-української війни, який зробили Р. Санчес дель Вас і Дж. Туньон Наварро [16], виявив ключову відмінність: у воєнному контексті домінує комбінований формат дезінформації (зображення + текст), тоді як під час пандемії переважала дезінформація у форматі тексту. Це підтверджує особливу роль візуально оформлених фейкових документів як напряму воєнної дезінформації.

В українському науковому дискурсі дослідження, безпосередньо присвячені фейковим документам як окремому феномену, є нечисленними. Зокрема, В. Козак [1] у статті «Фейкові документи як інструмент психологічного впливу в інформаційній війні Росії проти України» здійснює одну з перших спроб систематизувати характеристики документних підробок у контексті гібридної війни. Авторка аналізує методи легітимації фейкових документів, описує алгоритм їх ідентифікації, а також наголошує на центральній ролі анонімних телеграм-каналів як середовища розповсюдження маніпулятивних матеріалів. Попри концептуальний внесок, робота базується переважно на окремих прикладах і не пропонує систематизованої матриці маркерів підробки. Це визначає наукову лаку, яку заповнює пропонована стаття. Окремо про фейкові документи як складову загального «фейкоінструментарію» інформаційної війни згадували також Н. Шульська, Р. Зінчук, В. Башманівський [12].

Проведений аналіз досліджень і публікацій надає змогу виокремити ключову наукову лаку: попри значну кількість праць із дезінформації, когнітивної вразливості аудиторії та верифікаційних практик, фейкові документи як специфічний формат із власною «механікою переконання», процедурними маркерами та функціями в межах ширших інформаційно-психологічних операцій досі не отримали системного операціоналізованого опису. Наявні дослідження або оперують документом як ілюстрацією ширшого феномену дезінформації, або зосереджуються на технічних аспектах виявлення маніпуляцій із зображеннями, не розглядаючи специфіки псевдоофіційних документів та їхньої мімікрії під офіційні з метою забезпечити довіру до меседжу, який поширюють за допомогою такого формату. Першою спробою заповнити цю лаку в українському контексті є стаття В. Козак, однак вона не пропонує систематизованої порівняльної матриці маркерів і верифікаційного алгоритму, придатного для редакційного та університетського форматів. Саме на усунення цієї прогалини спрямована пропонована стаття.

## II. Постановка завдання та методи дослідження

Метою статті є виявлення та систематизація маркерів підробки фейкових «офіційних» документів як специфічного формату дезінформаційного контенту, а також розробка алгоритму їх верифікації на основі емпіричного аналізу кейсів російських інформаційно-психологічних операцій в російсько-українській війні. На відміну від попередніх досліджень, які розглядають фейкові документи як ілюстративний приклад ширшого феномену дезінформації або зосереджуються на технічних аспектах маніпуляції зображеннями, пропонується стаття спрямована на операціоналізацію цього явища як окремого типу мультимодального контенту.

Методологічну основу дослідження становить комплекс якісних і порівняльних методів соціально-комунікаційного аналізу. Емпіричною базою є десять кейсів фейкових офіційних документів, поширених в інформаційному просторі України у 2022–2025 рр. та верифікованих у межах фактчекінгової діяльності. Контент-аналіз застосовано для виявлення повторюваних структурних, лінгвістичних та візуальних характеристик документних підробок і формування типології маркерів фальсифікації. Метод кейс-аналізу забезпечив детальне вивчення конкретних прикладів дезінформаційних операцій та встановлення їхніх цілей у межах інформаційно-психологічного впливу. Порівняльний аналіз уможливив зіставлення підроблених документів з автентичними зразками офіційного діловодства, що надало змогу визначити процедурні невідповідності як ключовий індикатор фальсифікації. Метод операціоналізації використано для трансформації виявлених характеристик у практичний алгоритм верифікації фейкових документів. Зазначений комплекс методів надав змогу виокремити системні маркери підробки, встановити закономірності використання підроблених документів у дезінформаційних кампаніях і сформував верифікаційний протокол, придатний для редакційної та освітньої практики.

## III. Результати

### 3.1. Корпус дослідження та теоретична рамка

Емпіричну базу становить авторський корпус із 10 псевдоофіційних документів, зафіксованих у соціальних мережах (TikTok, Telegram, Facebook) упродовж 2022–2025 рр. Відбір здійснювався за критеріями: 1) документ поширювався як «доказ» суспільно чутливого меседжу; 2) документ оформлено у стилі офіційно-ділової комунікації державної/урядової інституції з наявністю візуальних атрибутів офіційного документа (бланк, реквізити, підпис, печатка); 3) верифікований статус фейку (підтверджений ЦПД, SPRAVDI, НотаЄнота або іншими фактчекінговими ініціативами чи офіційними структурами [2–8; 10; 11; 17]); 4) тематична різноманітність: охоплення різних типів установ і наративів. Таблиця 1 містить зведений опис корпусу.

