УДК 004.056.55

МАТЕМАТИЧНА МОДЕЛЬ ПРОТОКОЛУ АНОНІМНОГО ЕЛЕКТРОННОГО ПІДПИСУ НА ОСНОВІ ІДЕНТИФІКАЦІЙНИХ ДАНИХ

М.В. ЄСІНА

У роботі розглядається математична модель протоколу анонімного електронного підпису на основі алгоритмів ДСТУ ISO/IEC 14888-3:2014 IBS-1 та IBS-2. Розглядається можливість застосування механізмів електронного підпису на основі ідентифікаційних даних у протоколі анонімного підпису.

Ключові слова: анонімний підпис, електронний підпис, ідентифікаційні дані.

ВСТУП

З метою надання у різноманітних інформаційних технологіях електронних довірчих послуг на міжнародному, регіональних та національних рівнях застосовуються значне число стандартизованих механізмів електронних підписів (ЕП). При цьому у розробників та користувачів додатків електронних довірчих послуг є можливість вибору ЕП із значного числа існуючих міжнародних та національних стандартів, наприклад, ДСТУ ISO/IEC 14888-3:2014 [1,9]. У ряді додатків електронних довірчих послуг обов'язковою є вимога надання електронної послуги анонімності (невідстежуваності), наприклад, у системах таємного електронного голосування, електронних грошей тощо. Визнаним механізмом надання послуги анонімності є застосування механізму анонімного підпису. Анонімним (сліпим) називається підпис, який накладається третьою стороною на попередньо замасковане повідомлення [3 – 4,8,11 – 12].

Зважаючи на актуальність, на даний момент комітетом ISO/IEC JTC 1/SC 27 (одним з учасників якого є Україна) розробляється пакет стандартів стосовно електронних довірчих послуг. Анонімний підпис є однією з таких послуг і стосовно нього розробляється міжнаціональний стандарт ISO/IEC DIS 18370-2 [2], що регламентуватиме види анонімного підпису, їх використання та стандартизуватиме конкретні механізми і протоколи анонімного підпису.

Сьогодні широке розповсюдження отримують ЕП, стійкість яких ґрунтується на складності дискретного логарифмування в скінченних полях та групах точок еліптичних кривих (ЕК). Також пройшли дослідження та рекомендуються до застосування ЕП з додатком, що ґрунтуються на ідентичності – спарюванні точок ЕК [1,5 – 7,9 – 10].

На сьогоднішній день вже існують деякі механізми анонімних підписів. Всі вони ґрунтуються на еліптичних кривих. Але сьогодні також існують механізми ЕП, що базуються на ідентифікаційних даних, і вони рекомендуються до застосування. Тому важливою є задача розробки та детального дослідження даного виду механізмів ЕП з точки зору можливості застосування у механізмі анонімного підпису [3 – 12].

Метою цієї статі є визначення можливостей та умов реалізації, а також обґрунтування використання у протоколі анонімного підпису алгоритмів ЕП згідно з ДСТУ ISO/IEC 14888-3:2014, що базуються на ідентифікаційних даних.

1. СУТНІСТЬ ЕЛЕКТРОННИХ ПІДПИСІВ IBS-1 ТА IBS-2, ЩО ВИЗНАЧЕНІ ТА РЕАЛІЗОВАНІ В ДСТУ ISO/IEC 14888-3:2014

Розглянемо спочатку сутність механізмів ЕП IBS-1 та IBS-2 та етапи налаштування. Для застосування ЕП IBS-1 та IBS-2 спочатку мають бути введеними та налаштовані загальні параметри та згенеровані асиметричні пари ключів.

