**УДК 681.3.05**

В. Г. Красиленко[1], Р. О. Яцковська[2], Ю. М Тріфонова[1]

1 - Вінницький соціально-економічний інститут Університету «Україна»
2 – Вінницький національний аграрний університет

# ДЕМОНСТРАЦІЯ ПРОЦЕСІВ СТВОРЕННЯ СЛІПИХ ЕЛЕКТРОННИХ ЦИФРОВИХ ПІДПИСІВ НА ТЕКСТОГРАФІЧНУ ДОКУМЕНТАЦІЮ НА ОСНОВІ МОДЕЛЕЙ МАТРИЧНОГО ТИПУ

*В роботі розглядаються результати моделювання сліпих електронних цифрових підписів на конфіденційну текстографічну документацію на основі моделей матричного типу та демонструються конкретні приклади створення таких підписів у програмному середовищі Mathcad Professional. Показано, що на основі таких моделей час створення підписів для текстографічних документів формату А4 та напівтонових зображень значної розмірності не перевищує декількох хвилин.*

***Ключові слова:*** *сліпий електронний цифровий підпис, матрична модель RSA,криптографічна система, протокол формування ключів, верифікація електронних підписів.*

## Вступ

Однією з актуальних та необхідних задач, особливо при використанні сучасних електронних комунікацій для подання звітності в державні податкові органи у вигляді конфіденціальних текстографічних документів (ТГД) та необхідності їх засвідчення підписами відповідальних осіб, є задача створення електронних цифрових підписів (ЕЦП). Існує ціла низка різновидів таких ЕЦП. Серед них можна відмітити незаперечні підписи, сліпі підписи та інші. Документи з конфіденційною економічною інформацією часто представлені у вигляді цифрових масивів, таблиць, малюнків, графіків, діаграм, резолюцій та підписів осіб, що приймають рішення. Існує низка класичних шифрів та процедур створення цифрових підписів, в тому числі тих, що базуються на відповідних державних стандартах [1]. Але більшість відомих криптографічних алгоритмів та протоколів створення ЕЦП, протоколів формування ключів та систем верифікації ЕЦП орієнтовані на послідовну скалярну обробку блоків ТГД, які попередньо перетворені у відповідні цифрові формати. Особливістю таких блоків є те, що вони представлені числами дуже великої розрядності. Це спричинює до суттєвого зниження обчислювальної швидкодії криптографічних процедур, що виконуються програмно-апаратними засобами.

## Аналіз останніх досліджень та публікацій

В роботах [2,3] були запропоновані матричні моделі та алгоритми крипто перетворень на півтонових та кольорових зображень, які можуть бути успішно використані, як найбільш узагальнені, при за шифруванні та розшифруванні любих ТГД. Результатам моделювання матричних афінно-перестановочних алгоритмів присвячена робота [4], в якій показано, що такі алгоритми є теж деяким узагальненням матричних афінних шифрів та алгоритмів. Модифікації системи RSA на матричний випадок для створення матричних моделей та алгоритмів крипто перетворень зображень були запропоновані в роботі [5]. Там же були наведені результати моделювання таких алгоритмів при обробці ними зображень та ТГД. Сліпі ЕЦП на основі матричних афінних шифрів та результати їх моделювання розглядалися і в роботі [6]. Для більшості запропонованих матричних моделей криптоперетворень необхідні відповідні 2-D ключі, а тому в роботі [7] були наведені результати моделювання протоколів створення таких ключів. Проблемі створення та моделювання сліпих ЕЦП для ТГД за допомогою матричних моделей та алгоритмів на основі базової моделі RSA присвячена робота [8]. Але в ній наводилися результати моделювання таких ЕЦП названих авторами ЕЦП матричного типу (МТ), далі ЕЦП МТ, лише для невеликих масивів чорно-білих на півтонових зображень розмірністю 128×128 елементів.

