© Babenko Y, Pryshchepa O. Hybrid authentication method for mass PDF documents based on digital signature and steganographic embedding // *Ukrainian Scientific Journal of Information Security, 2026, vol. 32, issue 1, pp. 14-18. © This is an open access article under the* CC BY 4.0 International license.

DOI: 10.18372/2225-5036.32.21641

ГІБРИДНИЙ МЕТОД АВТЕНТИФІКАЦІЇ МАСОВИХ PDF-ДОКУМЕНТІВ НА ОСНОВІ ЦИФРОВОГО ПІДПИСУ ТА СТЕГАНОГРАФІЧНОГО ВБУДОВУВАННЯ

Юрій Бабенко, Олександра Прищепа

Київський національний університет імені Тараса Шевченка, Україна



БАБЕНКО Юрій Михайлович, доктор філософії
Рік та місце народження: 1996, м. Дніпродзержинськ (зараз Кам'янське), Україна
Освіта: Київський національний університет імені Тараса Шевченка
Посада: асистент кафедри кібербезпеки та захисту інформації факультету інформаційних технологій Київського національного університету імені Тараса Шевченка
Наукові інтереси: безпека інформаційних та комунікаційних систем, програмування.
Публікації: більше 30 наукових публікацій, серед яких наукові статті, матеріали та тези доповідей на конференціях, навчально-методичні посібники та патенти.
E-mail: yurii.babenko@knu.ua
ORCID ID: 0000-0002-8115-3329



ПРИЩЕПА Олександра Олександрівна.
Рік та місце народження: 2005, м. Ніжин, Україна.
Освіта: Київський національний університет імені Тараса Шевченка.
Посада: студентка Київського національного університету імені Тараса Шевченка.
Наукові інтереси: інформаційна безпека, електронний документообіг, криптографічні методи захисту інформації, управління криптографічними ключами, цифрова стеганографія.
Публікації: 1 наукова публікація.
E-mail: pryshchepaoleksa@gmail.com
ORCID ID:

Анотація: *Робота присвячена розв'язанню задачі автентифікації PDF-документів у системах масового електронного документообігу, де застосування кваліфікованого електронного підпису є ускладненим або економічно недоцільним. Метою дослідження є розроблення методу, здатного забезпечити цілісність і справжність документів без використання зовнішніх сервісів довіри. Запропоновано гібридний підхід, що базується на поєднанні криптографічних засобів і цифрової стеганографії, який дозволяє встановити стійкий зв'язок між видимим вмістом документа та його графічною основою. Запропонований метод призначений для автоматизованого створення та перевірки документів та орієнтований на інтеграцію у високошвидкісні робочі процеси. Отримані результати свідчать про ефективність запропонованого рішення для виявлення несанкціонованих змін і підтверджують доцільність його використання у прикладних системах електронного документообігу.*

Ключові слова: *електронний документообіг, PDF-документи, цифровий підпис, стеганографія, LSB-алгоритм, автентифікація, цілісність даних, інформаційна безпека.*

Вступ

У сучасних умовах стрімкої цифровізації суспільства особливого значення набуває питання забезпечення належного рівня інформаційної безпеки в системах електронного документообігу. Переважна більшість установ, підприємств і державних органів переходять на електронні формати зберігання, обробки та передачі документів, що значно підвищує ефективність управління та швидкість обміну інформацією. Проте разом із перевагами цифрових технологій зростають і ризики, пов'язані з кіберзагрозами, несанкціонованим доступом, витоком даних та втручанням у роботу інформаційних систем.

На сьогоднішній день багато організацій не забезпечені комплексними та сучасними засобами захисту систем електронного документообігу. Недостатній рівень технічного оснащення, використання застарілого програмного забезпечення, відсутність чітко регламентованої політики інформаційної безпеки та низький рівень обізнаності персоналу створюють сприятливі умови для здійснення кібератак. Унаслідок цього можливі збої в роботі систем, пошкодження або повна втрата електронних документів, а також заволодіння конфіденційною інформацією сторонніми особами.

