УДК 004.056.55

М.В. ЄСІНА, Н.В. КОВАЛЬОВА, І.Д. ГОРБЕНКО, д-р техн. наук

ПОРІВНЯЛЬНИЙ АНАЛІЗ ВЛАСТИВОСТЕЙ ЕЛЕКТРОННИХ ПІДПИСІВ ЗГІДНО З ДСТУ ISO/IEC 9796-3:2014

Вступ

Для надання в різноманітних інформаційних технологіях електронних довірчих послуг на міжнародному, регіональних та національних рівнях застосовується значне число стандартизованих механізмів електронних підписів (ЕП) [1 – 3, 7]. В Європейському Союзі (ЄС) виконано ряд проектів нормалізації відносно ЕП [6, 14]. Вважалось, що вони вирішують проблеми до 2030 р. Але з оглядом на останні дослідження, в частині вимог та розроблення постквантових стандартів ЕП, постали нові, як теоретичні так і практичні, задачі обґрунтування методів побудови, аналізу та порівняльного аналізу алгоритмів ЕП. При цьому розробники та користувачі додатків електронних довірчих послуг можуть вибрати алгоритми ЕП із існуючих міжнародних та національних стандартів, перше за все ДСТУ ISO/IEC 14888-1,2,3 [1, 2], ДСТУ ISO/IEC 9796-3 [3], ДСТУ 4145-2002 [7]. Тому, ми вважаємо, що нині важливими та такими, що вимагають вирішення, є теоретичні та практичні проблемні питання обґрунтування та вибору методів оцінки, а також створення на їх основі методики аналізу та порівняльного аналізу існуючих та перспективних ЕП.

Після проведення аналізу існуючих джерел було визначено, що такі методики аналізу та порівняльного аналізу ЕП було запропоновано в [4, 8, 16, 17], а потім детально надано в [6]. Сутність пропозицій полягала у поділі критеріїв оцінки ЕП на безумовні та умовні, а потім використання їх для обчислення значень інтегральних умовних та безумовних критеріїв оцінки ЕП. Запропоновані безумовні критерії та на їх основі інтегральний безумовний критерій є ефективними та дозволяють оцінити чи порівняти алгоритми ЕП. Але запропоновані в [6, 10, 21] методи обчислення значень інтегрального умовного критерію на основі методів попарного порівняння та ієрархій, значною мірою залежать від компетентності експертів та їх суб’єктивної думки. У той же час існують інші методи, серед яких заслуговує на увагу метод вагових коефіцієнтів [9, 18, 20], а також практичні рекомендації, що його підтримують.

Мета статті – теоретичне обґрунтування та практична реалізація методів оцінювання та розробка на їх основі методики оцінювання та порівняльного аналізу механізмів ЕП згідно ДСТУ ISO/IEC 9796-3:2014 за умовними та безумовними критеріями.

Постановка проблеми

Після аналізу джерел [4, 6, 8, 16, 17] було визначено, що важливим етапом вибору перспективного криптопримітиву є прийняття рішення про визначення найбільш перспективного алгоритму чи алгоритмів ЕП, причому завершальним етапом є їх порівняльний аналіз згідно з визначеними частковими та інтегральними умовними і безумовними критеріями. По суті, ця задача відносно криптографічних примітивів практично не вирішена, свідченням цього є проведення міжнародних проектів, таких як AES, NESSIE та SHA-3 [6]. На наш погляд, при прийнятті рішення відносно рекомендації певного криптографічного примітиву в якості стандарту в основному враховувались оцінки та думки спеціальних служб та суб’єктивне оцінювання експертів. Однак думки та вплив експертів, на наш погляд, були несуттєвими. Тому важливою теоретичною та практичною проблемою є обґрунтування та вибір, у відповідності з вимогами, множин показників та критеріїв оцінки, обґрунтування та вибір методу чи методів оцінювання та порівняльного аналізу властивостей, а також розроблення та практичне застосування науково обґрунтованих методик оцінювання та порівняльного аналізу певного класу криптопримітивів.

Вказану проблему розглянемо в основному на алгоритмах, стійкість яких ґрунтується на складності дискретного логарифмування в скінченному полі та групі точок еліптичних кри-

вих – ДСТУ ISO/IEC 9796-3 [3]. Таким чином, метою досліджень, що є предметом статті, є розгляд, аналіз та порівняльний аналіз ЕП ДСТУ ISO/IEC 9796-3 за сукупністю безумовних та умовних критеріїв [6], а також окремо аналіз та розробка рекомендацій із застосування методів та такого роду методики для аналізу та порівняння ЕП на прикладі алгоритмів ЕП згідно ДСТУ ISO/IEC 9796-3[3].

Застосування методів і методик оцінювання та порівняльного аналізу ЕП

З зазначенного витікає необхідність та актуальність вирішення проблеми автоматизації та суттєвого зменшення суб'єктивності прийняття рішень відносно переваг певної множини криптопримітивів, наприклад ЕП. Для оцінки та порівняльного аналізу ЕП в [10, 12, 13, 22 – 24] запропоновано методи попарного порівняння та метод ієрархій [5, 21].

