center/news/internet-of-things/. 6. Львівський IT-Кластер. Цілі [Електронний ресурс]. – Режим доступу до ресурсу: http://itcluster.lviv.ua/about-us/about-cluster/. 7. Win-Win стратегія для IT-галузі [Електронний ресурс]. – Режим доступу до ресурсу: http://biz.nv.ua/ukr/experts/back/win-win-strategija-dlja-it-galuzi-243352.html. 8. Без різких рухів. Експорт IT в Україні зросте до $5,1 млрд, якщо не заважатиме держава [Електронний ресурс]. – Режим доступу до ресурсу: http://biz.nv.ua/ukr/publications/bez-rizkih-ruhiv-eksport-it-v-ukrajini-zroste-do-5-1-mlrd-jakshcho-ne-zavazhatime-derzhava-232959.html. 9. Український гаджет LaMetric отримав престижну премію Red Dot Product Design Award [Електронний ресурс]. – Режим доступу до ресурсу: http://news.finance.ua/ua/news/-/372886/ukrayinskyj-gadzhet-lametric-otrymav-prestyzhnu-premiyu-red-dot-product-design-award. 10. Інноваційний мікрокосмос [Електронний ресурс]. – Режим доступу до ресурсу: http://zaxid.net/news/showNews.do?innovatsiyniy_mikrokosmos&objectId=1405864.

УДК 004.056.55

І. Д. Горбенко, М. В. Єсіна
Харківський національний університет імені В. Н. Каразіна,
кафедра безпеки інформаційних систем і технологій

МЕТОДИ, МЕТОДИКА ТА РЕЗУЛЬТАТИ ПОРІВНЯЛЬНОГО АНАЛІЗУ ЕЛЕКТРОННИХ ПІДПИСІВ ЗГІДНО З ДСТУ ISO/IEC 14888-3:2014

Розглядаються методи порівняльного аналізу властивостей механізмів електронного підпису (ЕП) згідно з ДСТУ ISO/IEC 14888-3:2014. Досліджено та проаналізовано існуючі методи порівняльного аналізу ЕП на основі методу аналізу ієрархій та методів вагових коефіцієнтів. Наведено певні критерії та показники, що можуть бути використані під час порівняльного аналізу властивостей механізмів ЕП.

Ключові слова: аналіз механізмів ЕП, вагові коефіцієнти, електронний підпис, критерій оцінки ЕП, методи порівняльного аналізу ЕП.

The paper deals with the comparative analysis methods of electronic signature (ES) mechanisms according to DSTU ISO/IEC 14888-3:2014 properties. The existing comparative analysis methods of ES based on the hierarchy analysis process and weight indices methods are investigated and analyzed. Some criteria and indicators that can be used in the comparative analysis of ES mechanisms properties are presented.

Key words: electronic signature mechanisms analysis, weight indices, electronic signature, electronic signature estimation criterion, electronic signature comparison analysis methods.

Вступ

Для надання електронних довірчих послуг на міжнародному, регіональних та національних рівнях прийнято до застосування багато стандартизованих механізмів електронних підписів (ЕП) [1, 2, 6, 7]. У Європейському Союзі (ЄС) виконано багато проектів нормалізації щодо ЕП [5, 14]. Раніше здавалось, що вони вирішують проблеми приблизно до 2030 р. Але згідно з останніми дослідженнями в частині вимог та розробки постквантових стандартів ЕП постали нові як теоретичні, так і практичні

завдання обґрунтування методів побудови, аналізу та порівняльного аналізу ЕП. При цьому розробники та користувачі додатків електронних довірчих послуг можуть обирати механізми ЕП із значної кількості існуючих міжнародних та національних стандартів, передусім ДСТУ ISO/IEC 14888-1,2,3 [1, 2], ДСТУ ISO/IEC 9796-3 [6], ДСТУ 4145–2002 [7] тощо. На наш погляд, сьогодні важливими та такими, що вимагають вирішення, є теоретичні та практичні проблемні питання обґрунтування та вибору методів оцінювання, а також створення на їх основі методики аналізу та порівняльного аналізу існуючих та перспективних механізмів ЕП.