Таким чином, проблема забезпечення інформаційної безпеки в системах електронного документообігу є надзвичайно актуальною та потребує комплексного підходу до її вирішення, що включає впровадження сучасних технологій захисту, удосконалення нормативно-правової бази та підвищення рівня кіберграмотності працівників.

Постановка проблеми

Сучасні процеси цифровізації зумовлюють стрімке зростання обсягів електронного

документообігу. Значна кількість документів, зокрема довідки, сертифікати, заяви та онлайн-анкети, нині формуються автоматизовано через вебсистеми та інформаційні платформи. Такий підхід істотно спрощує взаємодію між користувачами й установами, проте водночас актуалізує проблему забезпечення цілісності та автентичності електронних документів. Законодавчо в Україні передбачено використання кваліфікованого електронного підпису як юридичного аналога власноручного підпису [1]. Однак на практиці впровадження кваліфікованого електронного підпису у малих організаціях та сервісах масового формування документів часто є ускладненим через організаційні, фінансові та технічні чинники. У результаті багато установ застосовують спрощені механізми ідентифікації, такі як вставлення сканованих підписів, внутрішніх номерів або QR-кодів, що не забезпечують належного рівня захисту та легко піддаються підробці.

Особливо вразливими є PDF-документи, які є найбільш використовуваними і досить легко можуть бути змінені за допомогою відповідних інструментів без помітних для користувача слідів. Відсутність вбудованих механізмів контролю справжності в системах електронного документообігу створює передумови для фальсифікації інформації та знижує рівень довіри до цифрових сервісів.

Перспективним напрямом підвищення захищеності електронних документів є поєднання криптографічних методів із засобами цифрової стеганографії. Криптографія забезпечує цілісність і справжність даних [2], тоді як стеганографія дозволяє приховати сам факт наявності захисного маркера у візуальному вмісті документа [3]. Такий гібридний підхід створює можливість формування крихкого механізму верифікації, за якого будь-яка модифікація документа призводить до втрати його автентичності.

Особливу практичну цінність подібні рішення мають для автоматизованих систем масової генерації документів, наприклад, у приймальних комісіях закладів освіти, онлайн-сервісах подачі заяв або видачі сертифікатів, де важливими є швидкість обробки та мінімальна участь людини.

Аналіз останніх досліджень і публікацій

Питанню інформаційної безпеки в системі електронного документообігу присвячена досить велика кількість публікацій, як вітчизняних науковців [4 - 6], так і зарубіжних [7 -10].

У роботі [4] подано опис основних загроз для систем електронного документообігу та розглянуто важливість системи електронного документообігу для організаційних процесів підприємств та забезпечення інформаційної безпеки. Основну увагу зосереджено на сучасних антивірусних технологіях.

У роботі [5] розглянуто проблему ідентифікації документів в системах електронного документообігу. Після аналізу можливих методів ідентифікації встановлено, що метод, оснований на використанні електронних ключів дозволяє надійно встановити авторство документа, надає можливість встановити час підпису, забезпечує безвідмовність факту підпису та не потребує значних ресурсів для його формування та перевірки. В основу методу покладено алгоритм цифрового підпису еліптичної кривої.

У роботі [6] обгрунтовано, що впровадження заходів інформаційної безпеки в системах електронного документообігу сприятиме підвищенню ефективності прийняття управлінських рішень, прозорості в діяльності організації, покращенню рівня безпеки та збереженню інформації. Запропоновано напрями підвищення рівня інформаційної безпеки систем електронного документообігу, проаналізовано засоби захисту систем електронного документообігу.