Таблиця 1

**Опис корпусу псевдоофіційних документів (10 кейсів, 2022–2025 рр.)**

№	Тип документа	Основна тема	Домінантний наратив	Особливості поширення
1	2	3	4	5
Рис. 1	Указ Президента України [6]	Мобілізація та сексуальні обов'язки жінок під час воєнного стану	Президент нібито зобов'язав жінок задовольняти потреби військових; зрада у шлюбі не є зрадою під час війни	Telegram-канали, закриті групи у Facebook; орієнтований на деморалізацію та підірив довіри до держави
Рис. 2	Лист керівника Офісу Президента Начальнику Генштабу ЗСУ [3]	Заборона використання Ваукактар ТВ2 на певних напрямках	Влада приховує провали дронавої програми; обмежує ЗСУ у використанні ефективної зброї	Проросійські Telegram-канали; спрямований на дискредитацію оборонного потенціалу та міжнародної співпраці
Рис. 3	Лист Міністра охорони здоров'я Прем'єр-міністру України [4]	Заражена кров від країн НАТО; прихована загроза для ЗСУ	НАТО постачає Україні кров, заражену ВІЛ, гепатитом та іншими вірусами	Tik-Tok, Telegram і Facebook як «витік секретного документа»
Рис. 4	Епікриз «Лікарні Св. Луки» [7]	Поранений боець нібито перебуває на лікуванні; збір коштів	Шахрайство: підроблена медична довідка для збору коштів під виглядом допомоги пораненому	Viber-чати, Facebook-сторінки; схема регулярно перезапускається зі зміною імен та дат
Рис. 5	Наказ Міністерства оборони України [5]	Блокпости, затримання чоловіків, застосування зброї до тих, хто чинить опір	ЗСУ проводять масові насильницькі затримання призовників; військові отримали наказ стріляти на блокпостах	Tik-Tok, Telegram-канали; орієнтований на провокування паніки та недовіри до армії
Рис. 6	Лист від ДП НАЕК «ЕНЕРГОАТОМ» Міністру клімату та навколишнього середовища Польщі [8]	Хмельницька АЕС переорієнтовується на експорт електроенергії до Польщі	Україна в умовах блекаутів налагоджує постачання електроенергії до ЄС на шкodu власним громадянам	Tik-Tok, Telegram-канали; спрямований на підірив довіри між Україною та партнерами





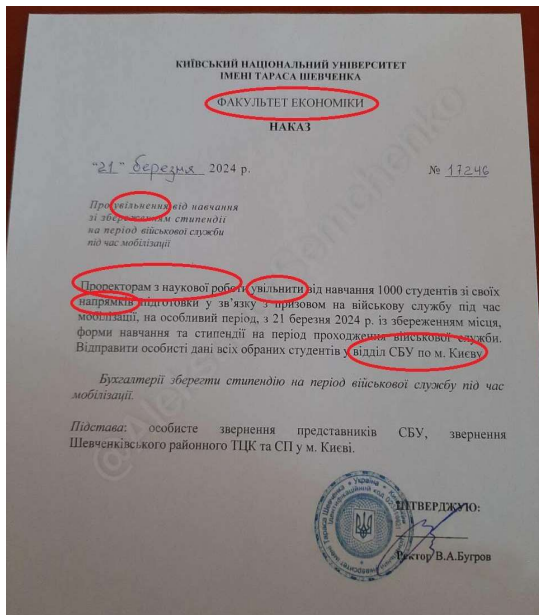


Рис. 7. Наказ ректора Київського національного університету імені Тараса Шевченка

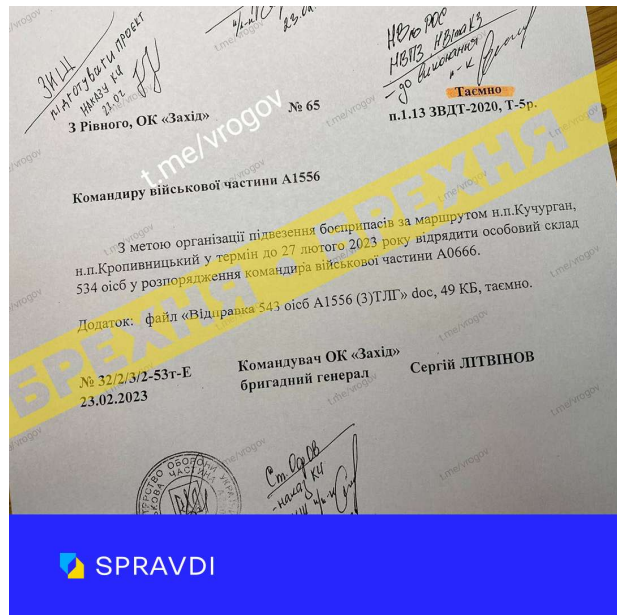


Рис. 8. Лист командувача ОК «Захід» з грифом «Таємно»

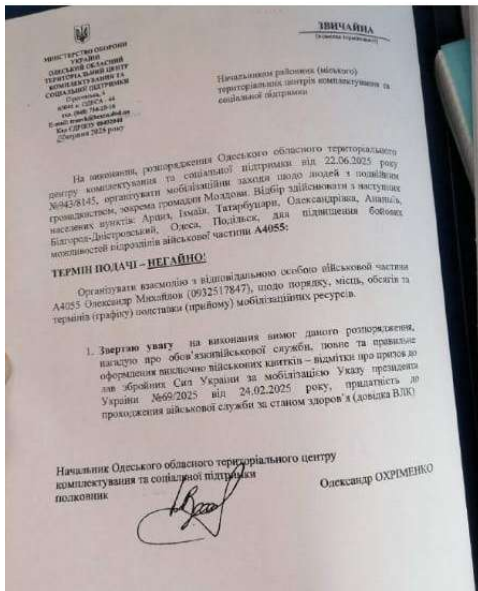


Рис. 9. Розпорядження Одеського обласного ТЦК та СП

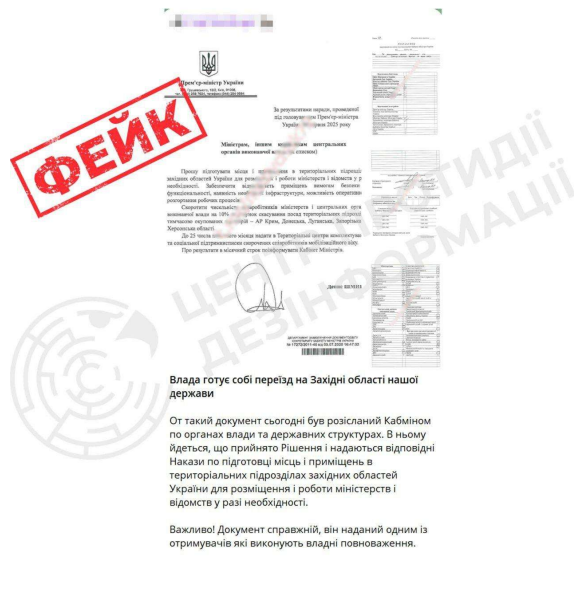


Рис. 10. Лист Прем'єр-міністра України керівникам центральних органів виконавчої влади

Для аналізу виявлених закономірностей у роботі застосовано концепцію документної мімікрії – відтворення зовнішніх ознак офіційного документа (формуляр, бланк, реквізити, підпис, печатка, гриф) з метою запозичення інституційної довіри. Ця стратегія спирається на ефект легітимності: наявність формальних атрибутів офіційності слугує для аудиторії когнітивним заміном змістової перевірки, вмикаючи периферійне опрацювання інформації [15].