Згідно з нашим аналізом, вперше такі методики оцінювання та порівняльного аналізу механізмів ЕП були запропоновані у [3, 8, 16, 17], потім детально були викладені у [5]. Сутність пропозицій зводилась до поділу критеріїв оцінки механізмів ЕП на безумовні та умовні, а потім використання їх для обчислення значень інтегральних умовних та безумовних критеріїв оцінки ЕП. При цьому запропоновані безумовні критерії та на їх основі інтегральний безумовний критерій є ефективними та дають змогу оцінити чи порівняти існуючі алгоритми ЕП. Але запропоновані у [3, 5, 10, 21] методи обчислення значень інтегрального умовного критерію, що ґрунтуються на методі аналізу ієрархій на основі попарного порівняння, значною мірою залежать від компетентності експертів та впливу їх суб'єктивної думки на результат оцінювання. У той самий час існують інші методи, серед яких заслуговує на увагу метод визначення вагових коефіцієнтів [9, 18, 20], а також практичні рекомендації, що його підтримують.

Мета роботи – теоретично обґрунтувати та практично реалізувати методи оцінювання та розробити на їх основі методики оцінювання та порівняльного аналізу механізмів ЕП згідно з ДСТУ ISO/IEC 14888-3:2014 за умовними та безумовними критеріями.

Постановка проблеми

Аналіз джерел [3, 5, 8, 16, 17] показав, що важливим етапом вибору перспективного крипто-примітиву є прийняття рішення про визначення найперспективнішого механізму чи перспективних механізмів ЕП, причому фінальним етапом є їх порівняльний аналіз згідно з визначеними частковими та інтегральними умовними і безумовними критеріями. Фактично це завдання щодо криптографічних примітивів фактично не вирішене, свідченням чого є проведення міжнародних проектів AES, NESSIE та SHA-3 [5]. На наш погляд, під час прийняття рішення щодо рекомендації певного криптографічного примітиву як стандарт переважно враховувались оцінки та думки спеціальних служб та суб'єктивні думки експертів. Однак ми вважаємо, що думки та вплив експертів був несуттєвими. Тому важливою теоретичною та практичною проблемою є обґрунтування та вибір, відповідно до вимог, множин показників та критеріїв оцінки, обґрунтування та вибір методу чи методів оцінки та порівняльного аналізу властивостей, а також розроблення та практичне застосування науково-обґрунтованих методик оцінювання та порівняльного аналізу певного класу криптографічних примітивів.

Вказану проблему розглянемо передусім на алгоритмах, стійкість яких ґрунтується на складності дискретного логарифмування у скінченному полі та групі точок еліптичних кривих – ДСТУ ISO/IEC 14888-3:2014 [1, 2]. В ДСТУ ISO/IEC 14888-3 до застосування рекомендовано 12 різних механізмів ЕП, які ґрунтуються на використанні математичного апарата скінченних полів, еліптичних кривих (ЕК) та спарювання точок ЕК. Отже, метою досліджень, що є предметом роботи, є розгляд, аналіз та порівняльний аналіз механізмів ЕП згідно з ДСТУ ISO/IEC 14888-3:2014 за сукупністю безумовних та умовних критеріїв [5], а також окремо аналіз та розроблення рекомендацій із застосуванням методів та методики для аналізу та порівняння ЕП на прикладі алгоритмів ДСТУ ISO/IEC 14888-3:2014 [1].

Застосування методів і методик оцінювання та порівняльного аналізу ЕП

Із вищенаведеного випливає необхідність та актуальність вирішення проблеми значною мірою автоматизації та істотного зменшення суб'єктивності прийняття рішень щодо переваг певної множини криптопримітивів, наприклад, ЕП. Вирішення певних складових завдань вказаної проблеми міститься у [5]. У [10, 12, 13, 22–24] для оцінювання та порівняльного аналізу ЕП запропоновано методи попарного порівняння та метод ієрархій.

Далі під критерієм розумітимемо ознаку, на основі якої здійснюється оцінка, визначення чи класифікація будь-чого [5], тобто, по суті, розумітимемо мірило оцінки. Попередні дослідження [5] дають змогу обґрунтувати висновок, що оцінку та порівняння стандартизованих алгоритмів ЕП необхідно виконувати, використовуючи дві сукупності критеріїв: безумовні та умовні [5]. Оцінку криптоперетворень типу ЕП можна виконувати у два етапи, враховуючи [5].

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. Саме за допомогою використання умовних часткових критеріїв та інтегрального умовного критерію і з'являється можливість порівняти різні криптоперетворення типу ЕП.