Далі під критерієм будемо розуміти ознаку, на основі якої здійснюється оцінка, визначення чи класифікація чого-небудь [4, 6], тобто, будемо розуміти мірило оцінки. Проведені попередні дослідження та [6] дозволяють обґрунтувати висновок, що оцінку та порівняння стандартизованих механізмів ЕП потрібно здійснювати, використовуючи дві сукупності критеріїв: безумовні та умовні [6]. Беручи до уваги [6], оцінку криптоперетворень типу ЕП можна виконати у два етапи.

На першому етапі перевіряється відповідність стандартизованих алгоритмів вимогам безумовних критеріїв – частковим та інтегральному, а на другому, з використанням умовних критеріїв, – часткових умовних та умовного інтегрального критерію. За допомогою використання умовних часткових критеріїв та інтегрального умовного критерію якраз і з'являється можливість порівняти різні криптографічні перетворення типу ЕП.

Оцінювання механізмів ЕП згідно ДСТУ ISO/IEC 9796-3:2014 за безумовними критеріями

До безумовних критеріїв будемо відносити ті критерії, виконання яких для криптоперетворень типу ЕП є обов'язковим, тобто безумовним.

Проведений аналіз стану застосування, досвід розроблення й оцінки властивостей криптоперетворень типу ЕП, в першу чергу в групі точок ЕК, досягнуті результати при практичному розв'язанні задач криптоаналізу та реалізації різних атак дозволяють як основні обирати наступні безумовні критерії [6]:

$W_{\delta 1}$ – надійність математичної бази, що застосовується для ЕП при криптоперетвореннях;

$W_{\delta 2}$ – практична захищеність криптографічних перетворень типу ЕП від відомих атак;

$W_{\delta 3}$ – реальна захищеність ЕП від усіх відомих та потенційно можливих криптоаналітичних атак;

$W_{\delta 4}$ – статистична безпечність криптографічного перетворення типу ЕП;

$W_{\delta 5}$ – теоретична захищеність криптографічного перетворення типу ЕП в групі точок ЕК;

$W_{\delta 6}$ – відсутність слабких особистих ключів криптографічного перетворення типу ЕП;

$W_{\delta 7}$ – складність прямого $I_{пр}$ та зворотного $I_{зв}$ криптографічних перетворень щодо ЕП має не вище за поліноміальний характер.

Оскільки наведені часткові критерії є безумовними, то критерієм добору є логічна зміна так/ні (1/0), отже, безумовний критерій можна записати у вигляді [6]:

$$\left(W_{\delta 1}, W_{\delta 2}, W_{\delta 3}, W_{\delta 4}, W_{\delta 5}, W_{\delta 6}, W_{\delta 7}\right) \in \left(1, 0\right). \quad (1)$$

Враховуючи наведені часткові безумовні критерії $W_{\delta 1}$–$W_{\delta 7}$ та умову (1), функцію відповідності криптоперетворення можно подати так:

$$f_{фв}() = \mathrm{W}_{\delta 1} \wedge \mathrm{W}_{\delta 2} \wedge \mathrm{W}_{\delta 3} \wedge \mathrm{W}_{\delta 4} \wedge \mathrm{W}_{\delta 5} \wedge \mathrm{W}_{\delta 6} \wedge \mathrm{W}_{\delta 7}. \quad (2)$$

Тобто, якість криптографічного перетворення ЕП може оцінюватись з використанням безумовного інтегрального критерію – функції відповідності криптоперетворення ЕП вимогам $f_{фв}() \in (0;1)$ та при $f_{фв}() = 1$ криптографічне перетворення ЕП, що оцінюється, відповідає вимогам.

Введений таким чином інтегральний критерій дозволяє встановити, чи відповідає криптоперетворення типу ЕП, що розглядається, розглянутим вимогам. У випадку, якщо ЕП відповідає вимогам, то він може бути обґрунтовано рекомендований для застосування.

За умови позитивної оцінки ЕП за інтегральним безумовним критерієм подальше порівняння та оцінку можна зробити на основі умовних критеріїв та інтегрального умовного критерію [6].

Таблиця 1

Критерій ЕП / Алгоритм ЕП	$\mathrm{W}_{\delta 1}$	$\mathrm{W}_{\delta 2}$	$\mathrm{W}_{\delta 3}$	$\mathrm{W}_{\delta 4}$	$\mathrm{W}_{\delta 5}$	$\mathrm{W}_{\delta 6}$	$\mathrm{W}_{\delta 7}$	W_{δ}
NR	1	1	1	1	1	1	1	1
ECNR	1	1	1	1	1	1	1	1
ECMR	1	1	1	1	1	1	1	1
ECAO	1	1	1	1	1	1	1	1
ECPV	1	1	1	1	1	1	1	1
ECKNR	1	1	1	1	1	1	1	1

Подальше порівняння та оцінювання на основі умовних критеріїв та інтегрального умовного критерію буде здійснюватись для усіх механізмів ЕП стандарту.

Оцінка механізмів ЕП згідно ДСТУ ISO/IEC 9796-3:2014 за умовними критеріями

У випадку, коли за інтегральним безумовним критерієм було отримано позитивну оцінку ЕП, подальше порівняння та оцінку можна зробити на основі визначення та порівняння умовних критеріїв та інтегрального умовного критерію.

Проведені дослідження показали, що якісне та кількісне порівняння криптографічних перетворень типу ЕП можна здійснити, використовуючи узагальнений умовний критерій переваги [4, 6], або інтегральний умовний критерій.

