Метою роботи є розробка комбінованого стеганографічного методу для захисту авторського права на цифрові зображення з застосуванням ЦВЗ, стійкого до стиснення.

В основі розробленого методу лежить комбінований підхід DWT-SVD як найбільш збалансований інструмент, що забезпечує одночасну візуальну невидимість (прозорість) вбудованого водяного знаку та його робастність (стійкість) до атак стиснення. Алгоритм вбудовування передбачає перехід зображення-контейнера в колірний простір YCbCr, де модифікації піддається лише канал яскравості (Y). До цього каналу застосовується дискретне вейвлет-перетворення на базі фільтра Хаара, що дозволяє виділити низькочастотну область апроксимації (LL), яка містить основну енергетичну складову зображення. Паралельно з цим, авторський водяний знак (логотип) піддається криптографічному скремблюванню за допомогою хаотичного перетворення Арнольда. Це перетворює впізнаваний підпис на візуальний шум, який неможливо відновити без знання секретного ключа. Математичне ядро системи реалізує модифікацію сингулярних чисел матриці LL-піддіапазону контейнера шляхом додавання до них сингулярних чисел зашифрованого знаку з певним коефіцієнтом інтенсивності α. Для реалізації «напівсліпої» схеми вилучення програма автоматично генерує та зберігає файл матричних ключів формату .npz. Це дозволяє проводити верифікацію авторства без наявності оригінального зображення, використовуючи лише захищене фото та збережені ортогональні матриці.

Експериментальні дані розробленого методу підтвердили його високу ефективність. PSNR = 41,8 дБ, що свідчить про ідеальну візуальну стійкість вбудованого ЦВЗ. Тестування на робастність продемонструвало, що водяний знак зберігає свою структуру та залишається впізнаваним після агресивного стиснення JPEG з фактором якості до 20%.

1. Мокін В. Б., Капшук О. В. Методи та засоби стеганографічного захисту інформації : монографія. Вінниця : ВНТУ, 2021. 180 с. URL: https://ir.lib.vntu.edu.ua/

Розробка безпечної системи таємного голосування

УДК 004.056.5

Володимир Гудиш [1], Валерій Трушевський [2]

Львівський національний університет імені Івана Франка, [1]volodymyr.hudysh@lnu.edu.ua, [2]valeriy.trushevsky@lnu.edu.ua

Голосування є ключовим механізмом народного волевиявлення в демократичному суспільстві. Проте сучасні виклики, зокрема пандемія COVID-19, повномасштабне збройне вторгнення Росії в Україну та вимушена міграція мільйонів громадян як всередині країни, так і за кордон, унеможливили або суттєво ускладнили участь у традиційному виборчому процесі. Ці обставини актуалізували запит на системи дистанційного електронного голосування як засіб забезпечення конституційного права на волевиявлення за будь-яких умов.

Більшість наявних рішень змушені балансувати між конкуруючими вимогами. Традиційні паперові системи не забезпечують математично доведеної верифікованості результатів, а процес підрахунку голосів залишається непрозорим для незалежних спостерігачів. Сучасна криптографія виборів демонструє фундаментальну напругу між верифікованістю результатів та захистом від примусу [6]: системи, що ставлять абсолютний пріоритет на верифікованості, як правило, надають виборцю докази, якими може скористатися зловмисник або роботодавець. Водночас повне усунення будь-якої верифікованості перетворює криптографію на "чорну скриньку", якій виборець змушений сліпо довіряти. Тому завданням є не вибір одного з полюсів, а свідоме позиціювання на цьому спектрі: досягнення достатнього рівня верифікованості при одночасному збереженні анонімності та недопущенні можливості довести конкретний вибір виборця стороннім особам.

З метою вирішення зазначених проблем розроблено безпечну систему таємного голосування, яка забезпечує анонімність виборця, верифікованість результатів та захист від широкого спектру криптографічних і мережевих атак без необхідності довіряти будь-якому окремому компоненту системи. Запропоновано та реалізовано систему з елементами підходу Zero Trust, що поєднує: гомоморфне шифрування ElGamal на еліптичній кривій SECP256R1 [1] для агрегації голосів без розшифрування; три незалежні рівні доказів з нульовим розголошенням (ZKP): диз'юнктивний OR-доказ коректності голосу, Sum-доказ одиничного вектора бюлетеня [9] та доказ коректності дешифрування Чаума–Педерсена [2]; сліпі підписи за RFC 9474 (RSABSSA-SHA384-PSS-Randomized) [3] для унеможливлення зв'язування виборця з бюлетенем; порогове дешифрування за схемою Шаміра (2-з-3) [4] із захистом ключових часток у HashiCorp Vault з шифруванням Fernet [7]; а також окремий клієнтський застосунок із вбудованим Tor для анонімної маршрутизації трафіку.