Таким чином, псевдодokument перетворюється на так званий матеріальний доказ, що активує механізм підтвердження попередніх переконань і підвищує вірогідність вірусного поширення.

### 3.2. Типологія маркерів підробки

Контент-аналіз і порівняльний аналіз корпусу із залученням верифікаційних матеріалів НотаЄнота, SPRAVDI та Центру протидії дезінформації [2–8; 10; 11; 17] надали змогу виокремити вісім типів маркерів підробки, що системно повторюються в досліджених кейсах. Таблиця 2 містить матрицю маркерів: для кожного типу вказано конкретні індикатори, приклади з корпусу та діагностичну цінність – від абсолютних ознак підробки до маркерів середнього рівня, що потребують додаткової перевірки.

Важливо, що виявлені індикатори охоплюють не лише мовні чи візуальні аспекти, а й процедурну логіку функціонування офіційного документообігу, що є ключовою відмінністю цього типу дезінформації від інших форматів фейкового контенту.

Матриця маркерів підробки фейкових офіційних документів

Тип маркера	Індикатори	Приклади з корпусу	Діагностична цінність
1	2	3	4
Формулярно-структурні (оформлення документа)	Відсутні обов'язкові елементи виду документа: констатувальна частина; ключова формула («НАКАЗУЮ» для наказів); відсутні відповідальні/терміни/контроль; некоректне оформлення підстави (без дати/номера); згадані додатки без вихідної інформації скільки додатків на скількох сторінках розміщено, нетипове розміщення підпису/«З повагою»	Рис. 3: є посилання на додатки у документі, але немає обов'язкового оформлення додатків («стілки то додатків на ... сторінках»). Рис. 5: відсутня обґрунтовувальна частина з посиланнями на норми права. Рис. 6: порушення розміщення блоку «З повагою», підписного блоку. Рис. 7: відсутня констатувальна частина, «НАКАЗУЮ», відповідальні, контроль виконання; підстава без дати і номера реєстрації, слово «ПІДТВЕРДЖУЮ» замість «ЗАТВЕРДЖУЮ»	Середня: вимагає знання ДСТУ 4163:2020, але порушення видно, якщо порівняти з оригінальними документами установи
Реквізитно-реєстраційні (ідентифікація через номери/реєстри)	Відсутній вихідний номер або підпис уповноваженої особи; документ не зареєстрований у відповідній канцелярії; посилання на неіснуючі або невідповідні укази/акти; вигадані службові електронні адреси	Рис. 1: посилання на закон, який прийняли в майбутньому. Рис. 3: відсутні обов'язкові вихідні і вхідні реквізити, вихідні дані листа, QR-код не відповідає реєстрації конкретного листа. Рис. 9: посилається на Указ № 69/2025 від 24.02.2025, тоді як реальний указ із цим номером датований 05.02.2025 і стосується інших питань; неіснуюча службова електронна адреса. Рис. 10: документ не зареєстрований у Департаменті документообігу КМУ	Абсолютна (реєстрація): відсутність у реєстрі – безумовна ознака підробки.  Висока (номер, підпис, електронна адреса): перевіряється за кілька хвилин
Інституційно-компетентнісні (хто може видати/підписати/кому адресувати)	Некоректна адресація (посада/орган/підрозділ не існує або названий неправильно); орган видає документ поза своєю компетенцією; «рівень» документа не відповідає повноваженням підписанта; неправильна відомча належність/підпорядкування	Рис. 2: лист адресується Начальнику Генштабу В. Залужному, проте що посаду у 2022 р. обіймав С. Шаптала в той час, як В. Залужний був Головнокомандувачем ЗСУ. Рис. 5: МОУ видає наказ частині А3056, що підпорядковується Нацгвардії (МВС). Рис. 7: немає факультету економіки, натомість є економічний факультет; наказ виданий від імені «Факультету економіки», завдання адресовані проректорам університету, хоча факультет не має таких повноважень	Висока: систематична плутанина у посадах і підпорядкуванні є ознакою незнання структури українських інституцій
Мовно-стилістичні (офіційно-діловий стандарт)	Росіянізми і кальки; порушення відмінювання у звертанні/адресації; граматичні та орфографічні помилки; нехарактерна для канцеляриту лексика; недоречна мова документа (напр., лист іноземному адресату не англійською)	Рис. 1: «інтереси держи» (замість «держави» у заголовку). Рис. 3: численні помилки («наплягаємо», «неприпустимим є закупівля...»), що нетипово для міжвідомчого листування. Рис. 4: неузгодженість (боєць «на стаціонарі», але поранення «несумісні з життям»). Рис. 6: «Цім» замість «цим», помилки у відмінюванні імені адресата («Пауліне» замість «Пауліні», «Хенніг-Клоске» замість «Генніг-Клосці»); лист написаний українською, хоча отримувач іноземний. Рис. 7: «увільнення» замість «звільнення»; «відділ СБУ по місту Києву» замість «Головне управління СБУ у місті Києві»	Середня; висока: орфографічні росіянізми очевидні без спеціальних знань; стилістичні порушення виявляються під час порівняння з оригінальними документами
Логіко-юридичні та процедурні (зміст, який неможливий у правовому полі)	Пункти суперечать законодавству/здоровому глузду; документ «створює право» не тим інструментом; внутрішні логічні суперечності; нереалістичність виконання приписів; відсутність правових підстав (закони/підзаконні акти) у наказах	Рис. 1 юридично й логічно неможливі приписи; невідповідність реальній війні (у ЗСУ служать і жінки). Рис. 4: боєць «перебуває на стаціонарному лікуванні» і водночас «п'ять кульових поранень, несумісних із життям». Рис. 5: пункти про затримання всіх чоловіків і застосування зброї до тих, хто чинить опір, суперечать законодавству України і є нереалістичними; відсутня обґрунтовувальна частина з посиланнями на норми	Абсолютна (внутрішні суперечності): логічна несумісність всередині документа є безумовною ознакою фальсифікації.  Висока (юридичний аналіз): вимагає знання законодавства