Як основні часткові умовні критерії пропонується використовувати наступні:

W_{y1} – можливість та умови вільного поширення й застосування міжнародного або національного стандарту криптографічних перетворень ЕП в Україні з урахуванням нормативно-правових актів України на експорт, імпорт і обмеження на його застосування, в тому числі для надання електронних довірчих послуг;

W_{y2} – рівень довіри до міжнародного або національного стандарту криптографічного перетворення в групі точок ЕК, що визначається результатами досліджень і степенем поширення застосування та визнання в різних державах і міжнародно визнаних системах, в тому числі для надання електронних довірчих послуг;

W_{y3} – перспективність застосування міжнародного або національного стандарту в Україні з урахуванням визнання та застосування перспективних інформаційно-телекомунікаційних систем, хмарних обчислень та інших інформаційних технологій тощо;

W_{y4} – часова та просторова складність апаратної, апаратно-програмної та програмної реалізацій засобів ЕП та управління й сертифікації ключів, в тому числі для надання електронних довірчих послуг тощо;

W_{y5} – можливість і умови застосування стандартів з різними значеннями загальносистемних параметрів і ключів, методами виготовлення та обслуговування сертифікатів відкритих ключів, в тому числі для надання електронних довірчих послуг тощо;

W_{y6} – степінь гнучкості ЕП з точки зору використання в різних додатках, за різних вимог та обмежень, у різних умовах, степінь уніфікації та стандартизації, в тому числі для надання електронних довірчих послуг тощо.

При застосуванні визначених критеріїв оцінки важливо вибрати метод згортання часткових умовних критеріїв в умовний інтегральний критерій. Проведений аналіз та практичні дослідження показали [6], що в якості методів згортання часткових умовних критеріїв можна обрати метод аналізу ієрархій на основі попарних порівнянь та метод визначення вагових коефіцієнтів.

При застосуванні методу аналізу ієрархій на основі попарних порівнянь, отримані судження виражаються в цілих числах з урахуванням дев'ятибальної шкали (табл. 2) [4, 6].

Таблиця 2

Ступінь значимості	Визначення	Пояснення
1	Однакова значимість	Дві дії роблять однаковий внесок у досягнення мети
3	Деяка перевага значимості однієї дії над іншою (слабка значимість)	Існують розуміння на користь переваги однієї з дій, однак ці розуміння недостатньо переконливі
5	Істотна або сильна значимість	Є надійні дані або логічні судження для того, щоб показати перевагу однієї з дій
7	Очевидна або дуже сильна значимість	Переконливе свідчення на користь однієї дії перед іншою
9	Абсолютна значимість	Свідчення на користь переваги однієї дії щодо іншої найвищою мірою переконливі
2, 4, 6, 8	Проміжні значення між двома сусідніми судженнями	Ситуація, коли необхідне компромісне рішення
Зворотні величини приведених вище ненульових величин	Якщо дії і при порівнянні з дією *j* приписується одне з визначених ненульових чисел, то дії *j* при порівнянні з дією *i* приписується зворотне значення	Якщо узгодженість була постульованою при одержанні *N* числових значень для утворення матриці

Метод аналізу ієрархій на основі попарного порівняння та особливості його застосування для оцінки алгоритмів ЕП

Для застосування даного методу необхідно вибрати систему умовних критеріїв. За допомогою такої множини показників з застосуванням умовних критеріїв можна обчислити значення інтегрального умовного критерію, та, як наслідок, виконати порівняння ЕП за умовним інтегральним критерієм.

Метод попарного порівняння елементів [4, 6, 8, 17] можна описати наступним чином. Будується множина матриць парних порівнянь. Парні порівняння проводяться в термінах домінування одного елемента над іншим. Отримані судження виражаються в цілих числах з урахуванням дев'ятибальної шкали у табл. 2 [4, 6].

При побудові матриці попарних порівнянь для усіх критеріїв необхідно визначити відношення узгодженості [6] для кожного з критеріїв.

Оцінку компоненти власного вектора вирахуємо за формулою

$$q_i = (W_{yi} \times W_{yi+1} \times \ldots \times W_{yn})^{\frac{1}{n}}. \quad (3)$$

Нормалізовану оцінку вектору пріоритету визначимо за формулою

$$r_i = q_i \div z, \quad (4)$$

де z – відношення узгодженості матриці, що обчислюється за формулою

$$z = \sum_{i=1}^{n} q_i \ . \tag{5}$$

Значення відношення узгодженості матриці знаходиться у діапазоні $[0, \sum_{i=1}^{n} q_{i\max}]$, де $q_{i\max}$ – максимально можливе значення оцінки компоненти власного вектора для обраного випадку.

Аналіз та умови застосування методу аналізу ієрархій на основі попарного порівняння у криптографії

Порівняльний аналіз механізмів ЕП згідно ДСТУ ISO/IEC 9796-3:2014

Розглянемо практичне застосування методу аналізу ієрархій на основі попарних порівнянь на прикладі механізмів ЕП згідно з ДСТУ ISO/IEC 9796-3:2014.

Порівняємо алгоритми ЕП відносно умовних критеріїв, для цього побудуємо дерево цілей (рис. 1).