Робота [7] присвячена дослідженню та опрацюванню методів створення систем електронного документообігу організацій, підвищення рівня захисту документів та інформації, що зберігаються та обробляються в цій системі. З цією метою розглянуто питання створення розподіленої структурованої системи управління електронними документами, використано різні методи захисту для забезпечення конфіденційності інформації, запропоновано використовувати процедуру аутентифікації та безпечні методи шифрування.

У роботі [8] описується децентралізована система управління електронними документами, яка підвищує безпеку та цілісність цифрових документів шляхом децентралізації прав доступу та використання технології блокчейн. Запропонована система шифрує цифрові документи за допомогою симетричного ключа, а потім ключ розділяється та розподіляється між декількома користувачами за допомогою схеми розподілу Шаміра. Зашифровані документи зберігаються за допомогою файлової системи InterPlanetary (IPFS), що забезпечує цілісність за допомогою адресації на основі вмісту. Хоча система має накладні витрати на продуктивність, особливо з великими документами, вона ефективно запобігає несанкціонованому доступу та фальсифікації.

Робота [9] містить огляд сучасних проблем і технологій у сфері безпеки електронних документів, а також презентує набір рішень для забезпечення їх інформаційної безпеки. Описані результати впровадження системи Electronic Security Suite контролю документів і цифрових підписів для захисту електронних документів, що динамічно захищає електронні документи як у мережі, так і поза нею, в режимі онлайн і офлайн, забезпечуючи комплексну безпеку протягом усього життєвого циклу електронного документа.

Цікавою є робота [10], де для захисту інформації в електронних документах формату Open Office XML використовується модифікований стеганографічний метод заміни найменш значущого біта. Зазвичай цей метод використовується з мультимедійним контентом, а у роботі він адаптований до кольорового простору RGB символів тексту електронного документа.

Аналіз літератури показує, що тема захищеності цифрових документів у системах електронного документообігу є актуальною для сучасних реалій. Водночас, тема недостатньо досліджена, оскільки багато аспектів залишаються відкритими.

Мета дослідження

Метою дослідження є розроблення гібридного методу автентифікації PDF-документів, орієнтованого на автоматизовані системи масової генерації, шляхом поєднання цифрового підпису та стеганографічного вбудовування захисного маркера у графічну основу документа.

Виклад основного матеріалу

Об'єктом дослідження є електронний PDF-документ, що складається з текстового шару та графічної основи. У контексті систем масового формування документів такий файл містить персональні дані користувачів, службові реквізити та іншу значущу інформацію, достовірність якої має бути гарантована.

Нехай D — фінальний PDF-документ, T — його видимий текстовий вміст, а G — фонове растрове зображення. Необхідно побудувати механізм M, який забезпечує криптографічний зв'язок між T та G таким чином, щоб будь-яка модифікація документа могла бути однозначно виявлена під час перевірки.

Задача полягає у створенні методу, що одночасно гарантує цілісність текстового шару, автентичність усього PDF-документа та можливість автоматизованого виявлення несанкціонованих змін без використання зовнішніх сервісів довіри. Додатковою вимогою є відсутність помітних візуальних спотворень, оскільки сформований документ має зберігати звичний для користувача вигляд.

Особливістю поставленої задачі є орієнтація на сценарії масової генерації документів, де підписання повинно виконуватися автоматично та швидко, з мінімальною участю людини. Типовим прикладом є приймальні комісії закладів освіти або онлайн-сервіси подачі заяв, у яких документ формується одразу після введення даних користувачем.

Таким чином, шуканий механізм має поєднувати криптографічну надійність цифрового підпису з можливістю прихованого вбудовування захисного маркера у графічну складову документа, що дозволяє встановити жорсткий зв'язок між його вмістом і візуальною основою.

У межах даної роботи розглядається модель порушника, який має повний доступ до фінального PDF-документа. Передбачається, що атакувальник може відкривати файл у стандартних редакторах, змінювати текстові поля, замінювати фонові зображення, перезберігати або перескладати документ у новому вигляді. Також допускається, що структура PDF може бути повністю проаналізована, а використовувані алгоритми є відомими (white-box модель). Водночас вважається, що порушник не має доступу до приватного ключа системи-видавця документа та не може згенерувати коректний цифровий підпис. Генерація і зберігання ключової пари здійснюється на стороні організації, яка формує документ, тоді як користувач бере участь лише на етапі введення даних і підтвердження заявки.