**Постановка задачі**. Тому метою даної роботи є подальше дослідження та узагальнення матричних моделей при створенні сліпих ЕЦП МТ та демонстрація за допомогою модельних експериментів у програмному середовищі Mathcad Professional їх функціональних можливостей в процесах створення підписів на конкретні великоформатні ТГД.

## Виклад основних результатів

Можна показати, що більшість відомих ЕЦП скалярного типу (СТ), модифікуються на матричний випадок аналогічно до підходів, що запропоновані в роботах [2,3,6]. Теоретичні основи створення сліпих ЕЦП МТ за допомогою матричних афінних шифрів розглядалися в роботі [6], а ідея модифікацій класичних ЕЦП СТ на матричний випадок базується на узагальненні та модифікації базового скалярного алгоритму RSA до відповідної матричної моделі, яка наведена в роботі [5]. Запропонований підхід при модифікації відомих ЕЦП до ЕЦП МТ полягає в тому, що якості ключів для за шифрування та розшифрування ТГД вибираються не скаляри, а відповідні матриці KEYP та OKEY. Кожен елемент таких матриць вибирається з допустимої множини значень, що відповідають умовам аналогічним у класичному RSA та базуються на використанні добутку двох простих чисел та функції Ейлера. Для цього вибирається таких два простих числа k та l або дві матриці K та L з елементами попарно простих чисел $k_{ij}$ та $l_{ij}$, таких щоб їх добуток $n_{ij} = k_{ij} * l_{ij}$ не перевищував значення елемента масиву, що підлягає за шифруванню і представлений байтом або трьома байтами для кольорового формату. Значення елементів матричних ключів KEYP та OKEY вибираються з множини взаємно простих чисел, що задається відповідною функцією Ейлера від $n_{ij}$, яка і визначає потужність цієї множини. Потужність множини ключів залежить як від потужності множини допустимих значень для кожного елемента так і від загальної кількості елементів у 2-D масиві. А це при значних розмінностях масивів дає прийнятні високі оцінки. Таким чином, підходящі ключі формуються як матриці великої розмірності, кожен елемент яких випадковим чином вибирається з великої множини допустимих значень відповідних скалярних ключів $e_{ij}$ та $d_{ij}$. Для моделювання ми використовували матриці розмірністю 704 × 572 елементи та ТГД формату А4.

Результати моделювання процесу створення сліпих ЕЦП МТ на основі модифікованих матричних RSA- алгоритмів у програмному середовищі Mathcad показані на рисунках 1 та 2. На рис. 1 показані інтерфейс, вікна програми, програмні модулі та формули, які використовувалися для моделювання.

Процес створення сліпих ЕЦП МТ полягає в здійсненні таких кроків. Для створення сліпого ЕЦП МТ на документ ТГД (матриця S1) останній коригується так, щоб отримати зображення – матрицю MPR. Така корекція полягає у зменшенні тих градацій інтенсивності чи значень пік селів, що перевищують допустимі значення $n_{ij}$. Ключ KG ми використовуємо для закриття документа S1 або скоригованого масиву MPR. Цей ключ також коригується абонентом, в результаті чого утворюється новий ключ KGP. Необхідність останнього коригування ключа полягає в додаванні одиничного рівня інтенсивності до тих значень інтенсивності елементів матриці KG, які не відповідають допустимій множині попарно взаємно простих чисел, що визначається функцією Ейлера від $n_{ij}$. Ключ KEYP, що формується з генерованої випадковим чином матриці G2, використовується для по елементного матричного піднесення у степінь за відповідним модулем ключа KGP. В результаті цього формується допоміжна матриця T1:

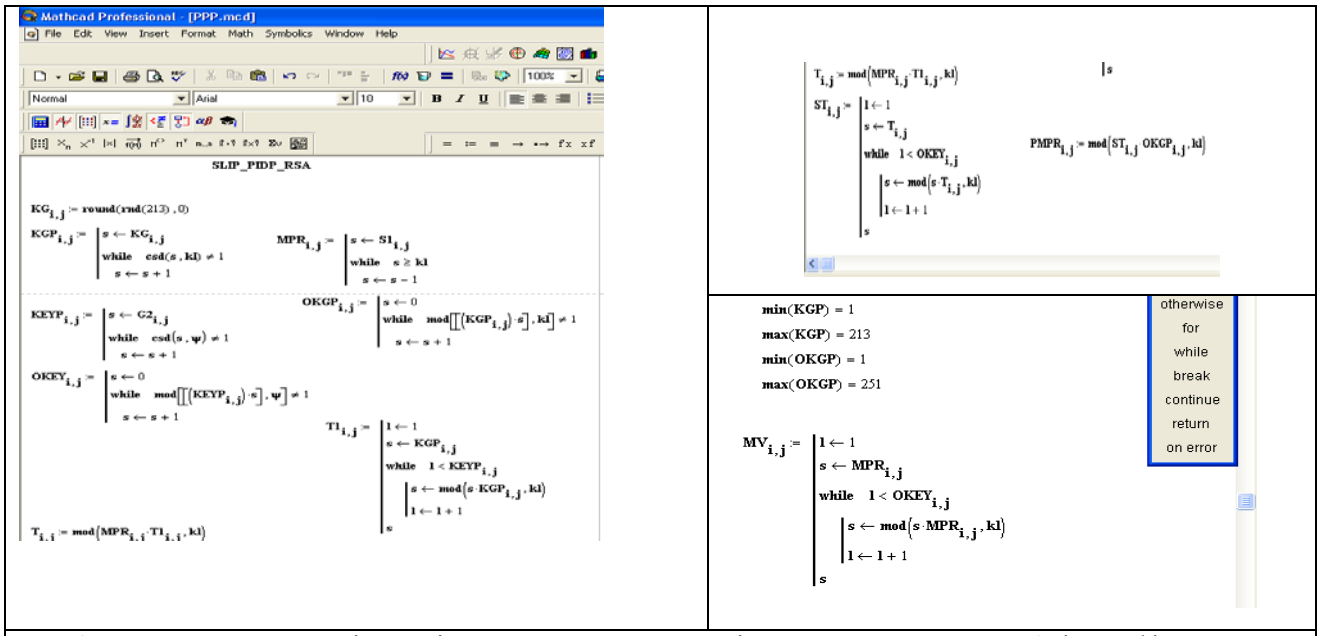


Рис.1. Формули та програмні модулі для моделювання процесів створення ЕЦП МТ на базі модифікованого на матричний випадок RSA-алгоритму

$$T1 = KGP^{[\wedge]KEYP} \bmod kl, \quad (1)$$

де $[\wedge]$ - операція по елементного піднесення в степінь за відповідним модулем.

За допомогою цієї матриці T1первинне відкориговане повідомлення – зображення MPR закривається, а закрите повідомлення у вигляді матриці T відсилається для підписування нотаріусу чи у відповідний державний орган, наприклад, у податкову службу. Матриця T формується наступним чином:

$$T = MPR \underset{kl}{\Theta} T1, \quad (2)$$

де $\left(\underset{kl}{\Theta}\right)$ - операція по елементного множення матриць за відповідним модулем kl або матрицею відповідних модулів $n_{ij}$, коли використовується не один і той же модуль kl для всіх елементів, а різні для різних елементів. Отримане відповідним органом повідомлення T підписується ним шляхом такого ж поелементного матричного піднесення за модулем у відповідну степінь, що визначається ключем OKEY. Створений таким шляхом підписаний документ у вигляді матриці ST відсилається абоненту:

$$ST = T^{[\wedge]OKEY} \bmod kl. \quad (3)$$

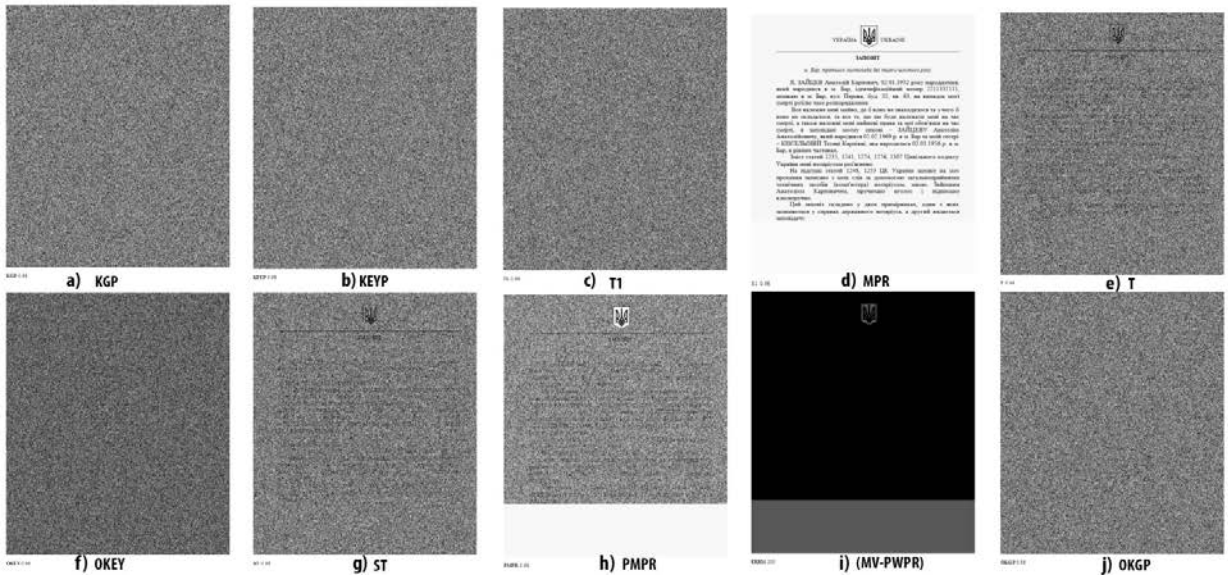


Рис. 2. Матриці-зображення, що формувалися в модельних експериментах та підтверджують правильну роботу процесів створення сліпих ЕЦП МТ: a) ключ для закриття MPR; b) ключ для поелементного матричного піднесення в степінь за відповідним модулем ключа KGP; c) допоміжна матриця T1; d) скоригований документ, який необхідно зашифрувати чи підписати; e) закрите повідомлення, що відсилається нотаріусу; f) обернений до KEYP ключ; g) шифрограма підписаного документа; h) підписаний документ (підпис); i) зображення різниці між MV та PMPR; j) обернений до KGP ключ

Ключ OKEY є закритим, таємним і взаємно відповідним матричному ключу KEYP. Сторона, що підписує, не бачить текст документу, бо бачить лише його закриту копію T, а ключ OKGP він не знає. Без знання останнього він не може побачити повідомлення MPR (MV). Отриманий підписаний документ (матриця ST), абонент поелементно за відповідною матрицею модулів перемножує на матрицю OKGP та отримує підписаний документ PMPR, який є по суті OKEY-степінню документу MPR (MV) за відповідним модулем:

$$PMPR = ST \underset{kl}{\Theta} OKGP, \quad (4)$$

$$MV = MPR^{[\wedge]OKEY} \bmod kl. \quad (5)$$

На рисунку 2 показані всі вищеописані матриці для випадку, що використовувався в експерименті і відповідав таким вибраним значенням: k = 11, l = 23, kl = k · l, kl = 253, при яких функція Ейлера дорівнювала:

$$\Psi = (k - 1) \cdot (l - 1) = (11 - 1) \cdot (23 - 1) = 220.$$

Ці матриці підтверджують правильну роботу запропонованого алгоритму створення сліпого ЕЦП МТ. Результати моделювання показують, що за допомогою таких сліпих ЕЦП МТ легко та криптостійко виконуються криптографічні перетворення ТГД формату А4 та близького до нього чи значно більших за час, що не перевищує однієї-двох хвилин.