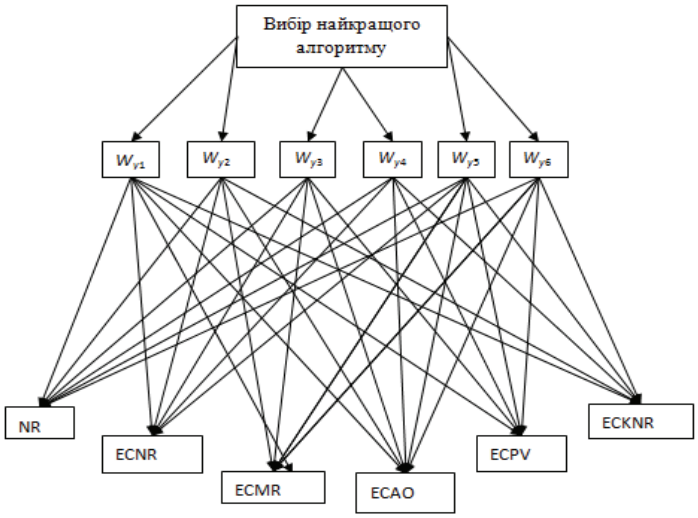

Рис. 1. Дерево цілей

Тепер зробимо оцінку кожного критерію. Побудуємо матрицю попарних порівнянь відносно порівнюваних алгоритмів ЕП для кожного критерію (табл. 3).

Таблиця 3

	W_{y1}	W_{y2}	W_{y3}	W_{y4}	W_{y5}	W_{y6}	q_i	r_i
W_{y1}	*1*	*1/6*	*4*	*1/4*	*1/2*	*1/3*	*0,5503*	*0,0714*
W_{y2}	*6*	*1*	*4*	*5*	*4*	*3*	*3,3604*	*0,4362*
W_{y3}	*1/4*	*1/4*	*1*	*3*	*2*	*1/2*	*0,7565*	*0,0982*
W_{y4}	*4*	*1/5*	*1/3*	*1*	*1/4*	*1/4*	*0,5054*	*0,0656*
W_{y5}	*2*	*1/4*	*1/2*	*4*	*1*	*1/3*	*0,8327*	*0,1081*
W_{y6}	*3*	*1/3*	*2*	*4*	*3*	*1*	*1,6984*	*0,2205*

Відношення узгодженості дорівнює 7,7037.

Як приклад наведемо матрицю попарних порівнянь відносно порівнюваних алгоритмів ЕП для критерію W_{y1}. Для цього побудуємо табл. 4, використовуючи формули (3) – (5). Інші матриці попарних порівнянь будуються аналогічним чином [4, 6].

Для обчислення результуючого вектора пріоритетів перемножимо вектор пріоритетів першого рівня і матрицю набутих значень першого рівня (рис. 2).

Таблиця 4

	NR	ECNR	ECMR	ECAO	ECPV	ECKNR	q_j	r_j
NR	1	1/5	2	1/2	1/5	1/3	0,487	0,072
ECNR	5	1	1/4	3	2	3	1,680	0,25
ECMR	1/2	4	1	1/2	1/4	1/2	0,707	0,105
ECAO	2	1/3	2	1	1/4	1/3	0,693	0,103
ECPV	5	1/2	4	4	1	1/2	1,647	0,245
ECKNR	3	1/3	2	3	2	1	1,513	0,225

Відношення узгодженості дорівнює 6,72.

$$B1 := \begin{pmatrix} 0.071 \\ 0.436 \\ 0.098 \\ 0.065 \\ 0.108 \\ 0.220 \end{pmatrix} \qquad B2 := \begin{pmatrix} 0.072 & 0.05 & 0.105 & 0.103 & 0.245 & 0.025 \\ 0.101 & 0.16 & 0.080 & 0.140 & 0.334 & 0.127 \\ 0.042 & 0.27 & 0.08 & 0.161 & 0.373 & 0.146 \\ 0.046 & 0.104 & 0.343 & 0.157 & 0.068 & 0.280 \\ 0.167 & 0.167 & 0.167 & 0.167 & 0.167 & 0.167 \\ 0.152 & 0.183 & 0.193 & 0.192 & 0.136 & 0.142 \end{pmatrix}$$

$$B := B1^{T} \cdot B2 = (0.108 \quad 0.165 \quad 0.133 \quad 0.155 \quad 0.252 \quad 0.139)$$

Рис. 2. Обчислення результуючого вектора пріоритетів

Розглянемо отримані чисельні результати. Досліджувані алгоритми ЕП, засновані на перетвореннях у групі точок ЕК та спарюванні точок ЕК, можна розташувати за місцями, які вони зайняли за результатами порівняння (1 – найкращий, 6 – найгірший):

1. ECPV – 0,252; 2. ECNR – 0,165; 3. ECAO –0,155; 4. ECKNR– 0,139; 5. ECMR – 0,133; 6. NR – 0,108.

Найбільш перспективними у ДСТУ ISO/IEC 9796-3:2014 є механізми ЕП ECPV (підпис з відновленням повідомлення Пінтсова – Ванстона, заснований на еліптичній кривій) та ECNR (підпис з відновленням повідомлення Ніберга – Рюпеля, заснований на еліптичній кривій). ECPV використовує симетричне шифрування (для включення інформації до підпису), та не надає обмежень щодо обсягу відновлюваної інформації. Алгоритм NR має найгірший результат за інтегральним показником, що обґрунтовується математичним апаратом, що використовується у даному алгоритмі.