1	2	3	4
Візуально-технічні (монтаж, якість, цілісність зображення)	Різна роздільна здатність тексту і підписів; «відірвані» печатка або підпис; обрізаний документ (немає шапки/реквізитів); артефакти монтажу; фіктивні печатки з неіснуючими кодами	Рис. 4: текст і підписи мають різну роздільну здатність; шапка обрізана, реквізити відсутні. Виявляється при детальному візуальному огляді. Рис. 5: на печатці вказаний неіснуючий ідентифікаційний код 07049100	Середня: видно без спеціальних інструментів, але легко усювається при наступних версіях підробки
Реквізитно-часові (реквізити установи, актуальність даних, часові «сліди» шаблону)	Застарілі телефони, рахунки, коди; неправильна організаційно-правова форма; відсутність актуальних каналів (e-mail) там, де вони обов'язкові; використання старих шаблонів оформлення документів	Рис. 3: відсутня електронна адреса, що є обов'язковим реквізитом на офіційних бланках. Рис. 6: банківський рахунок, актуальний на 2019 р.; «ДП НАЕК «Енергоатом»» замість «АТ» (реорганізовано); П. Котін підписує як «Президент», а не в. о. голови правління; неактуальний номер телефона	Висока: застарілі реквізити перевіряються за відкритими реєстрами за кілька хвилин; є індикатором використання старого шаблону
Маркери циркуляції в межах нарративу та «легенди»	«Легенда» про витік/злам як випереджувальна легітимація; водяні знаки російських або анонімних телеграм-каналів на «таємних» документах; серійність шаблону з заміною імен, дат; поширення через локальні/шкільні чати	Рис. 3: поширювався із «легендою» про злам пошти Прем'єр-міністра Шмигала. Рис. 4: схема регулярно перезапускається зі зміною імені «пораненого» та дат при незмінних технічних маркерах. Рис. 8 і рис. 10: на документах накладено водяні знаки проросійських каналів, легенди про інсайдерську інформацію	Висока (легенда про витік): типова тактика легітимації фейку

Реквізитно-реєстраційні та інституційно-компетентнісні маркери виявлено в усіх десяти кейсах без винятку, що підтверджує їх статус найнадійніших індикаторів підробки. Принципово важливою є закономірність: виробники фейків систематично ігнорують або не розуміють реєстраційну логіку офіційного документообігу в Україні. Найвиразніший приклад – рис. 10 (лист Шмигала), де ЦПД встановив відсутність реєстрації в Департаменті документообігу КМУ. Жодний справжній документ Кабінету Міністрів не може існувати без реєстраційного запису.

Інституційно-компетентнісні маркери свідчать про системне незнання виробниками фейків структури українських державних і військових інституцій. До характерних помилок належать плутанина в посадах: «начальник Генштабу Залужний» (рис. 2), наказ МО до частини НГУ (рис. 5), наказ факультету проректорам університету (рис. 7). Ця помилка повторюється незалежно від установи-прикриття, що свідчить про спільну модель створення фальшивих документів.

Мовно-стилістичні маркери зафіксовані в дев'яти кейсах. Найстійкішою діагностичною ознакою є заміна «і» на «и» та кальки з російської: «Цім листом» (рис. 6), «держи» (рис. 1), «наплягаємо» (рис. 3). Особливу цінність як маркер має внутрішня суперечність у рис. 4: «перебуває на стаціонарному лікуванні» і «поранення, несумісні з життям» в одному документі є абсолютним маркером фальсифікації.

Маркери циркуляції та «легенди» є специфічним типом, який характеризує не сам документ, а контекст його поширення. Одним із характерних маркерів є водяні знаки російських пропагандистських або українських анонімних Telegram-каналів на «таємних» документах. Цей маркер одночасно ідентифікує підробку й вказує на джерело її вкиду. Кейс рис. 4 (шахрайський епікриз) демонструє промислову модель: схема регулярно перезапускається зі зміною імені та дат при незмінних технічних маркерах.

Кейс рис. 6 (лист Енергоатому) і рис. 1 є найбагатшими на маркери в корпусі: у них одночасно присутні ознаки шести з восьми типів. Це свідчить про те, що пріоритетом авторів підробки була нарративна правдоподібність, а не процедурна точність. Можна припустити розрахунок на периферійне сприйняття аудиторії, яка готова прийняти документ як «підтвердження» вже наявних переконань [15].

Таким чином, аналіз табл. 2 дає підстави констатувати, що документна підробка як мультимодальний формат дезінформації спирається на документну мімікрію – стратегію запозичення інституційного авторитету через зовнішні атрибути. Проте «технологічна досконалість» таких фейків залишається низькою: у 100% досліджених кейсів виявлено сукупність маркерів щонайменше трьох різних типів. Найбільш вразливою ланкою для фальсифікаторів є інституційна компетентність та процедурна логіка, що вказує на відірваність авторів ІПСО від реального правового та адміністративного поля України.

