# *Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність*

**УДК 343.977**
**DOI 10.33244/2617-4154.1(18).2025.235-248**

**О. М. Дудник,**
*аспірант ННІ права,*
*Державний податковий університет*
*e-mail: o.dudnyk@outlook.com*
**ORCID ID 0009-0000-7163-3487**

# СПОСОБИ ПІДРОБКИ КРИМІНАЛІСТИЧНИХ ДОКУМЕНТІВ І ЯК ЇХ ВИЯВЛЯТИ

*Стаття розкриває значущість комплексного та системного вивчення способів фальсифікації документів у криміналістиці, враховуючи їхнє різноманіття й еволюцію, а також визначальну роль правопорушників, які постійно вдосконалюють свої навички підробки. Поєднання традиційних методів експертизи (зокрема, почеркознавчої, технічної, фізико-хімічної) із сучасними цифровими технологіями значно підвищує ефективність протидії використанню фіктивних документів у правовій практиці. У статті детально аналізується значення спеціалізованого обладнання, кваліфікованих фахівців-криміналістів та розвинених інформаційно-аналітичних систем, які є критично важливими для своєчасного виявлення та ідентифікації підроблених документів.*

*Особлива увага приділена необхідності врахування швидких трансформацій у сфері високих технологій і цифровізації, що відкривають для зловмисників нові інструменти підробки. Розглянуто питання внесення змін до електронних документів, включно з редагуванням PDF-файлів, підробкою електронного цифрового підпису, маніпуляціями з метаданими. Визначено, що для протидії подібним загрозам необхідно впроваджувати сучасне технічне забезпечення, проводити регулярне підвищення кваліфікації експертів, удосконалювати нормативно-правову базу, що регулює обіг і захист електронних документів.*

*Автори підкреслюють, що заходи з виявлення фальсифікацій документів мають бути комплексними. Вони повинні охоплювати посилення законодавчих гарантій, удосконалення організаційних механізмів у межах державних і приватних інституцій, активізацію міжнародної співпраці для обміну досвідом і найкращими практиками. Зроблено висновок, що прогрес у методичній базі експертизи, урахування сучасних викликів цифрової епохи та узгодження законодавчих підходів є ключем до формування дієвої системи захисту прав громадян і фінансових інтересів держави.*

***Ключові слова:*** *криміналістика; підробка документів; експертиза; фальсифікація; почеркознавство; цифровий аналіз; правове регулювання.*

**Методи дослідження.** Методологічну основу дослідження становить комплекс загальнонаукових і спеціальних методів, які забезпечують всебічне й глибоке вивчення способів фальсифікації документів та розробку ефективних способів їх виявлення. У процесі збору й аналізу інформації використовувалися методи аналізу та синтезу. Ці методи дали змогу ідентифікувати ключові тенденції, встановити спільні риси та відмінності між різними видами підробок, а також сформувати базу даних для подальших досліджень. Дослідження охоплювало аналіз літературних джерел, практичних кейсів та міжнародного досвіду у сфері виявлення фальсифікацій.

На етапі оцінки ефективності методів виявлення підробок використовувався метод порівняння. Це дало змогу не лише визначити переваги та недоліки кожного підходу, але й встановити оптимальні сфери застосування кожного з них. Метод порівняння також сприяв формуванню рекомендацій для практичного використання отриманих результатів. Завдяки цьому вдалося зіставити традиційні й сучасні підходи, а також оцінити їхню відповідність сучасним вимогам криміналістичної практики.

Системно-структурний метод, застосований у дослідженні, дав змогу всебічно описати комплекс взаємопов'язаних чинників, що впливають на ефективність боротьби з підробками. Це охоплює технологічну оснащеність, кваліфікацію фахівців, правові норми, а також особливості організації експертної діяльності. Цей метод дав змогу створити детальну модель взаємодії цих елементів, що є критично важливим для розуміння проблеми загалом.

Індукція й дедукція застосовувались у двох основних напрямах. По-перше, аналіз конкретних кримінальних кейсів дав змогу зробити загальні теоретичні висновки щодо типових ознак фальсифікацій та способів їх виявлення. По-друге, загальні закономірності криміналістики були застосовані для вивчення конкретних фактів використання підроблених документів у різних контекстах. Цей підхід дав змогу врахувати як теоретичні основи, так і практичні аспекти проблеми.

Емпіричні методи, зокрема інтерв'ю, спостереження та вивчення документів, були використані для збору даних із практичного досвіду криміналістів. Це забезпечило доступ до реальних прикладів фальсифікацій і дало змогу оцінити ефективність існуючих методів боротьби з ними. Завдяки такому підходу вдалося не лише розширити уявлення про проблему, але й сформувати базу для подальшого вдосконалення експертної діяльності.