Методи оцінювання та порівняльного аналізу механізмів ЕП згідно ДСТУ ISO/IEC 9796-3:2014 на основі визначення вагових коефіцієнтів

Якщо дані про важливість параметрів порівнюваних систем оцінити із використанням неформальних методів неможливо, необхідно використовувати формалізовані методи, до яких належать ті, що базуються на визначенні вагових коефіцієнтів [9, 11, 18 – 20, 22].

Розглянемо загальну постановку задачі для методики оцінювання ЕП на основі методу визначення вагових коефіцієнтів.

Нехай є k механізмів ЕП, які необхідно оцінити, m показників, за якими оцінюються системи, та n експертів, які проводять оцінювання.

Нижче наведено часткові показники, за якими можуть бути оцінені механізми ЕП:

x_1 – можливість вільного поширення та застосування міжнародного або національного стандарту криптографічних перетворень ЕП в Україні;

x_2 – рівень довіри до міжнародного або національного криптографічного перетворення в групі точок ЕК та на основі математичного апарату спарювання точок ЕК;

x_3 – перспективність застосування міжнародного або національного стандарту в Україні;

x_4 – часова та просторова складності апаратної, апаратно-програмної та програмної реалізації засобів ЕП;

x_5 – можливість застосування стандартів з різними значеннями загальносистемних параметрів та ключів;

x_6 – степінь гнучкості алгоритму ЕП з точки зору використання у різних додатках, за різних вимог та обмежень.

Далі визначають значення вагових коефіцієнтів самих показників. Необхідно провести експертне оцінювання цих часткових показників. Використовуються такі методи:

- за допомогою шкали Фішберна;
- на основі методу ранжування;
- на основі методу приписування балів;
- на основі числового способу.

Після цього необхідно провести експертне оцінювання систем за вказаними методами визначення вагових коефіцієнтів. Показники ранжуються за ступенем кращої характеристики в обраній системі.

Метод визначення вагових коефіцієнтів та оцінки ЕП за допомогою шкали Фішберна

Нехай в якості вхідних даних вибрано: n=4 – кількість експертів, m=6 – кількість показників.

Відповідно до правил проведення оцінювання згідно з визначеним методом побудуємо таблицю значень показників методу шкали Фішберна для алгоритмів ЕП стандарту ДСТУ ISO/IEC 9796-3. Результати наведено в табл. 5, 6.

Таблиця 5

Показники / Експерти	x_1	x_2	x_3	x_4	x_5	x_6
1	1	6	5	2	3	4
2	3	4	6	1	5	2
3	1	4	5	3	6	2
4	2	3	6	1	4	5

Таблиця 6

Експерти	Показники					
	x_1	x_2	x_3	x_4	x_5	x_6
1	0,285	0,047	0,095	0,238	0,190	0,142
2	0,190	0,142	0,047	0,285	0,095	0,238
3	0,285	0,142	0,095	0,190	0,047	0,238
4	0,238	0,190	0,047	0,285	0,142	0,095
w_i	0,249	0,130	0,071	0,249	0,118	0,178

Аналогічно будуємо таблиці для усіх механізмів ЕП згідно ДСТУ ISO/IEC 9796-3:2014.

Після проведення оцінювання отримаємо наступні результати, що наведені на рис. 3.

Далі проведемо аналіз отриманих результатів згідно з рис. 3. Для цього розміщаємо значення Rez_1 по мірі їх зменшення, тобто:

1. ECPV – 0,245; 2. ECNR – 0,223; 3. ECAO – 0,186; 4. ECKNR – 0,179; 5. ECMR – 0,160; 6. NR – 0,144.

Слід зазначити, що отримані результати не можна сприймати як для застосування, скоріше за все, це методика порівняння ЕП. Для реальних використань необхідно відповідним чином вибрати умовні критерії та провести дослідження.

$$M\_1 := \begin{bmatrix} 0.142 & 0.130 & 0.273 & 0.106 & 0.249 & 0.094 \\ 0.273 & 0.130 & 0.082 & 0.190 & 0.379 & 0.226 \\ 0.094 & 0.189 & 0.166 & 0.249 & 0.237 & 0.059 \\ 0.225 & 0.190 & 0.566 & 0.106 & 0.154 & 0.118 \\ 0.118 & 0.273 & 0.237 & 0.522 & 0.142 & 0.094 \\ 0.273 & 0.094 & 0.142 & 0.202 & 0.201 & 0.08 \end{bmatrix}$$

$$V\_F := [0.249 \;\; 0.130 \;\; 0.071 \;\; 0.249 \;\; 0.118 \;\; 0.178]$$

$$Rez\_1 := M\_1 \cdot V\_F^{\mathrm{T}}$$

$$Rez\_1^{\mathrm{T}} = [0.144 \;\; 0.223 \;\; 0.16 \;\; 0.186 \;\; 0.245 \;\; 0.179]$$

Рис. 3. Обчислення результуючого вектора пріоритетів

Метод визначення вагових коефіцієнтів та оцінки ЕП на основі методу ранжування

n=4 – кількість експертів, m=6 – кількість показників

Відповідно до правил проведення оцінювання згідно з визначеним методом, побудуємо таблицю для показників (табл. 7).

Таблиця 7

Експерти	Показники					
	x_1	x_2	x_3	x_4	x_5	x_6
1	5	1	4	6	3	2
2	4	2	6	5	3	1
3	5	3	6	4	2	1
4	5	2	4	6	1	3
$r_j = \sum_{i=1}^{n} r_{ij}$	19	8	20	21	9	7
w_j	0,226	0,095	0,238	0,250	0,226	0,083

Аналогічно будуємо таблиці для усіх механізмів ЕП згідно ДСТУ ISO/IEC 9796-3:2014.