Оцінювання механізмів ЕП згідно з ДСТУ ISO/IEC 14888-3:2014 за безумовними критеріями

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

Аналіз стану застосування, досвід розроблення й оцінки властивостей криптоперетворень типу ЕП, насамперед в групі точок ЕК, досягнуті результати під час практичного розв'язання задач криптоаналізу та реалізації різних атак дають змогу як основні обрати такі безумовні критерії оцінювання [5]:

W_{d1} – надійність математичної бази, що застосовується для ЕП під час криптоперетворень;

W_{d2} – практична захищеність криптографічних перетворень типу ЕП від відомих атак;

W_{d3} – реальна захищеність ЕП від усіх відомих та потенційно можливих криптоаналітичних атак;

W_{d4} – статистична безпечність криптографічного перетворення типу ЕП;

W_{d5} – теоретична захищеність криптографічного перетворення типу ЕП в групі точок ЕК;

W_{d6} – відсутність слабких особистих ключів криптографічного перетворення типу ЕП;

W_{d7} – складність прямого $I_{ïð}$ та зворотного $I_{зв}$ криптографічних перетворень щодо ЕП має не більше, ніж поліноміальний характер.

Оскільки наведені часткові критерії є безумовними, то критерієм добору є логічна зміна так/ні (1/0), тому безумовний критерій можна записати у такому вигляді [5]:

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

Враховуючи наведені часткові безумовні критерії W_{d1}–W_{d7} та умову (1), функція відповідності криптоперетворення може бути подана у вигляді

$$f_{фв}() = W_{d1} \wedge W_{d2} \wedge W_{d3} \wedge W_{d4} \wedge W_{d5} \wedge W_{d6} \wedge W_{d7}. \quad (2)$$

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

Введений у такий спосіб інтегральний критерій дає змогу встановити, чи відповідає криптоперетворення типу ЕП, що розглядається, розглянутим вимогам. Якщо механізм 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 [5].

У табл. 1 наведено результати порівняльного аналізу щодо безумовних критеріїв для механізмів ЕП згідно з ДСТУ ISO/IEC 14888-3:2014.

Подальше порівняння та оцінювання на основі умовних критеріїв та інтегрального умовного критерію здійснюватиметься для усіх механізмів ЕП стандарту, окрім механізмів ЕП DSA, KCDSA, Pointcheval/Vaudenay та SDSA, тобто механізмів, що ґрунтуються на математичному апараті скінченних полів.

Таблиця 1

Результати порівняння щодо безумовних критеріїв

Критерій ЕП / Алгоритм ЕП	$\underline{W_{d1}}$	$\underline{W_{d2}}$	$\underline{W_{d3}}$	$\underline{W_{d4}}$	$\underline{W_{d5}}$	$\underline{W_{d6}}$	$\underline{W_{d7}}$	$\underline{W_{d}}$
DSA	0	1	0	1	0	1	1	0
KCDSA	0	1	0	1	0	1	1	0
Pointcheval/Vaudenay	0	1	0	1	0	1	1	0
SDSA	0	1	0	1	0	1	1	0
EC-DSA	1	1	1	1	1	1	1	1
EC-KCDSA	1	1	1	1	1	1	1	1
EC-GDSA	1	1	1	1	1	1	1	1
EC-RDSA	1	1	1	1	1	1	1	1
EC-SDSA	1	1	1	1	1	1	1	1
EC-FSDSA	1	1	1	1	1	1	1	1
IBS-1	1	1	1	1	1	1	1	1
IBS-2	1	1	1	1	1	1	1	1

Оцінка механізмів ЕП згідно з ДСТУ ISO/IEC 14888-3:2014 за умовними критеріями

Якщо 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.

Таблиця 2

Шкала відносин (ступеня значущості дій)

Ступінь значущості	Визначення	Пояснення
1	Однакова значущість	Дві дії роблять однаковий внесок у досягнення мети
3	Деяка перевага значущості однієї дії над іншою (слабка значущість)	Існують розуміння на користь переваги однієї з дій, однак ці розуміння недостатньо переконливі
5	Істотна або сильна значущість	Є надійні дані або логічні судження для того, щоб показати перевагу однієї з дій
7	Очевидна або дуже сильна значущість	Переконливе свідчення на користь однієї дії перед іншою
9	Абсолютна значущість	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 i порівняно з дією j приписується одне з визначених вище ненульових чисел, то дії j порівняно з дією i приписується зворотне значення	Якщо узгодженість була постульованою під час одержання N числових значень для утворення матриці

Проведені дослідження показали, що якісне та кількісне порівняння криптографічних перетворень типу ЕП можна здійснити, використовуючи узагальнений умовний критерій переваги [3, 5] або інтегральний умовний критерій.