Завдяки міждисциплінарному підходу, що поєднував теоретичний і практичний аналіз, вдалося сформувати уніфікований погляд на проблему фальсифікацій. Це створило підґрунтя для розробки практичних рекомендацій, спрямованих на вдосконалення методів виявлення підробок і підвищення ефективності криміналістичних досліджень.

**Виклад основного матеріалу.** Для криміналістики надзвичайно важливо системно підходити до поняття «підроблений документ». Під цим терміном зазвичай розуміють офіційний або неофіційний носій (паперовий або електронний), у якому фальсифіковано зміст, підпис, печатку або реквізити з метою введення в оману державних органів, юридичних чи фізичних осіб. Сучасна практика показує, що підробки охоплюють широкий спектр дій – від найпростішого підроблення печаток до складних цифрових

маніпуляцій із використанням спеціалізованого програмного забезпечення. Основними видами підробок є технічна, що містить внесення штучних змін у структуру документа, таких як механічне стирання, хімічне травлення чи використання цифрових інструментів для редагування файлів, і інтелектуальна, що полягає у створенні документів, які формально відповідають стандартам, але містять свідомо неправдиву інформацію.

Злочинці часто комбінують ці методи, що ускладнює ідентифікацію підробок. Наприклад, створення зовнішньо автентичного документа із внесенням фіктивної інформації вимагає від експертів не лише високої кваліфікації, а й глибокого знання правових норм, які регулюють зміст документів.

Проблема виявлення підробок стає ще гострішою в умовах війни, як це спостерігається в Україні. Війна призводить до хаотизації документообігу, зокрема через масове переміщення людей, втрату частини офіційних реєстрів та баз даних, а також зростання кількості підроблених документів у сферах, пов'язаних із гуманітарною допомогою, військовими потребами та відновленням інфраструктури. У таких умовах злочинці використовують нестабільність ситуації, щоб уникнути перевірок або скористатися прогалинами в роботі державних і правових інституцій. Крім того, значна частина експертного складу криміналістів задіяна в інших напрямах, що ускладнює проведення детальних досліджень і статистичного аналізу підробок.

Традиційні методи фальсифікації містять підробку підпису, зміну друкованого тексту та маніпуляції з фотокартками і печатками. Підробка підпису може виконуватися «на око», через копіювання або сканування і друк, причому експерти можуть ідентифікувати такі підробки завдяки аналізу форм овалів, натиску та інших дрібних деталей. Зміна друкованого тексту, наприклад, за допомогою механічного стирання чи хімічної обробки, залишає сліди, такі як розпушення паперу або нерівномірне забарвлення. Маніпуляції з фотокартками та печатками можуть містити вклеювання фотографій, вирізання частини аркуша чи використання фальшивих кліше, що виявляється через мікропошкодження паперу або нестиковку елементів.

Цифрові методи фальсифікації стали особливо актуальними з розвитком електронного документообігу. Використання програм для редагування PDF-файлів, зміна метаданих документа, підробка електронних підписів і маніпуляції з RFID-чипами та біометричними документами значно ускладнюють процес ідентифікації підробок. Зловмисники можуть не лише змінювати зміст електронного документа, але й редагувати інформацію про автора чи дату створення, що потребує спеціалізованих програм для аналізу метаданих, перевірки автентичності електронних підписів і оцінки відповідності сертифікатів. Підробки біометричних даних, хоча й є складнішими через використання чипів, стають можливими через вразливості програмного забезпечення, і для їх виявлення потрібні спеціальні інструменти для читання та аналізу чипів.

Військові дії в Україні створюють особливі умови для збільшення кількості цифрових фальсифікацій. Масова мобілізація, велика кількість гуманітарних вантажів і транскордонних перевезень створюють значний попит на підроблені документи, такі як довідки, дозволи чи сертифікати. У таких обставинах проведення статистичного аналізу ускладнюється

через фрагментарність даних, відсутність координації між органами та виснаженість експертного персоналу. Крім того, війна змінює пріоритети державних структур, спрямовуючи ресурси на вирішення оперативних питань безпеки.

Комплексний підхід до експертизи документів базується на інтеграції фізичних, хімічних і цифрових методів. Візуально-тактильний контроль допомагає виявити ознаки ламінування, домальовування чи розбіжностей у текстурах паперу. Використання технічних приладів, таких як УФ-лампи, мікроскопи та спектрометри, дає змогу розпізнати приховані зміни в структурі документа. Цифровий аналіз забезпечує перевірку метаданих, аналіз електронних підписів і контроль хеш-суми документа, що особливо важливо в умовах цифровізації. Взаємодія з офіційними реєстрами та базами даних дає змогу зіставляти інформацію, виявляти невідповідності та викривати нелегітимні документи. Така багаторівнева система експертизи є ефективною для виявлення як простих, так і складних форм підробок.