Основною загрозою є несанкціонована модифікація вмісту документа з метою підробки персональних даних, службових реквізитів або ідентифікаторів. Типові сценарії атак включають зміну ПІБ, дат, номерів заяв чи сертифікатів, підміну інформації про отримувача, а також створення фальшивих копій документів з метою видавання себе за іншу особу або представлення підробленого документа як виданого легітимним сервісом. Окрему небезпеку становить можливість маніпуляцій із візуальним шаром PDF, коли справжній документ використовується як шаблон для створення переконливих фальсифікацій. Подібні дії є характерними для систем електронного документообігу, що не мають вбудованих механізмів контролю справжності.

Запропонований підхід орієнтований на протидію таким візуальним та структурним атакам шляхом жорсткого зв'язування текстового вмісту з графічною основою документа, що забезпечує виявлення будь-яких змін незалежно від способу їх внесення.

Метод вважається ефективним, якщо за заданої моделі загроз виконуються такі умови:

- будь-яка зміна текстового вмісту PDF призводить до негативного результату верифікації;
- заміна або модифікація фонового зображення також коректно виявляється системою;
- у випадку відсутності втручань документ успішно проходить перевірку автентичності;
- процес вбудовування захисного маркера не створює візуальних артефактів, помітних для користувача.

Додатковим практичним критерієм є можливість автоматичного використання методу в системах масової генерації документів без значного впливу на швидкодію та без необхідності залучення сторонніх сервісів електронного підпису.

Метод, запропонований в цій роботі, орієнтований саме на автоматизовані системи масового формування PDF-документів та реалізує гібридний підхід, що поєднує криптографічний цифровий підпис із прихованим стеганографічним вбудовуванням захисного маркера.

Процес створення документа починається з введення користувачем необхідних персональних або службових даних через програмний інтерфейс. Користувач не генерує криптографічних ключів і не виконує операцій підписання. Усі криптографічні процедури здійснюються серверним модулем системи-видавця.

Після підтвердження введених даних система автоматично формує PDF-документ на основі заданого шаблону. На цьому етапі реалізується логіка двостороннього підписання: документ

підписується від імені організації, а згода користувача фіксується у межах прикладного процесу. У результаті формується фінальний PDF-файл, що містить текстовий шар та фонове растрове зображення.

Особливістю архітектури є відсутність залежності від зовнішніх сервісів кваліфікованого електронного підпису, що забезпечує високу швидкодію та можливість масштабування рішення для сценаріїв масової генерації документів.

Ключовою особливістю запропонованого підходу є використання візуального представлення документа як основи для автентифікації. Замість аналізу структурних елементів PDF або текстового шару застосовується повний рендер сторінки у піксельне представлення.

Після формування документа PDF-сторінка рендериться у растрове зображення, з якого отримується масив піксельних даних P. Далі обчислюється криптографічний хеш H:

$$H = SHA256(P)$$

Отримане значення H є візуальним хешем документа і однозначно характеризує його фактичний зовнішній вигляд. Будь-яка, навіть мінімальна, зміна тексту, шрифтів, позиціонування елементів або графічної основи призводить до повної зміни хеш-відбитка.

Такий підхід дозволяє уникнути проблем, пов'язаних з неоднозначністю витягування тексту з PDF у різних середовищах, та забезпечує прив'язку автентичності саме до того вигляду документа, який сприймає користувач.

Сформований візуальний хеш підписується приватним ключем системи-видавця за алгоритмом ECDSA.

У результаті формується зашифрований бінарний блок, який використовується як корисне навантаження для подальшого вбудовування.