Як основні часткові умовні критерії пропонується використовувати такі:

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, зокрема 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 ступенем поширення застосування та визнання у різних державах і міжнародно визнаних системах, зокрема 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 складності апаратної, апаратно-програмної та програмної реалізацій засобів ЕП та управління й сертифікації ключів, зокрема 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, зокрема для надання електронних довірчих послуг тощо;

W_{y6} – ступінь гнучкості ЕП з погляду використання у різних додатках, за різних вимог та обмежень у різних умовах, ступінь уніфікації та стандартизації, зокрема для надання електронних довірчих послуг тощо;

W_{y7} – рівень захищеності під час реалізації різних видів загроз, за різних умов здійснення криптоаналітичних атак і відхилення властивостей загальних параметрів від визначених тощо;

W_{y8} – можливість та умови використання під час побудови анонімних підписів для національного та міжнародного застосування та рівень забезпечення анонімності.

Під час їх застосування важливо вибрати метод згортання часткових умовних критеріїв в умовний інтегральний критерій. Проведений аналіз та практичні дослідження показали [5], що як методи згортання часткових умовних критеріїв можна вибирати метод аналізу ієрархій на основі попарних порівнянь та метод визначення вагових коефіцієнтів.

Під час використання методу аналізу ієрархій на основі попарних порівнянь отримані судження виражаються у цілих числах з урахуванням дев'ятибальної шкали (табл. 2) [3, 5].

Метод аналізу ієрархій на основі попарних порівнянь та особливості його застосування для оцінки алгоритмів ЕП

Для застосування методу аналізу ієрархій необхідно вибрати систему умовних критеріїв. За допомогою такої множини показників, засобом застосування умовних критеріїв можна обчислити значення інтегрального умовного критерію, та, як наслідок, зробити порівняння ЕП за умовним інтегральним критерієм.

Метод попарного порівняння елементів [3, 5, 8, 17] можна описати так. Будується множина матриць парних порівнянь. Парні порівняння проводяться у термінах домінування одного елемента над іншим. Отримані судження виражаються у цілих числах з урахуванням дев'ятибальної шкали у табл. 2 [3, 5].

Під час побудови матриці попарних порівнянь для усіх критеріїв необхідно визначити відношення узгодженості [5] для кожного з критеріїв так.

Оцінку компоненти власного вектора вирахуємо за формулою (3):

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

Нормалізовану оцінку вектора пріоритету вирахуємо за формулою (4):

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

де z – відношення узгодженості матриці, яке обчислюється за формулою (5):

$$z = \sum_{i=1}^{n} q_i. \quad (5)$$

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 попарних порівнянь у криптографії.
Порівняльний аналіз механізмів ЕП згідно з ДСТУ ISO/IEC 14888-3:2014

Розглянемо практичне застосування методу аналізу ієрархій на основі попарних порівнянь на прикладі механізмів ЕП згідно зі стандартом ДСТУ ISO/IEC 14888-3:2014.

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

Тепер зробимо оцінку кожного критерію. Для цього побудуємо матрицю попарних порівнянь щодо порівнюваних алгоритмів ЕП для кожного критерію (табл. 3).

Таблиця 3

Внесок критеріїв у досягнення загальної мети.
Матриця попарних порівнянь

	W_{y1}	W_{y2}	W_{y3}	W_{y4}	W_{y5}	W_{y6}	W_{y7}	W_{y8}	q_j	r_j
W_{y1}	1	1/6	4	1/4	1/2	1/3	1/7	3	0,575	0,048
W_{y2}	6	1	4	5	4	3	1/7	5	2,38	0,198
W_{y3}	1/4	1/4	1	3	2	1/2	1/7	1	0,636	0,053
W_{y4}	4	1/5	1/3	1	1/4	1/4	1/7	1/6	0,376	0,031
W_{y5}	2	1/4	1/2	4	1	1/3	1/7	1/4	0,575	0,048
W_{y6}	3	1/3	2	4	3	1	1/7	1	1,167	0,097
W_{y7}	7	7	7	7	7	7	1	7	5,489	0,456
W_{y8}	1/3	1/5	1	6	4	1	1/7	1	0,832	0,069

Відношення узгодженості дорівнює 12,03.