Загальними параметрами ЕП IBS-1 та IBS-2 є [1,7,10]:

- U – секретний майстер-ключ – ціле число, $U \in [1, q-1]$;
- V – відкритий майстер-ключ – точка ЕК, $V = [U]P \bmod q$, $V \in G_1$;
- X – особистий (секретний) ключ підписувача – точка ЕК, $X = [U]Y \bmod q$, $X \in G_1$;
- Y – відкритий ключ (перевіряння) підписувача – точка ЕК, $Y = H_1(ID) \bmod q$, $Y \in G_1$;
- P – базова точка центру сертифікації ключів порядку q.

Генерація чи обчислення загальних параметрів мають здійснюватися з дотриманням таких умов:

- особистий ключ користувача X обчислюється за його запитом у центрі генерації ключів (ЦГК) та надається користувачеві по захищеному каналу;
- відкритий ключ користувача Y може обчислити кожен користувач домену;
- ID – є рядок даних, що містить ідентифікатор підписувача;
- H_1 – функція гешування, яка перетворює рядок даних у елемент групи G_1;
- H_2 – функція гешування, що визначена у ДСТУ ISO/IEC 10118-3:2005;
- G_1 – циклічна група простого порядку q, елементами якої є точки на ЕК над $GF(p)$;

- G_2 – циклічна група простого порядку q,
- елементами якої є елементи скінченого поля $GF(p^m)$.

В таблицях 1 та 2 наведені механізми IBS-1 та IBS-2 підписування та перевірки [1,7,10].

Таблиця 1

Механізм ЕП IBS-1

Підпис повідомлення	Перевірка підпису
1. Генерування випадкового чи псевдовипадкового одноразового таємного ключа – цілого числа K, $1 < K < (q-1)$.	1. Перевірник отримує цілісні загальні параметри та відкритий ключ підписувача.
2. Здійснення спарювання: $\Pi =< X, P >^K$, $\Pi \in G_2$ над полем $GF(p^m)$, Π – передпідпис	2. Відновлення одноразового відкритого ключа: – R та S відновлюються з доповнення; – бітова довжина R має дорівнювати довжині виходу функції H_2; – $S \in G_1$. Якщо хоча б одна з цих умов не виконується, підпис відхиляється.
3. Повідомлення у вигляді цілого M розбивається на його частини: M_2 – порожня частина, $M_1 = M$ – повідомлення, що треба підписати.	3. Підготування повідомлення до перевірки: – відновлення M з підписаного повідомлення; – розбиття повідомлення на M_1 та M_2: M_2 – порожнє, $M_1 = M$.
4. Обчислення одноразового відкритого ключа: $R = H_2(M_1 \,\|\, FE2BS(\Pi))$, $R \in G_2$.	4. Відновлення призначення: $T = (T_1, T_2)$, $T_1 = -Y$, $T_2 = [R]Y$.
5. Обчислення призначення: $T = (T_1, T_2) = (-Y, [R]Y)$.	5. Здійснення спарювання: $\overline{\Pi} =< S, P > \times < Y, V >^R$.
6. Обчислення компоненти підпису: $S = [K - R]X \bmod q$, $S \in G_1$. Підписом є $\Sigma = (R, S)$.	6. Обчислення одноразового відкритого ключа перевірки: $\overline{R} = H_2(M_1 \,\|\, FE2BS(\overline{\Pi}))$.
7. Побудова доповнення з конкатенуванням тексту у вигляді $(R, S) \,\|\, text$.	7. Порівняння $\overline{R} = R$: якщо не співпадають, то підпис хибний, інакше – істинний.
8. Побудова підписаного повідомлення у вигляді $M((R, S) \,\|\, text)$.	

Таблиця 2

Механізм ЕП IBS-2

Підпис повідомлення	Перевірка підпису
1. Генерування випадкового чи псевдовипадкового одноразового таємного ключа – цілого числа K, $1 < K < (q-1)$.	1. Перевірник отримує цілісні чинні загальні параметри та чинний відкритий ключ підписувача.
2. Здійснення скалярного множення: $\Pi = [K]Y \bmod q$, $\Pi \in G_1$, Π – передпідпис, точка ЕК.	2. Відновлення одноразового відкритого ключа: – R та S відновлюються з доповнення; – $R \in G_1$, $S \in G_1$. Якщо хоча б одна з цих умов не виконується, підпис відхиляється.