Зашифрований підпис інтегрується у фонове зображення формату PNG методом Least Significant Bit [3, 10]. Вбудовування виконується шляхом модифікації найменш значущого біта кожного з каналів RGB.

Використання багатоканального LSB забезпечує високу місткість контейнера при відсутності помітних візуальних артефактів. Додатково застосовується фонове зображення з хаотичною текстурою або шумовими елементами, що підсилює маскування змін і ускладнює їх виявлення.

Після завершення вбудовування модифіковане зображення використовується як графічна основа фінального PDF-документа. Таким чином формується крихкий механізм автентифікації, за якого будь-яке втручання у документ призводить до втрати його справжності.

Перевірка автентичності здійснюється у зворотній послідовності. Спочатку з PDF вилучається фонове зображення, з якого за допомогою зворотного LSB-алгоритму реконструюється зашифрований підпис. Після дешифрування отримується цифровий підпис S.

Паралельно документ повторно рендериться у піксельне представлення, і обчислюється поточний візуальний хеш:

$$H' = SHA256(P')$$

де P' — піксельні дані документа, що перевіряється.

На завершальному етапі за допомогою публічного ключа системи-видавця виконується перевірка відповідності підпису. У разі повної відповідності документ визнається автентичним. Будь-яка розбіжність інтерпретується як результат несанкціонованої модифікації, незалежно від способу її внесення.

Висновки

Запропонований гібридний метод для автентифікації PDF-документів у системах масового електронного документообігу демонструє властивості крихкого водяного знаку, за якого будь-яке втручання у документ призводить до втрати автентичності. Зокрема:

- редагування текстового вмісту призводить до зміни візуального рендера та детектується системою;
- заміна або модифікація фонового зображення також коректно виявляється;
- перезбереження або повторне формування PDF змінює піксельне представлення сторінки та спричиняє негативний результат перевірки.

Таким чином, автентичність документа жорстко прив'язується до його фактичного візуального вигляду, що робить метод ефективним проти поширених атак візуальної підробки.

Основною особливістю підходу є прив'язка автентичності не до внутрішньої структури файлу, а до його фактичного візуального вигляду, що дозволяє ефективно виявляти широкий спектр модифікацій.

Сильними сторонами запропонованого методу є:

- використання візуального хешу, сформованого на основі піксельного рендера документа;
- приховане стеганографічне вбудовування підпису у фонове зображення;
- відсутність залежності від зовнішніх сервісів кваліфікованого електронного підпису.

Масштабованість запропонованого методу забезпечується використанням лінійних за складністю операцій (рендеринг, хешування, LSB-вбудовування), що робить його придатним для використання у високонавантажених системах. Автоматизований характер підписання дозволяє застосовувати рішення у сценаріях масової генерації документів без залучення оператора на кожному етапі.

Найбільш очевидними сферами застосування є системи онлайн-подачі заяв, приймальні комісії навчальних закладів, сервіси видачі довідок та сертифікатів, а також внутрішні документообіги малих і середніх організацій.

У таких сценаріях користувач вводить дані та підтверджує заявку, після чого система автоматично

формує та підписує документ від імені установи. Отриманий PDF може бути перевірений будь-якою стороною без доступу до внутрішніх баз даних, що спрощує процес верифікації та знижує ризик фальсифікації.

Література

[1] Верховна Рада України. Про електронну ідентифікацію та електронні довірчі послуги: Закон України № 2155-VIII від 05.10.2017 р. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text (дата звернення: 12.02.2026).

[2] Wong D. Real-World Cryptography. Shelter Island, NY: Manning Publications, 2021. 475 p. URL: https://www.manning.com/books/real-world-cryptography (accessed: 12.02.2026).

[3] Конахович Г. Ф., Прогонов Д. О., Пузиренко О. Ю. Комп'ютерна стеганографічна обробка й аналіз мультимедійних даних: підручник. Київ: «Центр учбової літератури», 2018. 558 с.