На міжнародному рівні та в межах регіональних об'єднань діють численні нормативні документи, спрямовані на боротьбу з фальсифікацією документів. Одним із найважливіших є Регламент ЄС № 2252/2004 [1], який визначає мінімальні вимоги до захисту паспортів і проїзних документів. Цей документ зобов'язує країни Європейського Союзу впроваджувати біометричні дані в паспорти (оцифроване зображення обличчя та відбитки пальців), а також розробляти специфічні заходи безпеки. У результаті значно покращено захист документів, завдяки чому зменшилася кількість підробок. Крім того, регламент передбачає впровадження водяних знаків, антисканерних сіток, високоякісного друку та RFID-чипів, що ускладнює підробку ідентифікаційних документів. Країни-члени отримали перехідний період для адаптації національних міграційних служб і друкарень до нових стандартів, що також сприяло уніфікації підходів до захисту документів.

Іншим ключовим документом є Doc 9303 Міжнародної організації цивільної авіації (ICAO) [2], який встановлює глобальні стандарти для машинозчитуваних проїзних документів. Цей документ охоплює технічні вимоги до паспортів, елементів біометрії, зон MRZ (Machine Readable Zone) і цифрових підписів. ICAO Doc 9303 забезпечує сумісність паспортів різних країн, що прискорює перевірку на кордонах та ускладнює підробки завдяки уніфікації форматів. У ньому також закріплені вимоги до використання голографічних стрічок, лазерної перфорації та оптично змінних фарб, що є важливими елементами захисту документів.

Серед інших нормативних документів, які мають значення для забезпечення безпеки документів, варто згадати стандарти ISO/IEC 7816 [10] та ISO/IEC 14443 [11]. Ці стандарти регулюють специфікації для смарт-карт і безконтактних чипів, які широко застосовуються в сучасних біометричних паспортах і посвідченнях особи. Вони охоплюють питання сумісності обладнання для зчитування даних, криптографічних протоколів і захисту інформації. Застосування цих стандартів дає змогу забезпечити інтегровану безпеку ідентифікаційних документів та мінімізувати ризики несанкціонованого доступу до інформації.

Важливим також є Кіотська конвенція про спрощення та гармонізацію митних процедур [8]. Її положення спрямовані на вдосконалення механізмів контролю за переміщенням товарів і осіб через кордон, зокрема завдяки стандартизації митних документів і використання електронних систем обробки даних. Це допомагає швидко ідентифікувати підроблені сертифікати, дозволи та інші документи, що супроводжують товари або особисті перевезення.

На національному рівні держави розробляють додаткові нормативні акти, які враховують їхні унікальні обставини та виклики. Наприклад, в Україні важливе місце займають нормативні документи, що регулюють захист електронних документів і електронних цифрових підписів, зокрема закони України «Про електронні документи та електронний документообіг» [10] і «Про електронні довірчі послуги» [6]. Вони забезпечують правове підґрунтя для перевірки справжності електронних документів і боротьби з їхньою підробкою.

Отже, впровадження та дотримання міжнародних і національних стандартів є критично важливими для ефективної боротьби з фальсифікацією документів. Нормативні акти не лише встановлюють вимоги до технічних засобів захисту, але й забезпечують єдині підходи до перевірки документів, що сприяє підвищенню безпеки як на національному, так і на міжнародному рівнях.

Ефективна боротьба з фальсифікацією документів неможлива без системного вдосконалення нормативно-правової бази, яка регулює обіг документів, як у паперовій, так і в електронній формі. Існуючі законодавчі акти потребують адаптації до сучасних викликів, а також ухвалення нових норм, які враховують тенденції цифровізації. Зокрема, необхідно визначити порядок функціонування реєстрів електронних підписів, розробити стандарти обміну ключами між суб'єктами електронного документообігу, а також запровадити вимоги до збереження та обробки метаданих. Це сприятиме більшій прозорості процесів та унеможливленню підробок, водночас забезпечуючи надійний правовий захист учасників.

Особливої уваги потребує оновлення процесуальних кодексів, таких як Кримінальний процесуальний кодекс [7] та Кодекс України про адміністративні правопорушення. Ці документи мають чітко визначати права та обов'язки правоохоронців, суддів і експертів у процесі перевірки автентичності документів. Важливо також запровадити нові процедури для роботи з електронними доказами, зокрема щодо їхнього збору, зберігання та аналізування.

Удосконалення технічного інструментарію є ще одним ключовим елементом ефективної протидії фальсифікаціям. У сучасних умовах правоохоронцям та судово-експертним установам необхідно використовувати найновіше обладнання, таке як ультрафіолетові та інфрачервоні аналізатори, спектрометри, мікроскопи високої точності, а також програмне забезпечення для криптографічного аналізу електронних підписів. Інтеграція штучного інтелекту в процеси експертизи стає дедалі актуальнішою. Завдяки алгоритмам машинного навчання можна виявляти аномалії у друкованих або цифрових зображеннях документів, що значно прискорює процес ідентифікації підробок.