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

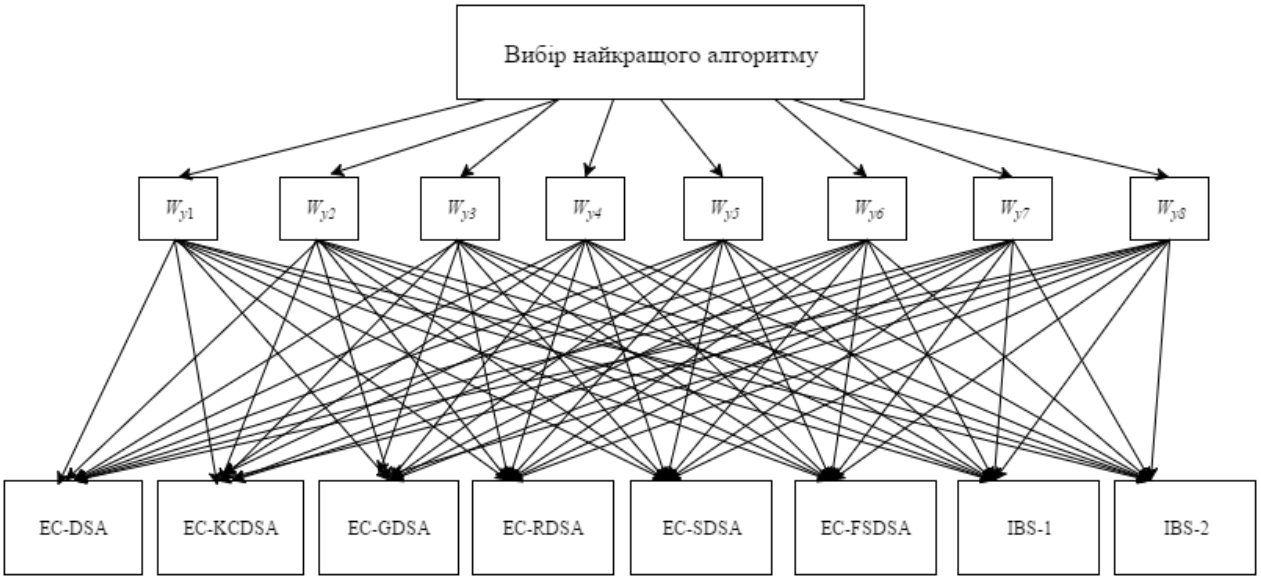

Рис. 1. Дерево цілей

Відношення узгодженості дорівнює 9,54.

Таблиця 4

Матриця попарних порівнянь за критерієм W_{y1}

	EC-DSA	EC-KCDSA	EC-GDSA	EC-RDSA	EC-SDSA	EC-FSDSA	IBS-1	IBS-2	q_j	r_j
EC-DSA	1	1	1	5	3	3	2	2	1,914	0,201
EC-KCDSA	1	1	1	5	3	3	2	2	1,914	0,201
EC-GDSA	1	1	1	5	3	3	2	2	1,914	0,201
EC-RDSA	1/5	1/5	1/5	1	1/3	1/3	1/5	1/5	0,278	0,029
EC-SDSA	1/3	1/3	1/3	3	1	1	1/2	1/2	0,639	0,067
EC-FSDSA	1/3	1/3	1/3	3	1	1	1/2	1/2	0,639	0,067
IBS-1	1/2	1/2	1/2	5	2	2	1	1	1,121	0,118
IBS-2	1/2	1/2	1/2	5	2	2	1	1	1,121	0,118

Для обчислення результуючого вектора пріоритетів перемножимо вектор пріоритетів 1 рівня і матрицю набутих значень 1 рівня (рис. 2).

$$v := \begin{pmatrix} 0.048 \\ 0.198 \\ 0.053 \\ 0.031 \\ 0.048 \\ 0.097 \\ 0.456 \\ 0.069 \end{pmatrix} \qquad M := \begin{pmatrix} 0.201 & 0.087 & 0.082 & 0.076 & 0.166 & 0.21 & 0.051 & 0.205 \\ 0.201 & 0.169 & 0.165 & 0.061 & 0.166 & 0.229 & 0.102 & 0.19 \\ 0.201 & 0.124 & 0.165 & 0.103 & 0.166 & 0.192 & 0.086 & 0.19 \\ 0.029 & 0.025 & 0.021 & 0.05 & 0.049 & 0.027 & 0.02 & 0.028 \\ 0.067 & 0.054 & 0.06 & 0.08 & 0.099 & 0.043 & 0.036 & 0.047 \\ 0.067 & 0.054 & 0.06 & 0.08 & 0.099 & 0.043 & 0.036 & 0.047 \\ 0.118 & 0.244 & 0.233 & 0.275 & 0.128 & 0.129 & 0.334 & 0.147 \\ 0.118 & 0.244 & 0.233 & 0.275 & 0.128 & 0.129 & 0.344 & 0.147 \end{pmatrix}$$

$$V2 := M \cdot v \qquad V2^T = (0.099 \quad 0.144 \quad 0.125 \quad 0.025 \quad 0.048 \quad 0.048 \quad 0.256 \quad 0.256)$$