Продовження таблиці 2

3. Повідомлення у вигляді цілого M розбивається на його частини: M_1 – порожня частина, $M_2 = M$ – повідомлення, що треба підписати.	3. Підготування повідомлення до перевірки: – відновлення M з підписаного повідомлення; – розбиття повідомлення на M_1 та M_2: M_1 – порожнє, $M_2 = M$.
4. Обчислення одноразового відкритого ключа: $R = \Pi$, $R \in G_1$.	4. Відновлення призначення: $T = (T_1, T_2)$, $T_1 = -Y$, $T_2 = [-H]Y$, $H = H_2(M_2 \,\|\|\, FE2BS(R_x))$.
5. Обчислення призначення: $T = (T_1, T_2) = (-Y, [-H]Y)$, $H \in G_2$, $H = H_2(M_2 \,\|\|\, FE2BS(\Pi_x))$.	5. Обчислення передпідпису: $\overline{\Pi} = R$, $\overline{\Pi} \in G_1$.
6. Обчислення компоненти підпису: $S = [K + H]X \bmod q$, $S \in G_1$. Підписом є $\Sigma = (R, S)$.	6. Обчислення: $\overline{R}_1 =< P, S >$ та $\overline{R}_2 =< V, \overline{\Pi} + [H]Y >$.
7. Побудова доповнення: $(R, S) \,\|\|\, text$.	7. Порівняння $\overline{R}_1 = \overline{R}_2$: якщо не співпадають, то підпис хибний, інакше – вірний.
8. Побудова підписаного повідомлення: $M((R, S) \,\|\|\, text)$.	

2. ЗАГАЛЬНИЙ ОПИС МЕХАНІЗМУ АНОНІМНОГО ЕЛЕКТРОННОГО ПІДПИСУ НА ЕЛІПТИЧНИХ КРИВИХ

Нехай у механізмі (схемі) анонімного (сліпого) ЕП на еліптичних кривих (ЕК) взаємодіють три сторони [3 – 4,8,10 – 12]: А – підписувач, В – абонент (емітент документу/повідомлення m), С – валідатор. При цьому валідатором може виступати будь-хто з них, або довірена третя особа. Емітент створює документ m, який підписувач має підписати анонімно, тобто не мати доступу до його семантичного змісту – на практиці – до реального геш-значення. Для цього емітент, отримавши згоду підписувача, маскує документ, а реально – геш-значення, за допомогою певного криптографічного перетворення та пересилає його підписувачу.

Після підпису замаскованого документу, підписувач надсилає його емітенту. Емітент здійснює зворотне, відносно маскування, перетворення та знімає його, залишивши ЕП неушкодженим. Перевірник, після отримання підписаного документу, перевіряє його цілісність, справжність та встановлює авторство за допомогою відкритого ключа підписувача.

Для забезпечення безпечності механізму, попередньо мають бути згенеровані та захищеним шляхом розповсюджені певні загальні параметри аналізу криптографічних перетворень на еліптичних кривих. Перелік перетворень та вимоги до них визначені у відповідних стандартах [1]. Також мають бути згенеровані асиметричні пари ключів для підписувачів А, а перевірник С повинен мати доступ до відкритих ключів (сертифікатів) підписувачів. Емітент повинен мати загальні параметри та ключі замаскування і розмаскування.

3. ПЕРЕВІРКА ЗАХИЩЕНОСТІ МЕХАНІЗМУ ЗА КРИТЕРІЄМ АНОНІМНОСТІ

Для схем анонімного підпису, на відміну від інших різновидів ЕП, актуальною є атака порушення анонімності. Якщо вважати, що ЕП, який застосовується, є стійким проти усіх відомих та потенційних атак, то для доведення безпечності механізму анонімного підпису необхідно довести ще його стійкість до атаки порушення анонімності.