Після проведення оцінювання отримаємо наступні результати, що наведені на рис. 4.

Далі проведемо аналіз отриманих результатів згідно з рис. 4. Для цього розміщаємо значення Rez_2 по мірі їх зменшення, тобто:

1. ECNR – 0,209; 2. ECPV – 0,207; 3. ECKNR – 0,200; 4. ECAO – 0,179; 5. ECMR – 0,168; 6. NR – 0,157.

Таким чином, ЕП ECNR за інтегральним показником має найбільші переваги. Алгоритм ЕП NR (як і у випадку порівняння за методом аналізу ієрархій та методом на основі шкали Фішберна) має найгірший результат, що обґрунтовується математичним апаратом, що використовується у даному алгоритмі.

$$M\_2 := \begin{bmatrix} 0.130 & 0.270 & 0.178 & 0.059 & 0.107 & 0.250 \\ 0.107 & 0.059 & 0.238 & 0.202 & 0.273 & 0.119 \\ 0.071 & 0.190 & 0.071 & 0.166 & 0.238 & 0.261 \\ 0.154 & 0.261 & 0.059 & 0.261 & 0.130 & 0.130 \\ 0.250 & 0.130 & 0.095 & 0.238 & 0.226 & 0.059 \\ 0.107 & 0.059 & 0.154 & 0.238 & 0.261 & 0.178 \end{bmatrix}$$

$$V\_2 := [0.226 \;\; 0.095 \;\; 0.238 \;\; 0.250 \;\; 0.226 \;\; 0.083]$$

$$Rez\_2 := M\_2 \cdot V\_2^{\mathrm{T}}$$

$$Rez\_2^{\mathrm{T}} = [0.157 \;\; 0.209 \;\; 0.168 \;\; 0.179 \;\; 0.207 \;\; 0.2]$$

Рис. 4. Обчислення результуючого вектора пріоритетів

Метод визначення вагових коефіцієнтів та оцінки ЕП на основі методу приписування балів

n=4 – кількість експертів, m=6 – кількість показників

Відповідно до правил проведення оцінювання згідно з визначеним методом, побудуємо таблицю для показників (табл. 8).

Таблиця 8

Показники / Експерти	x_1	x_2	x_3	x_4	x_5	x_6	$\sum_{j=1}^{m} h_{ij}$	Ваги показників					
								r_{i1}	r_{i2}	r_{i3}	r_{i4}	r_{i5}	r_{i6}
1	8	7	10	2	5	4	36	0,222	0,194	0,277	0,055	0,138	0,111
2	7	8	9	1	4	3	32	0,218	0,250	0,281	0,031	0,125	0,093
3	9	5	7	1	3	2	27	0,333	0,185	0,259	0,037	0,111	0,074
4	8	6	10	1	4	3	32	0,250	0,187	0,312	0,031	0,125	0,093
							$\sum_{i=1}^{n} r_j$	1,023	0,816	1,129	0,154	0,499	0,371
							w_j	0,256	0,204	0,282	0,038	0,125	0,092

Аналогічно будуємо таблиці для усіх механізмів ЕП згідно ДСТУ ISO/IEC 9796-3:2014.

Після проведення оцінювання отримаємо наступні результати, що наведені на рис. 5.

$$M\_3 := \begin{bmatrix} 0.162 & 0.037 & 0.089 & 0.290 & 0.185 & 0.233 \\ 0.108 & 0.175 & 0.245 & 0.178 & 0.120 & 0.170 \\ 0.155 & 0.065 & 0.086 & 0.229 & 0.295 & 0.164 \\ 0.061 & 0.282 & 0.115 & 0.202 & 0.123 & 0.212 \\ 0.197 & 0.248 & 0.284 & 0.107 & 0.100 & 0.049 \\ 0.226 & 0.06 & 0.179 & 0.231 & 0.167 & 0.128 \end{bmatrix}$$

$$V\_3 := [0.256 \;\; 0.204 \;\; 0.282 \;\; 0.038 \;\; 0.125 \;\; 0.092]$$

$$Rez\_3 := M\_3 \cdot V\_3^{\mathrm{T}}$$

$$Rez\_3^{\mathrm{T}} = [0.13 \;\; 0.17 \;\; 0.138 \;\; 0.148 \;\; 0.202 \;\; 0.162]$$

Рис. 5. Обчислення результуючого вектора пріоритетів

Далі проведемо аналіз отриманих результатів згідно з рис. 5. Для цього розміщаємо значення Rez_3 по мірі їх зменшення, тобто:

1. ECPV – 0,202; 2. ECNR – 0,170; 3. ECKNR – 0,162; 4. ECAO – 0,148; 5. ECMR – 0,138; 6. NR – 0,130.

Як і у попередньому методі, ЕП NR має найгірший результат, що обґрунтовується математичним апаратом, що використовується у даному алгоритмі. Найкращий результат має механізм ЕП ECPV.