Рис. 2. Обчислення результуючого вектора пріоритетів

Розглянемо отримані числові результати. Досліджувані алгоритми ЕП, що ґрунтуються на перетвореннях у групі точок ЕК та спарюванні точок ЕК, можна розташувати за місцями, які вони зайняли за результатами порівняння (1 – найкращий, 8 – найгірший):

1. IBS-1 – 0,256; 2. IBS-2 – 0,256; 3. EC-KCDSA – 0,144; 4. EC-GDSA – 0,125; 5. EC-DSA – 0,099; 6. EC-SDSA – 0,048; 7. EC-FSDSA – 0,048; 8. EC-RDSA – 0,025.

Отже, ЕП IBS-1,2 за інтегральним показником мають найбільші переваги. Алгоритм ЕП EC-RDSA має найгірший результат, що обґрунтовується реалізацією атак на цей алгоритм та неможливістю застосування на національному рівні.

Необхідно зазначити, що отримані результати не можна використовувати для застосування, найшвидше це є методика порівняння ЕП. Для реальних використань необхідно відповідно вибрати умовні критерії та провести дослідження.

Методи оцінювання та порівняльного аналізу механізмів ЕП згідно з ДСТУ ISO/IEC 14888-3:2014 на основі визначення вагових коефіцієнтів

У тому випадку, коли отримати дані про важливість параметрів порівнюваних систем із використанням неформальних методів неможливо, необхідно використовувати формалізовані методи. До них належать методи, що ґрунтуються на визначенні вагових коефіцієнтів. Таких методів є кілька [9, 11, 18–20, 22], деякі з них детально розглянуті далі.

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

Нехай є [9, 11, 18–20, 22]:

1) k систем (механізмів ЕП), які необхідно оцінити;

2) m показників, за якими оцінюються системи;

3) n експертів, які проводять оцінювання.

Визначимо деякі 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 у групі точок ЕК та на основі математичного апарата спарювання точок ЕК;

x_3 – перспективність застосування міжнародного або національного стандарту в Україні;

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

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

x_6 – ступінь гнучкості алгоритму ЕП з погляду використання у різних додатках, за різних вимог та обмежень;

x_7 – рівень захищеності від різних видів загроз за різних умов здійснення криптоаналітичних атак;

x_8 – можливість використання алгоритму ЕП під час побудови анонімних підписів для національного та міжнародного застосування та рівень забезпечення анонімності.

Тепер визначимо значення вагових коефіцієнтів самих показників. Для цього проведемо експертне оцінювання вищевказаних часткових показників. Для оцінювання використовуватимемо такі методи визначення вагових коефіцієнтів [9, 11, 18–20, 22]:

1) за допомогою шкали Фішберна;

2) на основі методу ранжування;

3) на основі методу приписування балів;

4) на основі числового способу.

Після того, як було визначене значення вагових коефіцієнтів самих показників, необхідно провести експертне оцінювання систем за вищевказаними методами визначення вагових коефіцієнтів.

Для цього щодо кожної із систем потрібно виконати ранжування показників у зв’язку з тим, який з показників найбільше визначається в обраній системі, краще за інші характеризує її. Тобто упорядкувати показники стосовно обраної системи: від більш значущого до найменш значущого.

Метод визначення вагових коефіцієнтів та оцінки ЕП за допомогою шкали Фішберна

Нехай як вхідні дані вибрано такі:

n – кількість експертів n=5;

m – кількість показників m=8.

Відповідно до правил проведення оцінювання згідно з визначеним методом побудуємо таблицю значень показників методу шкали Фішберна для алгоритмів ЕП стандарту ДСТУ ISO/IEC 14888-3:2014 (EC-DSA, EC-GDSA, EC-KCDSA, EC-RDSA, EC-SDSA, EC-FSDSA, IBS-1 та IBS-2). Результати наведені у табл. 5.

Аналогічно будуємо таблиці для усіх механізмів ЕП згідно з ДСТУ ISO/IEC 14888-3:2014.

Після проведення оцінювання отримаємо результати, показані на рис. 3.

Далі проведемо аналіз отриманих результатів згідно з рис. 3. Для цього розміщаємо значення Rez_Fishbern у міру їх зменшення, тобто:

1. IBS-1 – 0,159; 2. IBS-2 – 0,159; 3. EC-DSA – 0,15; 4. EC-GDSA – 0,147; 5. EC-KCDSA – 0,142; 6. EC-FSDSA – 0,118; 7. EC-SDSA – 0,117; 8. EC-RDSA – 0,106.