Система складається з трьох незалежних серверів та клієнтського застосунку. *Main Server* (Python/Flask) відповідає за автентифікацію виборців і ведення публічного Bulletin Board. *Validator Server* (TypeScript/Node.js, бібліотека @cloudflare/blindrsa-ts) верифікує право голосу та видає сліпий підпис, не маючи змоги асоціювати його з конкретним виборцем. *Election Agency* (Python/Flask) верифікує ZKP-докази і сліпий підпис та публікує агреговані результати. Клієнтський застосунок (Python/customtkinter) надсилає бюлетень безпосередньо до Election Agency через Tor (.onion-адреса) [8], повністю виключаючи Main Server з ланцюжка передачі голосу.

Бюлетень формується як unit vector — масив шифротекстів ElGamal, де кожна позиція містить зашифроване значення 0 або 1. Sum-доказ гарантує, що сума елементів вектора дорівнює рівно 1 [9]. Tracking Code, що є хешем SHA-384 від JSON-об'єкта бюлетеня, обчислюється на стороні клієнта і публікується на Bulletin Board: виборець у будь-який момент може переконатися у врахуванні свого голосу (Individual Verifiability). На етапі підрахунку Election Agency виконує гомоморфне додавання шифротекстів окремо для кожного кандидата, збирає частки приватного ключа з двох серверів і розшифровує агреговані суми. Для кожного кандидата публікується Decryption Proof — доказ рівності

квантових алгоритмів. Це означає, що у разі появи масштабованих квантових комп'ютерів такі алгоритми можуть бути повністю скомпрометовані.

Натомість симетричні алгоритми шифрування, зокрема AES, є менш вразливими до квантових атак. Використання алгоритму Гровера дозволяє лише квадратично прискорити перебір ключів, що фактично зменшує ефективну довжину ключа вдвічі. У практичному вимірі це означає необхідність переходу на довші ключі (наприклад, використання AES-256 замість AES-128) для збереження належного рівня безпеки [3]. Подібний підхід застосовується і до криптографічних хеш-функцій. Квантові алгоритми знижують їх стійкість до пошуку колізій, однак не призводять до повної компрометації. Відповідно, підвищення рівня безпеки досягається шляхом використання хеш-функцій із більшою довжиною вихідного значення.

З огляду на зазначені ризики, ключовим завданням є підготовка IT-інфраструктури до поступового переходу на квантово-стійкі механізми захисту. Одним із базових принципів такої підготовки є впровадження підходу crypto-agility — здатності систем гнучко змінювати криптографічні алгоритми без суттєвих змін архітектури. Першочерговим кроком є інвентаризація криптографічних залежностей, включаючи TLS, VPN, PKI, API та системи управління секретами. Це дозволяє визначити критичні компоненти інфраструктури та пріоритети їх модернізації. Важливим аспектом є централізоване управління ключами та сертифікатами, що спрощує їх ротацію та подальший перехід на нові алгоритми. Додатково доцільним є впровадження гнучких конфігурацій безпеки, зокрема підтримки змінюваних криптографічних наборів і гібридних рішень.

У висновку слід зазначити, що підготовка до квантової епохи не є одноразовим заходом, а тривалим процесом трансформації IT-інфраструктури. Впровадження принципів гнучкості, централізації управління криптографією та поступової міграції дозволить знизити ризики та забезпечити стійкість систем у майбутньому.

1. Kumar M. Post-quantum cryptography Algorithm's standardization and performance analysis. Array. – 2022. – Vol. 15. – Article 100242.
2. Воробець П. А., Горпенюк А. Я., Опірський І. Р. Перехід до постквантових криптографічних систем: виклики, стандартизація та перспективи // Безпека інформації. – 2024. – Т. 30, № 2. – С. 306–315
3. Alagic G., et al. Status Report on the Fourth Round of the NIST Post-Quantum Cryptography Standardization Process. NIST IR 8545. – 2025. – 54 p.

З історії становлення національної системи захисту інформації. 1992–1999 рр.

УДК 94:35.083.8(045)

Валерій Ворожко

СБ України, wp06vv@gmail.com