Сутність атаки на анонімність полягає в тому, що вона може бути здійснена підписувачем за умови, що він матиме для кожної сесії постановки підпису всі відомі йому параметри схеми анонімного підпису разом із ідентифікатором емітента. Накопичена таким чином база даних (БД) може бути використана в атаці, яка полягає у спробі визначення автора певного документа m із підписом $< r, s >$, який пройде перевірку за допомогою відкритого ключа підписувача Q.

Більш детально реалізація атаки порушення анонімності описана у [3].

4. ПРОТОКОЛ АНОНІМНОГО ЕЛЕКТРОННОГО ПІДПИСУ НА ОСНОВІ ІДЕНТИФІКАЦІЙНИХ ДАНИХ

Спочатку визначимо основні сторони протоколу, що взаємодіють [3 – 4,7 – 8,10 – 12]:

А – підписувач (у ролі підписувача виступає ЦГК);

В – емітент документу m;

С – перевірник (валідатор).

Ключову пару (U, V) та ключову пару (X, Y) обчислює ЦГК;

4.1 Протокол анонімного підпису на основі IBS-1

Генерація ключів: ЦГК у ролі підписувача А створює пару ключів (X,Y):

$$X=[U]Y \bmod q,\ Y=H_1(ID) \bmod q.$$

Постановка засліпленого підпису [3]:

Абонент А:

– вибирає одноразовий таємний ключ K: $1<K<(q-1)$;

– обчислює передпідпис Π: $\Pi=<X,P>^K$, $\Pi\in G_2$ над полем $GF(p^m)$;

– відправляє точку P емітенту В;

– передає обчислений передпідпис Π абоненту В.

Абонент В:

– розбиває повідомлення M на дві частини: M_2 – порожня частина, $M_1=M$ – повідомлення, що треба підписати;

– обирає параметр маскування α: $1<\alpha<(q-1)$;

– обчислення одноразового відкритого ключа R (також можна вважати і одночасним його засліпленням): $R=H_2(M_1\,||\,FE2BS(\Pi))$, $R\in G_2$ і передача його абоненту А.

Абонент А:

– формування засліпленого підпису S': $S'=[K-R]X \bmod q$, $S'\in G_1$. Підписом є $\Sigma=(R,S')$;

– передає засліплений підпис S' на перевірку абоненту В.

Перевірка засліпленого підпису [3]:

Емітент В перевіряє справжність засліпленого підпису S' за допомогою звичайної перевірки електронного підпису IBS-1:

$$\Pi=<X,P>^K;\ \overline{\Pi}'=<S',P>\times<Y,V>^R;$$

$\overline{R}=R$, якщо $\overline{\Pi}'=\Pi$, тоді:

$$\begin{aligned}\overline{\Pi}'&=e(S',P)\times e(Y,V)^R=e([K-R]X,P)\times\\&\times e(Y,[U]P)^R=e([K-R][U]Y,P)\times\\&\times e([U]Y,RP)=e(X,[K-R]P)\times\\&\times e(X,RP)=e(X,KP-RP+RP)=\\&=e(X,KP)=e(X,P)^K=\Pi\end{aligned}.$$

Таким чином, засліплений підпис проходить стандартну перевірку.

Постановка фінального підпису [3]:

Якщо S' проходить перевірку, то абонент В формує з нього фінальний анонімний підпис повідомлення M у вигляді (R,S), попередньо перетворивши S' у S:

$$S=\alpha S' \bmod q,$$

$\Sigma=(R,S)$ – фінальний анонімний підпис.