Таблиця 5

Значення вагових коефіцієнтів

Експерти	Показники							
	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8
1	0,194	0,167	0,111	0,139	0,056	0,028	0,222	0,083
2	0,194	0,167	0,111	0,083	0,028	0,056	0,222	0,139
3	0,222	0,139	0,111	0,056	0,028	0,083	0,194	0,167
4	0,222	0,111	0,139	0,028	0,083	0,056	0,194	0,167
5	0,167	0,139	0,028	0,056	0,111	0,083	0,222	0,194
w_i	0,200	0,144	0,100	0,072	0,061	0,061	0,211	0,150

Необхідно відзначити, що отримані результати не можна використовувати, швидше за все, це є методика порівняння ЕП. Для реальних використань необхідно вибрати умовні критерії та провести дослідження.

$$M\_Fishbem := \begin{pmatrix} 0.211 & 0.172 & 0.128 & 0.078 & 0.044 & 0.072 & 0.161 & 0.156 \\ 0.2 & 0.189 & 0.144 & 0.05 & 0.056 & 0.094 & 0.128 & 0.139 \\ 0.194 & 0.167 & 0.139 & 0.05 & 0.05 & 0.072 & 0.161 & 0.167 \\ 0.067 & 0.061 & 0.072 & 0.2 & 0.194 & 0.189 & 0.106 & 0.111 \\ 0.061 & 0.05 & 0.056 & 0.167 & 0.172 & 0.167 & 0.167 & 0.161 \\ 0.061 & 0.05 & 0.056 & 0.161 & 0.161 & 0.183 & 0.178 & 0.15 \\ 0.183 & 0.122 & 0.128 & 0.206 & 0.078 & 0.044 & 0.211 & 0.167 \\ 0.183 & 0.122 & 0.128 & 0.206 & 0.078 & 0.044 & 0.211 & 0.167 \end{pmatrix}$$

$$V\_Fishbem := w\_pokaz1$$

$$V\_Fishbem = (0.2 \quad 0.144 \quad 0.1 \quad 0.072 \quad 0.061 \quad 0.061 \quad 0.211 \quad 0.15)$$

$$Rez\_Fishbem := M\_Fishbem \cdot V\_Fishbem^T$$

$$Rez\_Fishbem^T = (0.15 \quad 0.142 \quad 0.147 \quad 0.106 \quad 0.117 \quad 0.118 \quad 0.159 \quad 0.159)$$

Рис. 3. Обчислення результуючого вектора пріоритетів

Метод визначення вагових коефіцієнтів та оцінки ЕП на основі методу ранжування

n – кількість експертів n=5;

m – кількість показників m=8.

Відповідно до правил проведення оцінювання, згідно з визначеним методом побудуємо таблицю для показників (табл. 6).

Таблиця 6

Значення вагових коефіцієнтів

Експерти	Показники							
	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8
1	7	6	5	4	2	1	8	3
2	8	7	5	3	1	2	6	4
3	8	6	4	3	2	1	7	5
4	7	6	3	4	1	2	8	5
5	6	7	5	3	2	1	8	4
$r_j = \sum_{i=1}^{n} r_{ij}$	36	32	22	17	8	7	37	21
w_j	0,2	0,178	0,122	0,094	0,044	0,039	0,206	0,117

Аналогічно будуємо таблиці для усіх механізмів ЕП згідно з ДСТУ ISO/IEC 14888-3:2014.

Після проведення оцінювання отримаємо результати, показані на рис. 4.

Далі проведемо аналіз отриманих результатів згідно з рис. 4. Для цього розміщаємо значення Rez_Ranj у міру їх зменшення, тобто:

1. IBS-1 – 0,147; 2. IBS-2 – 0,147; 3. EC-KCDSA – 0,143; 4. EC-GDSA – 0,142; 5. EC-DSA – 0,139; 6. EC-FSDSA – 0,115; 7. EC-SDSA – 0,111; 8. EC-RDSA – 0,103.