Разом із технічним прогресом виникає необхідність у постійному підвищенні кваліфікації фахівців, які працюють у галузі криміналістики. Регулярні тренінги, участь у семінарах та конференціях, обмін досвідом між експертами з різних регіонів і країн дають змогу не лише вдосконалювати професійні навички, а й оперативно реагувати на нові шахрайські схеми. Особливо це важливо в умовах розвитку складних електронних та біометричних підробок, де від рівня підготовки експерта залежить результат розслідування.

Міжнародна співпраця є невід'ємною складовою боротьби з транскордонними фальсифікаціями документів. Включення у глобальні ініціативи обміну даними, такі як FADO (False and Authentic Documents Online) або PRADO (Public Register of Authentic Travel and Identity Documents Online), сприяє швидкому виявленню підробок, що використовувалися в інших країнах. Система FADO, створена Європейським Союзом, є закритим ресурсом, доступним для компетентних органів держав-членів ЄС. Вона забезпечує обмін інформацією про підроблені та автентичні документи, охоплюючи їхні зображення, технічні описи та методи ідентифікації. Цей ресурс значно підвищує ефективність правоохоронців у виявленні та попередженні шахрайства, пов'язаного з документами.

PRADO є публічним реєстром, доступним для всіх зацікавлених осіб, включно з державними установами, приватними компаніями та громадянами. Він містить інформацію про автентичні документи, що використовуються в державах ЄС, а також детальні описи захисних елементів, які ускладнюють підробку. PRADO сприяє поширенню знань про характеристики захищених документів серед ширшої аудиторії, що дає змогу краще розпізнавати потенційно фальшиві документи.

Завдяки використанню таких систем, як FADO та PRADO, країни отримують інструменти для швидкого та ефективного аналізу документів, що особливо важливо в умовах зростання кількості міжнародних перевезень і міграції. Крім того, ці ресурси сприяють гармонізації підходів до перевірки документів на міжнародному рівні, що є ключовим для забезпечення глобальної безпеки.

Важливим аспектом є розробка та впровадження стандартів, які гармонізують підходи до перевірки документів у міжнародному контексті. Це стосується як паперових, так і електронних документів, що дедалі частіше використовуються в транскордонному обігу. Єдині технічні та правові підходи до верифікації забезпечують не лише вищий рівень безпеки, але й спрощують процедури ідентифікації для громадян і бізнесу.

Так, поєднання вдосконаленого нормативно-правового поля, розширення технічного інструментарію, постійної підготовки кадрів та активної міжнародної співпраці є основними складовими ефективної боротьби з фальсифікацією документів. Ці заходи створюють надійне підґрунтя для забезпечення прозорості, захисту прав громадян та зміцнення національної і міжнародної безпеки.

Полегшення розслідувань підробки документів в Україні потребує впровадження комплексного підходу, що охоплює вдосконалення нормативно-правової бази, технічне переоснащення, підготовку фахівців та посилення міжнародної співпраці. Важливо

адаптувати законодавство до сучасних викликів цифровізації, особливо щодо функціонування реєстрів електронних підписів і стандартів обміну ключами. Регулювання збереження метаданих має забезпечити прозорість електронного документообігу, зменшити можливості для фальсифікацій та створити надійний захист для користувачів.

Необхідно впровадити сучасне обладнання для аналізу документів, охоплюючи ультрафіолетові аналізатори, спектрометри та інструменти для роботи з біометричними даними. Інтеграція штучного інтелекту здатна автоматизувати виявлення підробок, скорочуючи час і підвищуючи точність аналізу. Додатково важливо створити національну базу підроблених документів, яка б об'єднувала інформацію з різних регіонів та сприяла швидкому доступу до потрібних даних.

Професійна підготовка експертів має стати регулярною, з акцентом на новітні методи ідентифікації підробок. Це передбачає проведення тренінгів, участь у міжнародних конференціях та обмін досвідом з іноземними колегами. Зокрема, використання ресурсів, таких як FADO та PRADO, може значно підвищити рівень професійної обізнаності. FADO, будучи закритим ресурсом для правоохоронців, дає змогу отримувати доступ до описів автентичних і фальшивих документів, тоді як PRADO забезпечує відкриту базу для громадськості, підвищуючи загальну поінформованість про захисні елементи документів.

Міжнародна співпраця є ключовим аспектом успішної протидії фальсифікаціям. Інтеграція у глобальні ініціативи обміну даними, участь у розробці єдиних стандартів перевірки документів та взаємодія з організаціями, що спеціалізуються на безпеці документів, дадуть змогу Україні покращити свої підходи та зміцнити власну систему захисту. Такі заходи сприятимуть не лише ефективнішому розслідуванню випадків підробки, а й зміцненню довіри до українських документів на міжнародній арені.