Перевірка фінального підпису [3]:

$$\Pi=<X,P>^{\alpha K};\ \overline{\Pi}=<S,P>\times<Y,V>^{\alpha R};$$

$\overline{R}=R$, якщо $\overline{\Pi}=\Pi$, тоді:

$$\begin{aligned}\overline{\Pi}&=e(S,P)\times e(Y,V)^{\alpha R}=e(\alpha S',P)\times e(\alpha Y,[U]P)^R=\\&=e(\alpha[K-R]X,P)\times e(\alpha[U]Y,RP)=\\&=e(\alpha[K-R]X,P)\times e(\alpha X,RP)=\\&=e(\alpha X,KP-RP+RP)=e(\alpha X,KP)=\\&=e(X,P)^{\alpha K}=\Pi\end{aligned}$$

Фінальний анонімний підпис проходить стандартну перевірку.

Перевірка за критерієм анонімності [3]:

$$\alpha'=\frac{S}{S'} \bmod q;\ \Pi=<X,P>^{\alpha K};\ \widetilde{\Pi}=<X,P>^{\alpha' K}$$

якщо $\widetilde{\Pi}=\Pi$, тоді підпис є стійким за критерієм анонімності:

$$\begin{aligned}\widetilde{\Pi}&=e(\alpha' X,KP)=e(\frac{S}{S'}X,KP)=\\&=e(\frac{\alpha S'}{S'}X,KP)=e(\alpha X,P)^K=\Pi\end{aligned}.$$

Отже, анонімний електронний підпис на основі IBS-1 є стійким за критерієм анонімності.

4.2 Протокол анонімного підпису на основі IBS-2

Генерація ключів: ЦГК у ролі підписувача А створює пару ключів (X,Y):

$$X=[U]Y \bmod q,\ Y=H_1(ID) \bmod q.$$

Постановка засліпленого підпису [3]:

Абонент А:

– вибирає одноразовий таємний ключ K: $1<K<(q-1)$;

– обчислює передпідпис Π: $\Pi=[K]Y \bmod q$, $\Pi\in G_1$;

– відправляє точку P емітенту В;

– передає обчислений передпідпис Π абоненту В.

Абонент В:

– розбиває повідомлення M на дві частини: M_1 – порожня частина, $M_2=M$ – повідомлення, що треба підписати;

– обирає параметр маскування α: $1<\alpha<(q-1)$;

– обчислення одноразового відкритого ключа R: $R=\Pi$, $R\in G_2$;

– обчислює геш-значення H повідомлення: $H=H_2(M_2\,||\,FE2BS(\Pi_x))$, $H\in G_2$ (і таким чином засліплює його);

– передає геш-значення H підписувачу А.

Абонент А:

– формування засліпленого підпису S': $S' = [K + H]X \bmod q$, $S' \in G_1$. Підписом є $\Sigma = (R, S')$;

– передає засліплений підпис S' на перевірку абоненту В.

Перевірка засліпленого підпису [3]:

Емітент В перевіряє справжність засліпленого підпису S' за допомогою звичайної перевірки електронного підпису IBS-2:

$$\overline{\Pi}' = R;\ \overline{R}_1 =< P, S' >,\ \overline{R}_2 =< V, \overline{\Pi}' + [H]Y >,$$

тоді:

$$\overline{R}_2 = e([U]P, [K]Y + [H]Y) = e(P, [K + H][U]Y) = \\ = e(P, [K + H]X) = e(P, S') = \overline{R_1}.$$

Таким чином, засліплений підпис проходить стандартну перевірку.

Постановка фінального підпису [3]:

Якщо S' проходить перевірку, то абонент В формує з нього фінальний анонімний підпис повідомлення M у вигляді (R, S), попередньо перетворивши S' у S:

$$S = \alpha S' \bmod q,$$

$\Sigma = (R, S)$ – фінальний анонімний підпис.

Перевірка фінального підпису [3]:

$$\overline{\Pi} = R;\ \overline{R}_1 =< P, S >,\ \overline{R}_2 =< V, \overline{\Pi} + [H]Y >^{\alpha},$$

тоді:

$$\overline{R}_2 = e(V, \overline{\Pi} + [H]Y)^{\alpha} = e([U]P, \alpha([K]Y + [H]Y)) = \\ = e(P, \alpha[K + H][U]Y) = e(P, \alpha[K + H]X) = \\ = e(P, \alpha S') = e(P, S) = \overline{R_1}.$$

Фінальний анонімний підпис проходить стандартну перевірку.