Запропонований алгоритм створення сліпого ЕЦП МТ дозволяє зробити верифікацію підпису лише при спільних діях обох сторін що створювали підпис. Крім того, запропонований алгоритм може бути покращений за рахунок подвійного, так званого нами двостороннього, закриття ТГД та реквізитів нотаріуса,

що полягає не лише в закритті повідомлення ТГД що відсилається нотаріусу, але і у аналогічному закритті реквізитів (особистих ідентифікаторів) нотаріуса при створенні таких підписів. Це ще більше підсилює надійність таких двосторонніх процедур формування сліпих ЕЦП МТ.

Спроба аналогічним чином модифікувати ЕЦП Ель-Гамаля до МТ та створені матричні моделі перевірити шляхом їх моделювання для конкретних ТГД також є актуальною. Це дозволить оцінити показники таких ЕЦП МТ Ель-Гамаля та їх особливості і сфери застосувань.

Тому другим експериментом є моделювання ЕЦП МТ Ель-Гамаля для ТГД у програмному середовищі Mathcad та оцінювання такої моделі. Розглянемо сутність математичної моделі. Вона полягає в тому, що вибирають просте число p, в нас p=257, та число b (твірну в Zp), в нас b=113. Формують матрицю BE=b*R, в якій всі елементи рівні b, а користувач A вибирає число *a* менше p-1, та обчислює число hs (*a*-ту степінь b за модулем p) і виставляє b, hs, p, як публічний ключ.

Генерування ЕЦП для документа Z, попередньо скоригованого, виконується так: 1) вибирається випадкова матриця U та коригується як і Z, так щоб всі її елементи були взаємно простими з p-1; 2) обчислюється матриця BEM, що є поелементним матричним піднесенням матриці BE у степінь-матрицю U за модулем p; 3) обчислюється матриця OU, елементи якої є оберненими за модулем p-1 до елементів матриці U; 4) обчислюється матриця BEMM, яка є функцією F від Z, BEM, OU та *a* за p-1 модулем, дивись формули на рис.1; 5) подає дві матриці BEM, BEMM як підпис МТ Ель-Гамаля для ТГД у вигляді матриці Z. Особа B для верифікації підпису виконує порівняння за модулем p, обчислюючи матриці HS1, HS2 та їх поелементний добуток-матрицю VER, а на підставі теореми Ферма остання і є Z- степінню за модулем p матриці BE, тобто матрицею BEMV. Формули для моделювання показані на рис. 3.