Розслідування сучасних підробок, у яких використовуються ключі шифрування, вимагає від правоохоронців глибоких знань, які виходять за межі класичних техніко-криміналістичних підходів. Електронний цифровий підпис (ЕЦП) є ключовим елементом сучасного документообігу, і його створення базується на складних криптографічних алгоритмах, таких як RSA, ECC або DSA. Розуміння принципів роботи цих алгоритмів є необхідним для оцінювання автентичності підпису, виявлення підробок і виявлення порушень у криптографічних протоколах. Крім того, аналіз криптографічних сертифікатів, що супроводжують ЕЦП, вимагає знань у сфері кібербезпеки. Перевірка автентичності таких сертифікатів, їхня відповідність довіреним центрам сертифікації, аналіз цифрових відбитків і ланцюгів довіри є невід'ємною частиною експертизи. Також сучасні підробки нерідко передбачають зміну зашифрованих елементів, таких як метадані або сам підпис, без порушення загальної структури документа. Для виявлення таких маніпуляцій необхідно знати методи перевірки цілісності хеш-функцій, аналізу криптографічних алгоритмів і виявлення вразливостей у системах шифрування. Зловмисники можуть використовувати атаки на криптографічні системи, зокрема на слабкі ключі або повторне використання підпису. Правоохоронцям важливо вміти ідентифікувати такі атаки та протидіяти їм, що потребує глибоких знань у галузі криптографії. Крім того,

підробки часто інтегруються з іншими цифровими технологіями, такими як редагування PDF-файлів, маніпуляція RFID-чипами або зміна цифрових відбитків. Це вимагає від фахівців розуміння криптографічних аспектів у ширшому контексті цифрової криміналістики. Законодавчі та нормативні аспекти також відіграють важливу роль, оскільки в багатьох країнах діють закони, які регулюють використання криптографії в електронному документообігу. Так, знання криптографії стають невід'ємною частиною роботи правоохоронців, що займаються розслідуванням підробок документів, і вимагають інтеграції міждисциплінарного підходу, який охоплює цифрову експертизу, криміналістику та інформаційну безпеку.

Згідно з дослідженням Cybersecurity Exposure Index (CEI) 2020 року, Україна посіла 50-те місце серед 108 країн з індексом 0,569 [4; 5], що свідчить про дуже високий рівень вразливості до кіберзагроз (Cybercrime Magazine) [3].

Таблиця 1 – Рейтинг вразливості країн до кіберзагроз

| Місце | Країна | Індекс вразливості |
|---|---|---|
| 1 | 2 | 3 |
| 1 | Фінляндія | 0.110 |
| 2 | Данія | 0.117 |
| 3 | Люксембург | 0.124 |
| 4 | Австралія | 0.131 |
| 5 | Естонія | 0.134 |
| 5 | Норвегія | 0.134 |
| 6 | Японія | 0.138 |
| 7 | Сполучені Штати | 0.145 |
| 8 | Австрія | 0.162 |
| 9 | Швейцарія | 0.172 |
| 10 | Нова Зеландія | 0.179 |
| 11 | Бельгія | 0.190 |
| 12 | Маврикій | 0.200 |
| 13 | Канада | 0.207 |
| 13 | Сполучене Королівство | 0.207 |
| 14 | Іспанія | 0.210 |
| 14 | Швеція | 0.210 |
| 15 | Франція | 0.228 |
| 16 | Сінгапур | 0.231 |
| 17 | Німеччина | 0.241 |

Продовження таблиці 1

| 1 | 2 | 3 |
|---|---|---|
| 17 | Катар | 0.241 |
| 18 | Хорватія | 0.255 |
| 18 | Ірландія | 0.255 |
| 19 | Нідерланди | 0.262 |
| 19 | Словаччина | 0.262 |
| 20 | Італія | 0.269 |
| 20 | Південна Корея | 0.269 |
| 21 | Словенія | 0.283 |
| 22 | Угорщина | 0.286 |
| 22 | Польща | 0.286 |
| 23 | Малайзія | 0.293 |
| 24 | Ізраїль | 0.297 |
| 24 | Литва | 0.297 |
| 25 | Португалія | 0.303 |
| 26 | Кіпр | 0.334 |
| 26 | Чехія | 0.334 |
| 27 | Ісландія | 0.348 |
| 27 | Уругвай | 0.348 |
| 28 | Латвія | 0.352 |
| 28 | Північна Македонія | 0.352 |
| 29 | Об’єднані Арабські Емірати | 0.359 |
| 30 | Грузія | 0.383 |
| 31 | Саудівська Аравія | 0.390 |
| 32 | Греція | 0.400 |
| 33 | Парагвай | 0.414 |
| 34 | Південна Африка | 0.417 |
| 35 | Кувейт | 0.428 |
| 36 | Сербія | 0.434 |
| 37 | Коста-Ріка | 0.438 |
| 38 | Таїланд | 0.445 |
| 39 | Румунія | 0.462 |
| 40 | Чилі | 0.469 |