[4] Fedoruk O. Security and protection of information in electronic document management systems: improving the level of cyber defense. *Вісник Книжкової палати*. 2024. № 4. P. 39-44. DOI: 10.36273/2076-9555.2024.4(333).39-44.

[5] Батурін Є. Л., Воловщиков В. Ю., Шапо В. Ф. Інформаційна технологія підсистеми ідентифікації на основі електронних ключів в системах електронного документообігу. *Вісник Національного технічного університету «ХПІ». Серія: Системний аналіз, управління та інформаційні технології*. 2020. № 1 (3). С. 89-96. DOI: 10.20998/2079-0023.2020.01.16.

[6] Піддубна Л.В., Павліченко В.М. Інформаційна безпека в системах електронного документообігу. *Науковий вісник ПУЕТ*. 2019. № 4 (95). С. 59—66. DOI: 10.37734/2409-6873-2019-4-7.

[7] Gasimov V.A., Mammadzada N.F., Mammadov J.I., Aliyeva K.J. The problem of information protection in electronic document management systems of medical organizations. *Проблеми інформатизації та управління*. 2025. 1 (81). P. 37-45. DOI: 10.18372/2073-4751.81.20127.

[8] Han J., Son Y. Design and implementation of a decentralized document management system. *Expert Systems with Applications*. 2024. P. 125516. DOI: 10.1016/j.eswa.2024.125516.

[9] Sunbula M., Nafisa Y., Nuriddin S. Aspects of information security in the electronic document management system (EDMS) for bank system. *Research and education*. 2022. Vol. 1, no. 9. P. 331–340. DOI: 10.5281/zenodo.7487114.

[10] Barannik V., Babenko M., Babenko Y., Yalova K. and Yashyna K. Modification of the RGB Color Space in MS Word Documents for Steganographic Information Protection. *Intelligent & CyberPhysical Systems ICyberPhyS-2024*: CEUR Workshop Proceedings 1th International Conference, Khmelnytskyi, Ukraine, 27 - 29 June 2024. Vol. 3736, pp. 269–281. URL: https://ceur-ws.org/Vol-3736/paper20.pdf

УДК 004.056

Babenko Y. M., Pryshchepa O.O. Hybrid authentication method for mass PDF documents based on digital signature and steganographic embedding

***Abstract**. This paper is devoted to solving the problem of PDF document authentication in mass electronic document management systems, where the use of qualified electronic signatures is complicated or economically impractical. The aim of the research is to develop a method capable of ensuring the integrity and authenticity of documents without the use of external trust services. A hybrid approach based on a combination of cryptographic means and digital steganography is proposed, which allows establishing a stable connection between the visible content of the document and its graphic basis. The proposed method is designed for automated document creation and verification and is focused on integration into high-speed workflows. The results obtained demonstrate the effectiveness of the proposed solution for detecting unauthorized changes and confirm the feasibility of its use in applied electronic document management systems.*

***Keywords:** electronic document management, PDF documents, digital signature, steganography, LSB algorithm, authentication, data integrity, information security.*

Бабенко Юрій Михайлович, доктор філософії, асистент кафедри кібербезпеки та захисту інформації факультету інформаційних технологій Київського національного університету імені Тараса Шевченка.
Yurii Babenko, PhD, Assistant Professor, Department of Cybersecurity and Information Protection, Faculty of Information Technologies, Taras Shevchenko National University of Kyiv.

Прищепа Олександра Олександрівна, студентка кафедри кібербезпеки та захисту інформації факультету інформаційних технологій Київського національного університету імені Тараса Шевченка.
Oleksandra Pryshchepa, student, Department of Cybersecurity and Information Protection, Faculty of Information Technologies, Taras Shevchenko National University of Kyiv.

Дата надходження:	Дата прийняття:	Дата публікації:
24.02.2026	10.03.2026	22.04.2026