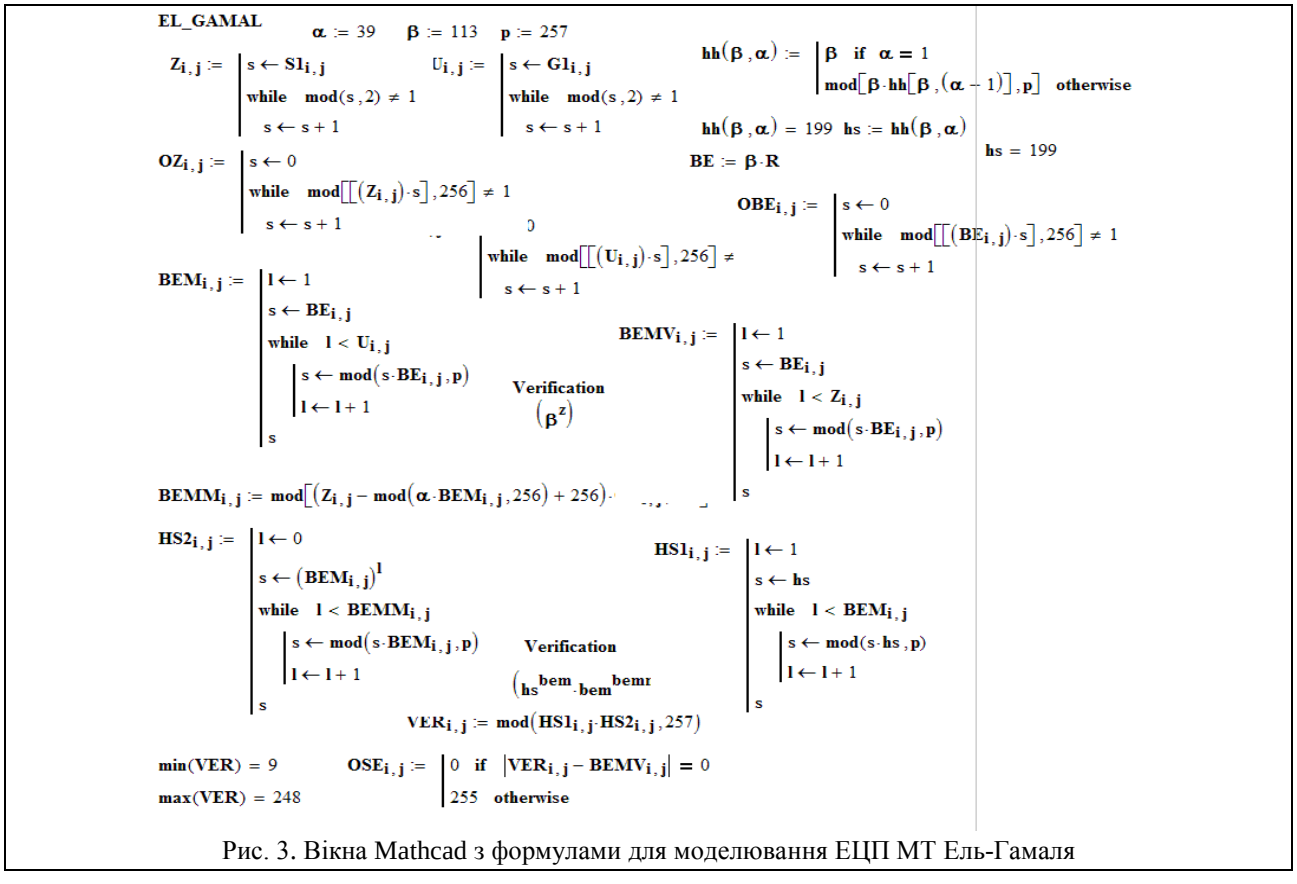


Рис. 3. Вікна Mathcad з формулами для моделювання ЕЦП МТ Ель-Гамаля

Результати моделювання процесів створення ЕЦП МТ Ель-Гамаля показані на рис. 4. Тут показані для демонстрації масиви невеликої розмірності, з урахуванням обмежень на обсяг сторінок. Але у доповіді будуть наводитись експерименти стосовно роботи даної моделі з ТГД значної розмірності.

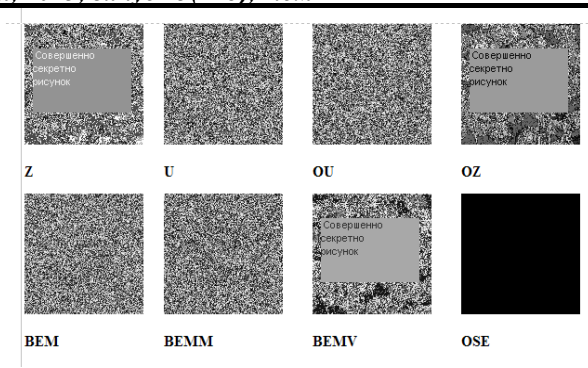


Рис.4. Результати моделювання ЕЦП МТ Ель-Гамаля

**Висновки**. Виконана демонстрація функціональних можливостей та переваг процедур та алгоритмів створення сліпих ЕЦП МТ на текстографічні документи конфіденційного характеру. Наведені результати моделювання процесів створення таких підписів для великоформатних документів у програмному середовищі Mathcad, що підтвердили правильність їх функціонування та верифікації і визначили час та обмеження відповідних криптоперетворень.