### 3.3. Функціональна типологія псевдоофіційних документів

На підставі аналізу корпусу виокремлюються чотири функціональні типи фейкових офіційних документів залежно від їхньої ролі.

Перший тип – документи деморалізації. Вони спрямовані на піддрив довіри до армії та держави. Такі документи імітують внутрішній документообіг закритих структур і містять меседжі про насильницькі дії або стратегічні поразки (рис. 1, 2, 5, 10).

Другий тип – документи паніки. Вони розраховані на провокування масового страху та панічних настроїв серед визначених соціальних груп: студентів, батьків (рис. 7), військовозобов'язаних, які не служать, громадян Молдови (рис. 9), широкої аудиторії через максимальний емоційний ефект (рис. 1).

Третій тип – документи делегітимації партнерства. Вони спрямовані на руйнування довіри між Україною та союзниками через нарративи про загрозу з боку НАТО або зраду партнерів (рис. 3, 6).

Четвертий тип – шахрайські документи. У них використовуються атрибути офіційності для збору коштів під виглядом допомоги військовим (рис. 4). На відміну від ІПСО-документів, вони мають комерційну мотивацію й тиражуються за схемою «швидкого перезапуску» зі зміною особистих даних і дат.

### 3.4. Алгоритм верифікації фейкових документів

На підставі систематизованої матриці маркерів розроблено восьмикроковий алгоритм верифікації псевдоофіційних документів (табл. 3). Алгоритм побудований за принципом економії верифікаційних ресурсів: перші чотири кроки виконуються за 3–5 хвилин без спеціальних інструментів і є достатніми для прийняття рішення у більшості кейсів; кроки 5–8 застосовуються у складних випадках або коли висновок матиме публічне значення.

Таблиця 3

Алгоритм верифікації фейкових офіційних документів

Крок	Дія	Перевірочне питання	Критерій рішення
1	Перевірка джерела поширення	Де вперше з'явився документ? Чи є перша публікація в офіційному акаунті установи? Чи є посилання на першоджерело?	Анонімний Telegram-канал або невідома сторінка має підвищений ризик підробки
2	Перевірка реквізитів	Перевірити актуальну назву установи, адресу, телефони, рахунки, коди ЄДРПОУ на актуальність (відкриті реєстри, офіційний сайт)	Застарілі або неіснуючі реквізити є чітким маркером підробки
3	Перевірка посади підписанта та адресата	Чи існує така посада? Чи відповідає підписант установі та займав він цю посаду на дату підписання?	Неіснуюча або неправильна посада, неактуальна посада на дату документа є чітким маркером підробки
4	Мовний аналіз	Чи характерна мова для офіційно-ділового стилю? Чи є російські, граматичні та орфографічні помилки?	Росіянізми, помилки, нехарактерна лексика є ознакою підробки
5	Аналіз змісту та внутрішньої логіки	Чи є зміст юридично можливим? Чи немає внутрішніх суперечностей? Чи відповідає документ компетенції органу?	Абсурдний зміст, логічні та юридичні суперечності є ознакою підробки
6	Візуальна перевірка	Чи однакова роздільна здатність елементів (підпис, печатка, текст, логотипи)? Чи немає водяних знаків сторонніх каналів? Чи не обрізана шапка?	Артефакти монтажу, розмиті печатки, чужі водяні знаки є ознакою підробки
7	Наративний аналіз	Чи збігається зміст із відомими нарративами, які поширює російська пропаганда? Чи провокує документ надмірну емоційну реакцію?	Збіг з нарративами російської пропаганди є додатковою ознакою підробки
8	OSINT-верифікація	Пошук документа в офіційних реєстрах і зворотний пошук зображення; перевірка наявності спростувань на офіційних сторінках установ, ЦПД / SPRAVDI / фактчекерів	Відсутність у реєстрах, а також наявне спростування є основною ознакою підтвердженого фейку

Перевірка алгоритму на корпусі показала, що перші чотири кроки є діагностичними для всіх десяти кейсів. Кейс рис. 10 (лист Шмигалья) є показовим з огляду на канал поширення: на відміну від решти документів корпусу, цей псевдодокумент цілеспрямовано розсилався безпосередньо до органів влади та державних структур, а не через масові Telegram-канали для широкої аудиторії. Це ілюструє, що фейкові документи можуть мати не лише масову, а й таргетовану інституційну аудиторію – і це підвищує вимоги до верифікаційних протоколів у самих органах влади.

### IV. Висновки

Проведене дослідження підтверджує, що фейкові «офіційні» документи є самостійним форматом дезінформаційного контенту з власною «механікою переконання», яка принципово відрізняє їх від інших типів фейків. Ключовою властивістю цього формату є документна мімікрія – стратегія запозичення інституційної легітимності через відтворення зовнішніх атрибутів

офіційного документа (бланк, реквізити, підпис, печатка, гриф). Саме ці атрибути сприяють перетворенню підробки на «матеріальний доказ» в очах аудиторії, підвищуючи вірогідність вірусного поширення.

Аналіз корпусу з десяти верифікованих кейсів (2022–2025 рр.) надав змогу виокремити вісім типів комплексних маркерів підробки: формулярно-структурні, реквізитно-реєстраційні, інституційно-компетентнісні, мовно-стилістичні, логіко-юридичні та процедурні, візуально-технічні, реквізитно-часові й маркери циркуляції в межах наративу та «легенди». Найнадійнішими індикаторами підробки є реквізитно-реєстраційні та інституційно-компетентнісні маркери: вони виявлені в усіх десяти кейсах без винятку. Показово, що «технологічна досконалість» досліджених підробок є низькою: у 100% кейсів зафіксовано сукупність маркерів щонайменше трьох різних типів. Найбільш вразливою ланкою для фальсифікаторів виявилася процедурна логіка офіційного документообігу та інституційна компетентність – систематичне незнання структури українських державних і військових органів. Це вказує на відірваність авторів фейкових документів від реального правового та адміністративного поля України і водночас визначає найефективнішу точку верифікації.