Метод визначення вагових коефіцієнтів та оцінки ЕП на основі числового способу

n=4 – кількість експертів, m=6 – кількість показників

Таблиця 9

Показники / Оцінювання	x_1	x_2	x_3	x_4	x_5	x_6
$x_{i\min}$	0,190	0,047	0,047	0,190	0,047	0,095
$x_{i\max}$	0,285	0,190	0,095	0,285	0,190	0,238
δ_i	0,333	0,752	0,505	0,333	0,752	0,600
w_i	0,101	0,229	0,154	0,101	0,229	0,183

Відповідно до правил проведення оцінювання згідно з визначеним методом, побудуємо таблицю для показників (табл. 9). Значення коефіцієнтів обираються із методу на основі шкали Фішберна.

Аналогічно будуємо таблиці для усіх механізмів ЕП згідно ДСТУ ISO/IEC 9796-3:2014.

Після проведення оцінювання отримаємо наступні результати, що наведені на рис. 6.

$$M\_4 := \begin{bmatrix} 0.246 & 0.053 & 0.109 & 0.262 & 0.108 & 0.219 \\ 0.054 & 0.108 & 0.224 & 0.180 & 0.216 & 0.216 \\ 0.250 & 0.166 & 0.054 & 0.250 & 0.054 & 0.222 \\ 0.073 & 0.083 & 0.357 & 0.179 & 0.223 & 0.083 \\ 0.052 & 0.240 & 0.214 & 0.213 & 0.214 & 0.064 \\ 0.227 & 0.170 & 0.204 & 0.113 & 0.113 & 0.171 \end{bmatrix}$$

$$V\_4 := [0.101 \;\; 0.229 \;\; 0.154 \;\; 0.101 \;\; 0.229 \;\; 0.183]$$

$$Rez\_4 := M\_4 \cdot V\_4^{\mathrm{T}}$$

$$Rez\_4^{\mathrm{T}} = [0.145 \;\; 0.172 \;\; 0.15 \;\; 0.166 \;\; 0.175 \;\; 0.162]$$

Рис. 6. Обчислення результуючого вектора пріоритетів

Проведемо аналіз отриманих результатів згідно рис. 6. Для цього розміщаємо значення Rez_4 по мірі їх зменшення, тобто:

1. ECPV – 0,175; 2. ECNR – 0,172; 3. ECAO – 0,166; 4. ECKNR – 0,162; 5. ECMR – 0,150; 6. NR – 0,145.

У даному випадку також необхідно зазначити, що отримані результати не можна сприймати до застосування, скоріше всього, це методика порівняння механізмів ЕП. Для реальних використань необхідно відповідним чином вибрати умовні критерії та провести дослідження.

Аналіз результатів досліджень ЕП згідно з ДСТУ ISO/IEC 9796-3:2014

За вибраними методиками оцінювання механізмів ЕП отримано результати, що показані у попередніх розділах. Порівняння механізмів ЕП було виконано на основі оцінок експертів. Після цього були виконані розрахунки за вказаними вище методиками.

Оцінки механізмів ЕП згідно з ДСТУ ISO/IEC 9796-3:2014 мають схожий порядок ранжування за різними методами оцінювання – від найбільшої до найменшої.

На рис. 7 графічно зображено результати оцінювання механізмів ЕП за різними методами оцінювання. Цифрами від 1 до 6 позначено механізми ЕП: 1 – NR, 2 – ECNR, 3 – ECMR, 4 – ECAO, 5 – ECPV, 6 – ECKNR.

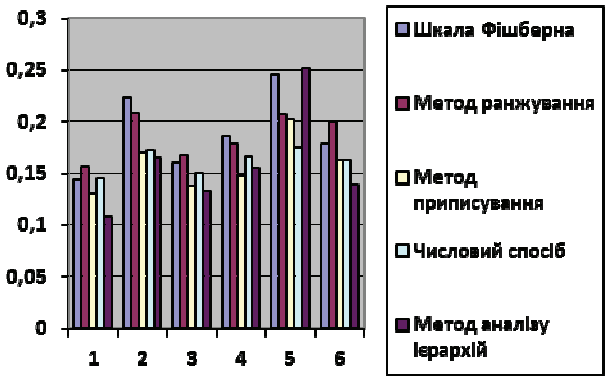

Рис. 7. Результати оцінювання механізмів ЕП за різними методиками

Висновки

1. У зв'язку із специфікою вимог до криптографічних перетворень, у тому числі до ЕП, основні критерії необхідно розділити на два класи: умовні та безумовні.

Безумовними називаються такі критерії, виконання яких для будь-яких криптографічних перетворень є обов'язковим, тобто безумовним.

Умовними називаються критерії, виконання яких для будь-яких криптографічних перетворень відбувається лише за визначеної умови.

2. У результаті проведених досліджень було визначено, що в якості основного критерію для інтегральної оцінки можна та рекомендується використовувати інтегральний безумовний критерій, який отримується на основі часткових безумовних критеріїв.

Якщо хоча б один частковий критерій не відповідає умовам, то таке криптоперетворення відкидається як таке, що не відповідає вимогам.

3. Запропонована методика порівняльного аналізу стандартизованих ЕП ґрунтується на використанні сукупності часткових безумовних і умовних критеріїв, на основі яких обчислюється значення інтегральних умовних та безумовних інтегральних критеріїв.

4. Результати досліджень дозволили зробити висновок, що з точки зору об'єктивності оцінювання краще застосовувати метод визначення вагових коефіцієнтів, оскільки в методі аналізу ієрархій на основі попарних порівнянь на результат суттєво впливає суб'єктивність експертів.