Перевірка за критерієм анонімності [3]:

$$\alpha' = \frac{S}{S'} \bmod q;\ \overline{R}_1 =< P, S >;\ \widetilde{R} =< V, \overline{\Pi} + [H]Y >^{\alpha'},$$

якщо $\widetilde{R} = \overline{R_1}$, тоді підпис є стійким за критерієм анонімності:

$$\widetilde{R} = e(V, \alpha'(\overline{\Pi} + [H]Y)) = e([U]P, \frac{S}{S'}([K]Y + [H]Y)) = \\ = e(P, \frac{S}{S'}[K + H][U]Y) = e(P, \frac{S}{S'}[K + H]X) = \\ = e(P, \frac{S}{S'}S') = e(P, S) = \overline{R_1}$$

Отже, анонімний електронний підпис на основі IBS-2 є стійким за критерієм анонімності.

ВИСНОВКИ

1. Механізм анонімного підпису забезпечує підтвердження справжності документів без розкриття їхнього авторства і може бути реалізований з використанням стандартних ЕП, що ґрунтуються на спарюванні точок еліптичної кривої.

2. До критеріїв перевірки захищеності механізму анонімного (сліпого) підпису додається критерій анонімності. При його застосуванні доводиться неможливість визначити підписувачу автора документа, якщо він використовуватиме всі відомі йому параметри, які використовувались при постановці підпису.

3. Визначено та обґрунтовано можливості використання механізмів ЕП, що базуються на ідентифікаційних даних, у протоколі анонімного підпису. Доведено, що в ході використання даних механізмів ЕП, анонімний (сліпий) підпис є стійким за критерієм анонімності, тобто неможливо визначити автора документу, що підписується.

Література

[1] Information technology – Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms : ISO/IEC 14888-3 (Edition 2) : 2014. – 130 p.

[2] Information technology – Security techniques – Blind digital signatures – Part 2: Discrete logarithm based mechanisms : ISO/IEC DIS 18370-2:2014(E):2015. – 70 p.

[3] *Gorbenko I.* Blind electronic signature mechanisms on elliptic curves improvement / I. Gorbenko, M. Yesina, V. Ponomar // COMPUTER SCIENCE AND CYBERSECURITY. – Харківський національний університет імені В.Н. Каразіна, Випуск 1(1), 2016. Електронний ресурс. Режим доступу: http://periodicals.karazin.ua/cscs/article/view/6205/5744

[4] *Gorbenko I.* Anonymous electronic signature method / I. Gorbenko, M. Yesina, V. Ponomar // Problems of Infocommunications Science and Technology (PIC S&T 2016), October 4–6, 2016, Kharkov National University of Radio Electronics, Kharkiv, Ukraine.

[5] *Акользіна О. С.* Сутність та порівняльний аналіз криптографічної стійкості електронного підпису на ідентифікаційних даних / О. С. Акользіна, І. Д. Горбенко // Компьютерное моделирование в наукоемких технологиях (КМНТ-2016) : Труды научно-технической конференции с международным участием, 26-31 мая 2016 г. – Х. : Харьковский национальный университет им. В. Н. Каразина, 2016. – С. 89–92.

[6] *Горбенко Ю. І.* Електронні підписи на основі ідентифікаторів та бінарного відображення / Ю. І. Горбенко, Р. С. Ганзя, О. С. Акользіна // Прикладная радиоэлектроника. – Х. : Харьковский национальный университет радиоэлектроники, 2015. – Т. 14, № 4 – С. 284–290.