Продовження таблиці 1

| 1 | 2 | 3 |
|---|---|---|
| 41 | Болгарія | 0.483 |
| 41 | Китай | 0.483 |
| 41 | Мексика | 0.483 |
| 41 | Туреччина | 0.483 |
| 42 | Домініканська Республіка | 0.497 |
| 43 | Аргентина | 0.514 |
| 44 | Росія | 0.528 |
| 45 | Азербайджан | 0.531 |
| 46 | Бразилія | 0.541 |
| 47 | Молдова | 0.545 |
| 48 | Єгипет | 0.548 |
| 48 | Кенія | 0.548 |
| 49 | Албанія | 0.566 |
| 50 | Панама | 0.569 |
| 50 | Україна | 0.569 |

*Джерело [4].*

Водночас у рейтингу National Cyber Security Index (NCSI), який вимірює готовність країн запобігати кіберзагрозам і реагувати на інциденти, Україна увійшла до топ-25, набравши 68,83 зі 100 можливих балів (Cybercrime Magazine) [3]. Це свідчить про певний прогрес у сфері кібербезпеки, однак залишається потреба в подальшому вдосконаленні захисних заходів для зниження вразливості до цифрових атак.

Вразливість країни до кіберзагроз та проблема підробки цифрових документів є взаємопов'язаними явищами, оскільки обидва загрожують стабільності цифрової екосистеми та безпеці інформації. Цифрові документи є важливим елементом сучасного документообігу, і їхня автентичність відіграє ключову роль у багатьох сферах – від фінансових операцій до державного управління. Уразливість систем, які відповідають за захист цих документів, дає зловмисникам можливість створювати підробки, маніпулювати даними або отримувати несанкціонований доступ до інформації. Кібератаки нерідко стають інструментом для порушення цілісності електронних документів або підробки цифрових сертифікатів.

Країна, що має слабку кіберзахисну інфраструктуру, стикається з великими ризиками в усіх секторах, де використовуються цифрові документи. Зокрема, слабкість криптографічних алгоритмів чи недосконаліть систем шифрування дають змогу зловмисникам обходити захист і підробляти електронні підписи або метадані. Це може стосуватися як державних реєстрів, так і приватних баз даних. У багатьох випадках такі підробки спрямовані на підрив довіри до державних інституцій чи фінансових систем.

Сучасні методи підробки документів використовують технології, подібні до тих, що застосовуються в кібератаках. Це охоплює злом програмного забезпечення, маніпуляції із зашифрованими файлами та використання вразливостей у протоколах передачі даних. Відсутність сучасної інфраструктури кіберзахисту робить країну вразливою до таких атак, особливо в умовах зростання кількості транскордонних операцій, що вимагають перевірки електронних документів. У багатьох випадках відсутність уніфікованих стандартів захисту створює додаткові труднощі в боротьбі з цими загрозами.

Так, недостатній рівень кібербезпеки підвищує ризики, пов'язані з використанням підроблених документів, і вимагає розробки комплексних заходів захисту. До них належать впровадження сучасних технологій, гармонізація міжнародних стандартів, а також системна підготовка фахівців, здатних оперативно виявляти загрози. Без надійного кіберзахисту ефективна боротьба з підробками електронних документів є практично неможливою, адже зловмисники постійно адаптуються до нових умов і технологій.

Під час воєнного стану вразливість до кіберзагроз стає особливо критичною, оскільки цифрові атаки набувають стратегічного характеру та стають невід'ємною частиною гібридної війни. Кібернапади спрямовуються не лише на критичну інфраструктуру, а й на урядові установи, військові системи, банки та енергетичні підприємства. Наприклад, під час воєнних дій в Україні 2022–2023 рр. хакерські атаки спричиняли збої в роботі державних сайтів, електронних реєстрів та комунікаційних систем. Відомий інцидент – кібератака на енергетичну інфраструктуру 2015 року, яка призвела до вимкнення електроенергії для сотень тисяч громадян, наочно демонструє руйнівні наслідки таких дій.

Крім того, під час війни зростає обсяг дезінформації, яка поширюється через зламані облікові записи, підроблені новини та фейкові вебресурси. Це підриває довіру громадян до державних інституцій та ускладнює координацію зусиль між військовими й цивільними органами. Наприклад, 2022 року зловмисники атакували сайти українських ЗМІ, розміщуючи фейкові новини про воєнні успіхи противника, щоб посіяти паніку серед населення.