## Список літератури

1. *Ємець В. Сучасна криптографія. Основні поняття / В. Ємець, А. Мельник, Р. Попович. – Львів: БаК, 2003. – 144 с.*

2. *Красиленко В.Г. Моделювання матричних алгоритмів криптографічного захисту / В.Г. Красиленко, Ю.А. Флавицька // Вісник НУ «Львівська політехніка». «Компьютерні системи та мережі». – 2009. – №658. – С.59-63.*

3. *Красиленко В.Г. Моделювання матричних афінних алгоритмів для шифрування кольорових зображень / В.Г. Красиленко, К.В. Огородник, Ю.А. Флавицька // Комп'ютерні технології: Наука і освіта: Тези доповідей V Всеукр. наук. – пр. конф. – К. 2010. – С.120-124.*

4. *Красиленко В. Г. Матричні афінно-перестановочні алгоритми для шифрування і дешифрування зображень [Текст] / В.Г. Красиленко, С. К. Грабовляк // Системи обробки інформації . – 2012 . – №3(101). – С.53-61.*

5. *Красиленко В. Г. Модифікації системи RSA для створення на її основі матричних моделей та алгоритмів для зашифрування та розшифрування зображень [Текст] / В.Г. Красиленко, С. К. Грабовляк // Системи обробки інформації. – 2012 . – №8(106). – С.102-106.*

6. *Красиленко В.Г., Матричні афінні шифри для створення цифрових сліпих підписів на текстографічні документи / В.Г. Красиленко, С.К. Грабовляк // Системи обробки інформації. – Х.: ХУПС, 2011. – Вип. 7(97**). –** С.60 – 63.*

7. *Красиленко В. Г. Алгоритми формування двовимірних ключів для матричних алгоритмів криптографічних перетворень зображень та їх моделювання [Текст] / В.Г. Красиленко, В. І. Яцковський, Р. О. Яцковська // Системи обробки інформації. – 2012 . – №8(106). – С.107-110.*

8. *Красиленко В.Г. Моделювання сліпих електронних цифрових підписів матричного типу на конфіденційну текстографічну документацію / В.Г. Красиленко, Р. О. Яцковська, С. К. Грабовляк, // І Міжнародна науково-методична конференція Вінниця: ВНАУ, 2012. – С.103-107.*

*Надійшла до редколегії 4.03.2013*

**Рецензент:** доктор технічних наук, професор В.М. Лисогор, Вінницький національний аграрний університет, Вінниця

**ДЕМОНСТРАЦІЯ ПРОЦЕСІВ СТВОРЕННЯ СЛІПИХ ЕЛЕКТРОННИХ ЦИФРОВИХ ПІДПИСІВ НА ТЕКСТОГРАФІЧНУ ДОКУМЕНТАЦІЮ НА ОСНОВІ МОДЕЛЕЙ МАТРИЧНОГО ТИПУ**

В.Г. Красиленко, Р.А. Яцковская, Ю.М. Трифонова

*В статье рассматриваются результаты моделирования слепых электронных цифровых подписей на конфиденциальную текстографическую документацию на основе моделей матричного типа и демонстрируются конкретные примеры создания таких подписей в программной среде Mathcad Professional. Показано, что на основе таких моделей при создании подписей для текстографических документов формата А4 и полутоновых изображений значительной размерности не превышает нескольких минут.*

***Ключевые слова**: слепая электронная цифровая подпись, матричная модель RSA, криптографическая система, протокол формирования ключей, верификация электронных подписей.*

**DEMONSTRATION PROCESSES CREATE BLIND DIGITAL SIGNATURE TG DOCUMENTATION BASED ON THE MODELS OF MATRIX TYPE.**

V.G Krasilenko, R.A Yatskovska, Y.M. Trifonova

*The article deals with the results of modelling the blind digital signatures to confidential TG documentation based on the models of the matrix type and demonstrate specific examples of such signatures in the software environment Mathcad Professional. It is shown that on the basis of such models to create signatures for TG A4 documents and greyscale images large dimension does not exceed a few minutes.*

***Keywords**: blind digital signature, matrix model RSA, cryptographic system, making key protocol, and verifying electronic signatures*

 