5. Порівняльний аналіз механізмів підпису згідно ДСТУ ISO/IEC 9796-3:2014 показав, що найбільш перспективними є механізми підпису ECPV (підпис з відновленням повідомлення Пінтсова – Ванстона, заснований на еліптичній кривій) та ECNR (підпис з відновленням повідомлення Ніберга – Рюпеля, заснований на еліптичній кривій).

Алгоритм ЕП NR має найгірший результат, що обґрунтовується математичним апаратом, який використовується у даному алгоритмі.

6. Для отримання більш точних результатів оцінювання, а також для точного співпадіння розташування механізмів ЕП за усіма методами оцінювання необхідно виконати процедуру оцінювання декілька разів та ретельно підійти до вибору експертів, що будуть проводити оцінювання.

Список літератури: 1. *Information t*echnology – 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 – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms : ISO/IEC 14888-3 (Edition 2 (2006-11-15)) : 2006. – 68 p. 3. *Information* technology – Security techniques – Digital signatures schemes giving message recovery. – Part 3: Discrete logarithm based mechanisms : ISO/IEC 9796-3:2014. 4. *Андрейчиков, А. В.* Анализ, синтез, планирование решений в экономике / А.В. Андрейчиков, О.Н. Андрейчикова. – М. : Финансы и статистика, 2002. – 359 с. 5. *Аналитическая* иерархическая процедура Саати [Електронний ресурс]. – Режим доступу: http://www.gorskiy.ru/Articles/Dmss/AHP.html. 6. *Горбенко, Ю.І.* Методи побудування та аналізу криптографічних систем : монографія / Ю.І. Горбенко. – Харків : Форт, 2015. – 959 с. 7. *Інформаційні* технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка : ДСТУ 4145-2002. – К. : Держстандарт України, 2003. – 35 с. 8. *Корченко, А.Г.* Построение систем защиты информации на нечетких множествах / А.Г. Корченко. – М. : МК-Пресс, 2006. – 320 с. 9. *Макарова, И.Л.* Анализ методов определения весовых коэффициентов в интегральном показателе общественного здоровья / И.Л. Макарова // Международный научный журнал «Символ науки». – Уфа, 2015. – № 7 – С.87–94. 10. *Метод* анализа иерархий [Електронний ресурс]. – Режим доступу: https://ru.wikipedia.org/wiki/%D0%9C 11. Методы определения весовых коэффициентов [Електронний ресурс]. – Режим доступу: http://8v83.tom.ru/8V83 12. *Методы* экспертных оценок [Електронний ресурс]. – Режим доступу: https://habrahabr.ru/post/189626/. 13. *Метод* экспертных оценок [Електронний ресурс]. – Режим доступу: http://center-yf.ru/data/Marketologu/Metod-ekspertnyh-ocenok.php. 14. *Новицький, А. М.* Електронний документообіг як елемент забезпечення правового регулювання становлення інститутів інформаційного суспільства / А.М. Новицький // Наук. вісник Нац. ун-ту державної податкової служби України (економіка, право). – 2013. – № 4. – С. 11–20. – Режим доступу: http://nbuv.gov.ua/UJRN/Nvnudpsu_2013_4_3. 15. *Ногин, В.Д.* Упрощенный вариант метода анализа иерархий на основе нелинейной свертки критериев / В.Д. Ногин. – Режим доступу: http://www.apmath.spbu.ru/ru/staff/nogin/nogin_p11.pdf. 16. *Окунев, Ю.Б.* Принципы системного подхода к проектированию в технике связи / Ю.Б. Окунев, В.Г. Плотников. – М. : Связь, 1975. – 184 с. 17. *Орловский, С.А.* Проблемы принятия решений при нечеткой исходной информации / С.А. Орловский. – М. : Наука, 1981. – 208 с. 18. *Постников, В.М* Методы выбора весовых коэффициентов локальных критериев / В.М. Постников, С.Б. Спиридонов // Наука и образование. – МГТУ им. Н.Э. Баумана, 2015. – № 6. Режим доступу: http://technomag.bmstu.ru/index.html. 19. *Потапов, Д.К.* О методиках определения весовых коэффициентов в задаче оценки надежности коммерческих банков / Д.К. Потапов, В.В. Евстафьева. – Режим доступу: http://www.ibl.ru/konf/041208/60.pdf. 20. *Романова, И.К*. Об одном подходе к определению весовых коэффициентов метода пространства состояний / И.К. Романова // Наука и образование. – МГТУ им. Н.Э. Баумана, 2015. – № 4. Режим доступу: http://technomag.bmstu.ru/doc/763768.html. 21. *Саати, Т.* Принятие решений: метод анализа иерархий / Т. Саати ; пер. с англ. – М. : Радио и связь, 1993. 22. *Согласование р*езультатов оценки объектов улучшений [Електронний ресурс]. – Режим доступу: http://edu.dvgups.ru/METDOC/EKMEN/FK/OTS_ NEDV/METOD/UP/frame/3_4.htm. 23. *Экспертное* оценивание [Електронний ресурс]. – Режим доступу: https://ru.wikipedia.org/wiki/%D0%AD 24. *Экспертные* оценки при разработке решений [Електронний ресурс]. – Режим доступу: http://books.ifmo.ru/file/pdf/817.pdf.

Харківський національний
університет імені В.Н.Каразіна

Надійшла до редколегії 05.09.2016