За функціональним призначенням псевдоофіційні документи розподіляються на чотири типи: документи деморалізації (підрив довіри до армії та держави), документи паніки (провокування страху серед визначених соціальних груп), документи делегітимації партнерства (руйнування довіри між Україною та союзниками) і шахрайські документи (комерційна мотивація під виглядом допомоги військовим).

На підставі систематизованої матриці маркерів розроблено восьмикроковий алгоритм верифікації, побудований за принципом економії верифікаційних ресурсів. Перші чотири кроки (перевірка джерела поширення, реквізитів, посади підписанта та мовний аналіз) виконуються за кілька хвилин без спеціальних інструментів і є достатніми для більшості кейсів. Перевірка алгоритму підтвердила його діагностичну ефективність: перші чотири кроки виявилися достатніми для ідентифікації підробки в усіх десяти досліджених кейсах.

Практична цінність запропонованих інструментів виходить за межі фактчекінгової діяльності. Матриця маркерів і верифікаційний алгоритм є придатними для використання в редакційній практиці медіа, освітніх програмах з медіаграмотності та інформаційної гігієни, а також у підготовці державних службовців до розпізнавання цілеспрямованих дезінформаційних атак на інституційному рівні.

Перспективи подальших досліджень пов'язані з розширенням корпусу та кількісним аналізом динаміки поширення фейкових документів у часі, дослідженням ефективності різних форматів верифікаційних алгоритмів для непрофесійної аудиторії, а також порівняльним аналізом документних підробок у контексті інших збройних конфліктів.

#### Список використаної літератури

1. Козак В. А. Фейкові документи як інструмент психологічного впливу в інформаційній війні Росії проти України. *Вчені записки ТНУ імені В. І. Вернадського. Серія: Філологія. Журналістика*. 2025. Т. 36 (75). № 1. Ч. 2. С. 242–247.
2. НотаЄнота. Фейк: лист керівника Офісу Президента начальнику Генштабу ЗСУ щодо Bayraktar TB2. *Facebook*. URL: <https://www.facebook.com/notaenota1/posts/pfbid02gPJXZRtTLtiNtuqW5Z4Kts3iU5sZy3acTpFAWEAefkawn7wrTTmeZryCB14aMtFbl> (дата звернення: 09.11.2025).
3. НотаЄнота. Фейк: лист Міністра охорони здоров'я Прем'єр-міністру України про заражену кров НАТО. *Facebook*. URL: <https://www.facebook.com/notaenota1/posts/pfbid02sYNZF1426MrZT5BbBywk5gLNspHubATz1Zeps3bjzbFvWZ5EPkaLtpuKoE1t7J8yl> (дата звернення: 09.11.2025).
4. НотаЄнота. Фейк: лист НАЕК «Енергоатом» міністру клімату Польщі. *Facebook*. URL: <https://www.facebook.com/photo/?fbid=498856482727853&set=a.164756532804518> (дата звернення: 09.11.2025).
5. НотаЄнота. Фейк: наказ командира військової частини А3056 про блокування та застосування зброї. *Facebook*. URL: <https://www.facebook.com/notaenota1/posts/pfbid02GVkgUwvfHAZsMvFM8sh2xL4DcSo9i1jnfWbU6XmjWZUgSwvR7NWgqR5WNZeTCSsl> (дата звернення: 09.11.2025).
6. НотаЄнота. Фейк: Указ Президента України про сексуальні обов'язки жінок під час воєнного стану. *Facebook*. URL: <https://www.facebook.com/notaenota1/posts/137219152222567> (дата звернення: 09.11.2025).
7. НотаЄнота. Шахрайство: підроблений епікриз лікарні «Св. Луки» для збору коштів. *Facebook*. URL: <https://www.facebook.com/notaenota1/posts/pfbid037XatiRDx2GDwdCYW9jUyPykYDy3kRGnnWByBKn2Rbme55gLCj58jFkkL3pQt685gl> (дата звернення: 09.11.2025).
8. Одеський обласний ТЦК та СП. Фейк: розпорядження про мобілізацію громадян Молдови. *Facebook*. URL:

- <https://www.facebook.com/photo/?fbid=795033779522912&set=a.217576063935356> (дата звернення: 09.11.2025).
9. «Труха», «Блискавка», УНІАН – найбільш популярні джерела новин для українців під час війни. *Detector Media*. 2022. URL: <https://detector.media/infospace/article/205497/2022-11-30-trukha-blyskavka-unian-naubylsh-populyarni-dzherela-novyn-dlya-ukraintsiv-pid-chas-viyny/> (дата звернення: 09.11.2025).
  10. Центр комунікацій КНУ імені Тараса Шевченка. Фейк: наказ ректора КНУ про відрахування студентів та передачу даних до СБУ. *Facebook*. URL: <https://www.facebook.com/stratcomknu/posts/pfbid0sUvfjsEHQnNlHVEc5iXTsPhxnFj5PVXVzd fRaAYj8oV3DJmiBCNixgL6S3Uz223zl> (дата звернення: 09.11.2025).
  11. Центр протидії дезінформації. Росіяни розсилають фейковий лист нібито за підписом Прем'єр-міністра Дениса Шмигала про евакуацію міністерств. *Telegram*. 2025. URL: <https://t.me/CenterCounteringDisinformation/14837> (дата звернення: 09.11.2025).
  12. Шульська Н. М., Зінчук Р. С., Башманівський В. І. Фейкоінструментарій ведення інформаційної війни в Україні: на матеріалі мови сучасних медіа. *Вчені записки ТНУ імені В. І. Вернадського. Серія: Філологія. Журналістика*. 2023. Т. 34 (73). № 1. Ч. 2. С. 274–279.
  13. Aïmeur E., Amri S., Brassard G. Fake news, disinformation and misinformation in social media: a review. *Social Network Analysis and Mining*. 2023. Vol. 13. № 1. Art. 30.
  14. Lazer D. et al. The science of fake news. *Science*. 2018. Vol. 359. № 6380. P. 1094–1096.
  15. Pennycook G., Rand D. G. The Psychology of Fake News. *Trends in Cognitive Sciences*. 2021. Vol. 25. № 5. P. 388–402.
  16. Sánchez del Vas R., Tuñón Navarro J. Disinformation on the COVID-19 pandemic and the Russia-Ukraine War: Two sides of the same coin? *Humanities and Social Sciences Communications*. 2024. Vol. 11. Art. 826.
  17. SPRAVDI. Фейк: лист командувача ОК «Захід» з грифом «Таємно» щодо переміщення боєприпасів. *Facebook*. URL: <https://www.facebook.com/photo/?fbid=528215419462444&set=a.293130419637613> (дата звернення: 09.11.2025).
  18. Terracino J. B., Matasick C. Disinformation and Russia's War of Aggression Against Ukraine: Threats and Governance Responses. Paris : OECD, 2022. 49 p. URL: [https://www.oecd.org/en/publications/disinformation-and-russia-s-war-of-aggression-against-ukraine\\_37186bde-en.html](https://www.oecd.org/en/publications/disinformation-and-russia-s-war-of-aggression-against-ukraine_37186bde-en.html) (date of request: 09.11.2025).
  19. Vosoughi S., Roy D., Aral S. The spread of true and false news online. *Science*. 2018. Vol. 359. № 6380. P. 1146–1151.
  20. Wardle C., Derakhshan H. Information Disorder: Toward an Interdisciplinary Framework for Research and Policymaking. Strasbourg : Council of Europe, 2017. 108 p. URL: <https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html> (date of request: 09.11.2025).

#### References

1. Kozak, V. A. (2025). Feikovi dokumenty yak instrument psykholohichnoho vplyvu v informatsiinii viini Rosii proty Ukrainy [Fake documents as a tool of psychological influence in Russia's information war against Ukraine]. *Vcheni zapysky TNU imeni V. I. Vernadskoho. Seriya: Filolohiia. Zhurnalistyka*, 36 (75)(1, part 2), 242–247. doi: 10.32782/2710-4656/2025.1.2/38 [in Ukrainian].
2. NotaYenota. (2022). Feik: lyst kerivnyka Ofisu Prezydenta nachalnyku Henshtabu ZSU shchodo Bayraktar TB2 [Fake: letter from the Head of the President's Office to the Chief of the General Staff of the Armed Forces of Ukraine regarding Bayraktar TB2]. *Facebook*. Retrieved from <https://www.facebook.com/notaenota1/posts/pfbid02gPJXZRt-TLtiNtuqW5Z4Kts3iU5sZy3acTpFAWEAefkawn7wrTTmeZryCB14aMtFbl> [in Ukrainian].
3. NotaYenota. (2022). Feik: lyst Ministra okhorony zdorovia Prem'ier-ministru Ukrainy pro zarazenu krov NATO [Fake: letter from the Minister of Health to the Prime Minister of Ukraine about NATO-contaminated blood]. *Facebook*. Retrieved from <https://www.facebook.com/notaenota1/posts/pfbid02sYNZF1426MrZT5BbBywk5gLNspxubATz1Zeps3bjzFvWZ5EPkaLtpu-KoE1tJ8yl> [in Ukrainian].
4. NotaYenota. (2024). Feik: lyst NAEK «Enerhoatom» ministru klimatu Polshchi [Fake: letter from NAEK «Energoatom» to the Minister of Climate of Poland]. *Facebook*. Retrieved from <https://www.facebook.com/photo/?fbid=498856482727853&set=a.164756532804518> [in Ukrainian].
5. NotaYenota. (2023). Feik: nakaz komandyra viiskovoi chastyny A3056 pro blokposty ta zastosuvannia zbroi [Fake: order of the commander of military unit A3056 on checkpoints and use of weapons]. *Facebook*. Retrieved from <https://www.facebook.com/notaenota1/posts/pfbid02GVkgUwvfHAZsMvFM8sh2xL4DcSo9i1jnfWbU6XmjWZUg-SwvR7NWgqR5WNZetTCSsl> [in Ukrainian].
6. NotaYenota. (2022). Feik: Ukaz Prezydenta Ukrainy pro seksualni obov'iazky zhinok pid chas voiennoho stanu [Fake: Decree of the President of Ukraine on sexual duties of women during