[7] *Горбенко Ю.І.* Сутність та умови здійснення атаки на зв'язаних ключах відносно електронних підписів IBS-1 та IBS-2 ДСТУ ISO/IEC 14888-3 / Ю.І. Горбенко, М.В. Єсіна, В.А. Кулібаба // Системи обробки інформації. – Х. : Харківський університет Повітряних Сил, 2016. – № 7(144) – С.113–118.

[8] *Єсіна М. В.* Математична модель протоколу сліпого електронного підпису на еліптичних кривих / М. В. Єсіна // Прикладная радиоэлектроника. – Х. : Харьковский национальный университет радиоэлектроники, 2015. – Т. 14, № 4 – С.300–305.

[9] *Єсіна М. В.* Порівняльний аналіз та умови застосування електронних підписів з додатком ДСТУ ISO/IEC 14888 / М. В. Єсіна // Компьютерное моделирование в наукоемких технологиях (КМНТ-2016) : Труды научно-технической конференции с международным участием, 26-31 мая 2016 г. – Х. : Харьковский национальный университет им. В.Н. Каразина, 2016. – С. 141–144.

[10] *Єсіна М. В.* Реалізація атаки на зв'язаних ключах відносно електронних підписів IBS-1 та IBS-2 ДСТУ

ISO/IEC 14888-3/ М. В. Єсіна // V Міжнародна науково-технічна конференція “Захист інформації і безпека інформаційних систем” : Праці Науково-технічної конференції, 02–03 червня 2016 р. – Л. : Національний університет “Львівська політехніка”, 2016. – С. 100 – 101.

[11] *Пономар В. А.* Удосконалення механізмів сліпого електронного підпису на еліптичних кривих / В.А. Пономар, М. В. Єсіна // Науково-практична конферен-ція “Проблеми кібербезпеки інформаційно-телекомунікаційних систем”: Праці Науково-практичної конференції, 10-11 березня 2016 р. – К. : Київський національний університет імені Тараса Шевченка, 2016. – С. 67 – 68.

[12] *Пономар В. А.* Механізми та умови реалізації анонімних електронних підписів на основі стандартних та перспективних алгоритмів / В. А. Пономар, М. В. Єсіна // Безпека інформації в інформаційно-телекомунікаційних системах : Матеріали міжнародної науково-практичної конференції, Випуск 18, 25-26 травня 2016 р. – К. : Державна служба спеціального зв’язку та захисту інформації України, 2016 – С. 24.

Єсіна Марина Віталіївна, аспірантка факультету комп’ютерних наук, кафедри безпеки інформаційних систем і технологій Харківського національного університету імені В.Н. Каразіна. Наукові інтереси: електронний підпис, анонімний підпис, протоколи анонімного електронного підпису, криптографічний захист інформації.

УДК 004.056.55

Математическая модель протокола анонимной электронной подписи на основе идентификационных данных / М.В. Есина // Прикладная радиоэлектроника: науч.-техн. журнал. – 2016. – Том 15, № 3. – С. – 151 – 156.

В работе рассматривается математическая модель протокола анонимной электронной подписи на основе алгоритмов ДСТУ ISO/IEC 14888-3:2014 IBS-1 и IBS-2. Рассматривается возможность применения механизмов электронной подписи на основе идентификационных данных в протоколе анонимной подписи.

Ключевые слова: анонимная подпись, электронная подпись, идентификационные данные.

Табл.: 02. Библиогр.: 12 назв.

UDC 004.056.55

Mathematical model of an anonymous electronic signature protocol based on identity / M.V. Yesina // Applied Radio Electronics: Sci. Joum. – 2016. – Vol. 15, № 3.– P. 151 – 156.

The paper deals with a mathematical model of an anonymous electronic signature protocol based on the algorithms DSTU ISO/IEC 14888-3:2014 IBS-1 and IBS-2. A possibility of using electronic signature mechanisms based on the identity in the anonymous signature protocol is considered.

Keywords: anonymous signature, electronic signature, identity.

Tab.: 02. Ref.: 12 items.