Також під час воєнного стану особливо критичними стають атаки на системи управління логістикою та постачанням. Збої у таких системах можуть вплинути на транспортування гуманітарної допомоги, доставку озброєння та евакуацію населення. Один із прикладів – спроби зламати логістичні системи українських залізниць, що потенційно могли призвести до транспортного колапсу.

Отже, висока вразливість України до кіберзагроз у період війни несе значні ризики для функціонування держави, захисту критичної інфраструктури та підтримки інформаційної безпеки. Це підкреслює необхідність посилення захисних заходів, зокрема вдосконалення кібербезпеки на стратегічному рівні, посилення міжнародної співпраці та оперативної підготовки фахівців.

**Висновок.** Проблема підробки криміналістичних документів є однією з найбільш поширених форм злочинної діяльності, яка завдає значної шкоди інтересам громадян, державному бюджету, економіці країни та національній безпеці. Використання підроблених документів створює серйозні загрози, оскільки вони можуть слугувати інструментом для незаконних фінансових операцій, шахрайства, ухилення від податків, незаконного

перетину кордонів, приховування злочинів та інших протиправних дій. Традиційні методи, такі як почеркознавство, технічна експертиза та фізико-хімічний аналіз, є важливими інструментами у виявленні підробок. Однак сучасні реалії потребують їх поєднання з новітніми цифровими технологіями. Серед останніх – аналіз PDF-документів, перевірка автентичності електронних підписів, вивчення RFID-чипів, що використовуються в біометричних документах. Комплексний підхід до експертизи документів, за якого залучаються фахівці різних спеціалізацій, значно підвищує ефективність виявлення як примітивних, так і високотехнологічних махінацій.

Важливим елементом боротьби з підробками є міжнародна співпраця, що базується на систематизації безпекових вимог і стандартизації процесів перевірки документів. Регламенти, такі як Council Regulation (EC) No 2252/2004 [1] та ICAO Doc 9303 [2], відіграють ключову роль у створенні уніфікованих технічних і поліграфічних норм. Вони передбачають запровадження біометричних елементів у паспорти, стандарти безконтактних чипів і механізми інтеграції сучасних технологій у проїзні документи. Завдяки цим стандартам країни отримують можливість зменшити кількість фальсифікацій, уніфікувати процедури перевірки автентичності документів та налагодити більш ефективну взаємодію між різними відомствами як на національному, так і міжнародному рівнях. Це особливо важливо в умовах глобалізації, коли документи дедалі частіше використовуються у транскордонних операціях.

Однак для досягнення максимального ефекту від впровадження цих стандартів необхідно розвивати нормативно-правову базу. Законодавство повинно враховувати специфіку цифрових загроз, зокрема регулювати питання збереження та обробки електронних даних, обміну ключами між учасниками електронного документообігу та функціонування реєстрів електронних підписів. Удосконалення правових механізмів має супроводжуватися розширенням технічних можливостей. У цьому контексті важливим є придбання сучасного обладнання для криміналістичних досліджень, такого як спектрометри, ультрафіолетові та інфрачервоні аналізатори, а також впровадження програмних засобів для перевірки цифрових підписів і біометричних даних. Інтеграція штучного інтелекту дасть змогу автоматизувати процеси аналізу документів, підвищивши точність і скоротивши час їх вивчення.

Не менш важливим є аспект підготовки кваліфікованих фахівців. Регулярне проведення тренінгів, участь у міжнародних конференціях, обмін досвідом між експертами з різних країн дають змогу забезпечити високий професійний рівень криміналістів. Особлива увага має приділятися роботі з новітніми технологіями та методиками, що дає змогу виявляти навіть найскладніші випадки фальсифікацій. Паралельно потрібно заохочувати активну міжнародну співпрацю, яка сприятиме обміну найкращими практиками та підвищенню ефективності боротьби з підробками на глобальному рівні.

Отже, поєднання вдосконаленої нормативно-правової бази, використання сучасних технологій, підготовки компетентних фахівців і міжнародної координації утворюють єдиний ланцюг заходів, що забезпечують ефективну протидію фальсифікаціям документів. Усе це сприяє формуванню прозорого правового середовища, захисту прав громадян, збереженню стабільності та зміцненню довіри до державних і міжнародних документів.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States. *Official Journal of the European Union*, L 385/1.

2. International Civil Aviation Organization (ICAO). (2006). *Machine Readable Travel Documents, Part 1: Machine Readable Passports (6th ed.).* ICAO Doc 9303.