- martial law]. *Facebook*. Retrieved from <https://www.facebook.com/notae-nota1/posts/137219152222567> [in Ukrainian].
7. NotaYenota. (2023). Shakhraistvo: pidroblenyi epikryz likarni «Sv. Luky» dlia zboru koshtiv [Fraud: forged medical report from St. Luke's Hospital for fundraising]. *Facebook*. Retrieved from <https://www.facebook.com/notae-nota1/posts/pfbid037XatiRDx2GDwdCYW9jUyPykYDy3kRGnnWByBKn2Rbme55gLCj58jFkkL3pQt685gl> [in Ukrainian].
  8. Odeskyi oblasnyi TsTsK ta SP. (2025). Feik: rozporiadzhennia pro mobilizatsiiu hromadian Moldovy [Fake: order on mobilization of Moldovan citizens]. *Facebook*. Retrieved from <https://www.facebook.com/photo/?fbid=795033779522912&set=a.217576063935356> [in Ukrainian].
  9. «Trukha», «Blyskavka», UNIAN – naibilsh populiarne dzherelo novyn dlia ukraintsiv pid chas viiny [«Trukha», «Blyskavka», UNIAN – the most popular news sources for Ukrainians during the war]. (2022). *Detector Media*. Retrieved from <https://detector.media/infospace/article/205497/2022-11-30-trukha-blyskavka-unian-naybilsh-populyarni-dzherela-novyn-dlya-ukraintsiv-pid-chas-viiny/> [in Ukrainian].
  10. Tsentr komunikatsii KNU imeni Tarasa Shevchenka. (2024). Feik: nakaz rektora KNU pro vidrakhuvannia studentiv ta peredachu danykh do SBU [Fake: order of the KNU rector on expulsion of students and transfer of data to the SBU]. *Facebook*. Retrieved from <https://www.facebook.com/stratcomknu/posts/pfbid0sUvifsEHQnNlH-VEc5iXTsPhxnFj5PVXVzdfRaAYj8oV3DJmiBCHixgL6S3Uz223zl> [in Ukrainian].
  11. Tsentr protydii dezinformatsii. (2025). Rosiany rozsilaiut feikovy lyst nibito za pidpysom Prem'ier-ministra Denysa Shmyhalia pro evakuatsiiu ministerstv [Russians are sending a fake letter allegedly signed by Prime Minister Denys Shmyhal about the evacuation of ministries]. *Telegram*. Retrieved from <https://t.me/CenterCounteringDisinformation/14837> [in Ukrainian].
  12. Shulska, N. M., Zinchuk, R. S., & Bashmanivskyi, V. I. (2023). Feikoinstrumentarii vedennia informatsiinoi viiny v Ukraini: na materialii movy suchasnykh media [Fake tools of information warfare in Ukraine: based on the language of modern media]. *Vcheni zapysky TNU imeni V. I. Vernadskoho. Seriya: Filolohiia. Zhurnalistyka*, 34(73)(1, part 2), 274–279. doi: 10.32782/2710-4656/2023.1.2/43 [in Ukrainian].
  13. Aïmeur, E., Amri, S., & Brassard, G. (2023). Fake news, disinformation and misinformation in social media: A review. *Social Network Analysis and Mining*, 13 (1), 30. doi: 10.1007/s13278-023-01028-5 [in English].
  14. Lazer, D., Baum, M. A., Benkler, Y., Berinsky, A. J., Greenhill, K. M., Menczer, F., Metzger, M. J., ..., & Zittrain, J. L. (2018). The science of fake news. *Science*, 359 (6380), 1094–1096. doi: 10.1126/science.aao2998 [in English].
  15. Pennycook, G., & Rand, D. G. (2021). The psychology of fake news. *Trends in Cognitive Sciences*, 25 (5), 388–402. doi: 10.1016/j.tics.2021.02.007 [in English].
  16. Sánchez del Vas, R., & Tuñón Navarro, J. (2024). Disinformation on the COVID-19 pandemic and the Russia-Ukraine War: Two sides of the same coin? *Humanities and Social Sciences Communications*, 11, 826. doi: 10.1057/s41599-024-03355-0 [in English].
  17. SPRAVDI. (2026, February 19). Feik: lyst komanduvacha OK «Zakhid» z hryfom «Taiemno» shchodo peremishchennia boieprypasiv [Fake: letter from the commander of OC «West» classified «Secret» regarding the movement of ammunition]. *Facebook*. Retrieved from <https://www.facebook.com/photo/?fbid=528215419462444&set=a.293130419637613> [in Ukrainian].
  18. Terracino, J. B., & Matasick, C. (2022). Disinformation and Russia's war of aggression against Ukraine: Threats and governance responses. *OECD*. Retrieved from [https://www.oecd.org/en/publications/disinformation-and-russia-s-war-of-aggression-against-ukraine\\_37186bde-en.html](https://www.oecd.org/en/publications/disinformation-and-russia-s-war-of-aggression-against-ukraine_37186bde-en.html) [in English].
  19. Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *Science*, 359 (6380), 1146–1151. doi: 10.1126/science.aap9559 [in English].
  20. Wardle, C., & Derakhshan, H. (2017). Information disorder: Toward an interdisciplinary framework for research and policymaking. *Council of Europe*. Retrieved from <https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html> [in English].

Стаття надійшла до редакції 15.11.2025.  
Received 15.11.2025.

---

#### Romaniuk A. Fake «Official» Documents as a Disinformation Tool: Forgery Markers and Verification

**Research objective** is to identify and systematize the markers of forgery in pseudo-official documents as a specific format of disinformation content, and to develop a verification algorithm based on empirical analysis of Russian information and psychological operations in the Russian-Ukrainian war.

**Research methodology** is based on a combination of qualitative and comparative methods: content analysis, case analysis, comparative analysis of forged documents against authentic official

records, and operationalization of identified characteristics. The empirical base comprises a corpus of ten verified pseudo-official documents circulated in Ukraine's information space in 2022–2025.

**Results.** Eight types of forgery markers were identified: formulary-structural, requisite-registration, institutional-competence, linguistic-stylistic, logical-legal and procedural, visual-technical, requisite-temporal, and circulation-narrative markers. It was established that 100% of the examined cases contained markers from at least three different categories; the most reliable indicators proved to be requisite-registration and institutional-competence markers. A functional typology of fake documents was proposed (demoralization documents, panic-inducing documents, partnership-delegitimization documents, and fraudulent documents), alongside an eight-step verification algorithm.

**Novelty** consists in introducing the concept of documentary mimicry – a strategy of borrowing institutional legitimacy by replicating the formal attributes of official documents – and in creating the first systematized matrix of forgery markers for pseudo-official documents in the Ukrainian context.

**Practical significance.** The marker matrix and verification algorithm are applicable in media editorial practice, media literacy and information hygiene education programs, and in training civil servants to recognize targeted disinformation attacks.

**Key words:** disinformation, fake documents, documentary mimicry, verification, information and psychological operations, Russian-Ukrainian war, social media, fact-checking.