3. Cybercrime Magazine. (2020). *Global Cybersecurity Exposure Index 2020.* URL : https://cybersecurityventures.com

4. National Cyber Security Index (NCSI). (2020). *NCSI Rankings.* URL : https://ncsi.ega.ee/ncsi-index

5. 10Guards. (2020, June 26). *Global Cybersecurity Exposure Index 2020.* URL : https://10guards.com

6. Про електронні довірчі послуги : Закон України. *Відомості Верховної Ради України (ВВР).* 2017. № 45. Ст. 400. URL : https://zakon.rada.gov.ua/laws/show/2155-19

7. Кримінальний процесуальний кодекс України. *Відомості Верховної Ради України (ВВР).* 2012. № 9–10, № 11–12, № 13. Ст. 88. URL : https://zakon.rada.gov.ua/laws/show/4651-17

8. Міжнародна конвенція про спрощення і гармонізацію митних процедур (Кіотська конвенція) від 12.07.2023. URL : https://zakon.rada.gov.ua/laws/show/995_643#Text

9. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України. *Відомості Верховної Ради України (ВВР).* 1994. № 31. Ст. 286. URL : https://zakon.rada.gov.ua/laws/show/80/94-вр

10. Про електронні документи та електронний документообіг : Закон України. *Відомості Верховної Ради України (ВВР).* 2003. № 36. Ст. 275. URL : https://zakon.rada.gov.ua/laws/show/851-15#Text

# REFERENCES

1. Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States. *Official Journal of the European Union.* L 385/1.

2. International Civil Aviation Organization (ICAO). (2006). *Machine Readable Travel Documents, Part 1: Machine Readable Passports (6th ed.).* ICAO Doc 9303.

3. Cybercrime Magazine. (2020). *Global Cybersecurity Exposure Index 2020.* URL : https://cybersecurityventures.com

4. National Cyber Security Index (NCSI). (2020). *NCSI Rankings.* URL : https://ncsi.ega.ee/ncsi-index

5. 10Guards. (2020, June 26). *Global Cybersecurity Exposure Index 2020.* URL : https://10guards.com

6. On Electronic Trust Services : Law of Ukraine. *Official Bulletin of the Verkhovna Rada of Ukraine (VVR).* 2017. No. 45. Art. 400. URL : https://zakon.rada.gov.ua/laws/show/2155-19

7. Criminal Procedure Code of Ukraine. (2012). *Official Bulletin of the Verkhovna Rada of Ukraine (VVR).* No. 9–10, No. 11–12, No. 13. Art. 88. URL : https://zakon.rada.gov.ua/laws/show/4651-17

8. International Convention on the Simplification and Harmonization of Customs Procedures (Kyoto Convention) as of 12.07.2023. URL : https://zakon.rada.gov.ua/laws/show/995_643#Text

9. On Information Protection in Information and Telecommunication Systems : Law of Ukraine. *Official Bulletin of the Verkhovna Rada of Ukraine (VVR).* 1994. No. 31. Art. 286. URL : https://zakon.rada.gov.ua/laws/show/80/94-вр

10. On Electronic Documents and Electronic Document Management : Law of Ukraine. *Official Bulletin of the Verkhovna Rada of Ukraine (VVR).* (2003). No. 36. Art. 275. URL : https://zakon.rada.gov.ua/laws/show/851-15#Text

**O. M. Dudnyk. METHODS OF FORGING FORENSIC DOCUMENTS AND THEIR DETECTION**

*The article highlights the importance of a comprehensive and systematic study of methods of document falsification in forensics, taking into account their diversity and evolution, as well as the pivotal role of offenders who continuously improve their forgery skills. Combining traditional examination methods (such as handwriting analysis, technical, and physicochemical approaches) with modern digital technologies significantly enhances the effectiveness of countering the use of fake documents in legal practice. The article thoroughly analyzes the role of specialized equipment, qualified forensic specialists, and advanced information-analytical systems, which are critically important for the timely detection and identification of forged documents.*

*Special attention is paid to the need to consider rapid transformations in the field of high technologies and digitalization, which provide offenders with new tools for forgery. Issues related to modifying electronic documents, including editing PDF files, forging electronic digital signatures, and manipulating metadata, are discussed. It is noted that to counter such threats, it is necessary to implement modern technical solutions, conduct regular training for experts, and improve the regulatory framework governing the circulation and protection of electronic documents.*

*The authors emphasize that measures to detect document falsifications must be comprehensive. They should include strengthening legislative guarantees, improving organizational mechanisms within state and private institutions, and fostering international cooperation for the exchange of experience and best practices. The conclusion is drawn that progress in the methodological framework of forensic examination, considering modern challenges of the digital era, and harmonizing legislative approaches are key to forming an effective system for protecting the rights of citizens and the financial interests of the state.*

***Keywords:*** *forensics; document forgery; expertise; falsification; handwriting analysis; digital analysis; legal regulation.*

*Стаття надійшла до редколегії 4 лютого 2025 року*