Отже, ЕП IBS-1 та IBS-2 за інтегральним показником мають найбільші переваги. Алгоритм ЕП EC-RDSA (як і у випадку порівняння за методом аналізу ієрархій та методом на основі шкали Фішберна) має найгірший результат, що обґрунтовується реалізацією атак на цей алгоритм та неможливістю застосування на національному рівні.

$$M\_Ranj := \begin{pmatrix} 0.189 & 0.183 & 0.156 & 0.1 & 0.067 & 0.061 & 0.072 & 0.172 \\ 0.189 & 0.161 & 0.122 & 0.056 & 0.072 & 0.094 & 0.15 & 0.156 \\ 0.194 & 0.15 & 0.172 & 0.05 & 0.061 & 0.106 & 0.144 & 0.122 \\ 0.05 & 0.05 & 0.067 & 0.133 & 0.194 & 0.2 & 0.133 & 0.172 \\ 0.05 & 0.061 & 0.056 & 0.167 & 0.167 & 0.167 & 0.167 & 0.167 \\ 0.056 & 0.061 & 0.05 & 0.156 & 0.15 & 0.161 & 0.183 & 0.183 \\ 0.178 & 0.122 & 0.089 & 0.106 & 0.078 & 0.044 & 0.211 & 0.172 \\ 0.178 & 0.122 & 0.089 & 0.106 & 0.078 & 0.044 & 0.211 & 0.172 \end{pmatrix}$$

$$V\_Ranj := w\_pokaz2$$

$$V\_Ranj = (0.2 \quad 0.178 \quad 0.122 \quad 0.094 \quad 0.044 \quad 0.039 \quad 0.206 \quad 0.117)$$

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

$$Rez\_Ranj^{T} = (0.139 \quad 0.143 \quad 0.142 \quad 0.103 \quad 0.111 \quad 0.115 \quad 0.147 \quad 0.147)$$

Рис. 4. Обчислення результуючого вектора пріоритетів

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

n – кількість експертів n=5;

m – кількість показників m=8.

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

Таблиця 7

Значення вагових коефіцієнтів

Показники / Експерти	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	$\sum_{j=1}^{m} h_{ij}$	Ваги показників							
										r_{i1}	r_{i2}	r_{i3}	r_{i4}	r_{i5}	r_{i6}	r_{i7}	r_{i8}
1	7	5	2	4	6	1	10	8	43	0,163	0,116	0,046	0,093	0,139	0,023	0,232	0,186
2	6	5	3	4	9	2	8	7	44	0,136	0,114	0,068	0,091	0,204	0,045	0,182	0,159
3	8	6	1	5	4	3	9	7	43	0,186	0,140	0,023	0,116	0,093	0,070	0,209	0,163
4	7	5	3	8	4	2	9	6	44	0,159	0,114	0,068	0,182	0,091	0,045	0,204	0,136
5	9	6	2	5	4	3	10	7	45	0,196	0,130	0,043	0,109	0,087	0,065	0,217	0,152
									$\sum_{i=1}^{n} r_j$	0,84	0,614	0,248	0,591	0,614	0,248	1,044	0,796
									w_j	0,168	0,123	0,050	0,118	0,123	0,050	0,209	0,159

Аналогічно будуємо таблиці для усіх механізмів ЕП згідно з ДСТУ ISO/IEC 14888-3:2014.

Після проведення оцінювання отримаємо результати, показані на рис. 5.

Далі проведемо аналіз отриманих результатів згідно з рис. 5. Для цього розміщаємо значення Rez_Bal у міру їх зменшення, тобто:

1. IBS-1 – 0,137; 2. IBS-2 – 0,137; 3. EC-RDSA – 0,132; 4. EC-FSDSA – 0,128; 5. EC-DSA – 0,127; 6. EC-SDSA – 0,127; 7. EC-GDSA – 0,126; 8. EC-KCDSA – 0,124.

$$M\_Bal := \begin{pmatrix} 0.193 & 0.169 & 0.146 & 0.076 & 0.065 & 0.101 & 0.095 & 0.156 \\ 0.178 & 0.15 & 0.167 & 0.086 & 0.081 & 0.107 & 0.098 & 0.133 \\ 0.177 & 0.143 & 0.145 & 0.08 & 0.094 & 0.121 & 0.119 & 0.121 \\ 0.065 & 0.046 & 0.04 & 0.167 & 0.177 & 0.127 & 0.119 & 0.259 \\ 0.062 & 0.081 & 0.053 & 0.153 & 0.171 & 0.174 & 0.151 & 0.155 \\ 0.05 & 0.081 & 0.055 & 0.167 & 0.173 & 0.16 & 0.155 & 0.161 \\ 0.193 & 0.142 & 0.142 & 0.066 & 0.047 & 0.075 & 0.2 & 0.134 \\ 0.193 & 0.142 & 0.142 & 0.066 & 0.047 & 0.075 & 0.2 & 0.134 \end{pmatrix}$$

$$V\_Bal := w\_pokaz3$$

$$V\_Bal = (0.168 \quad 0.123 \quad 0.05 \quad 0.118 \quad 0.123 \quad 0.05 \quad 0.209 \quad 0.159)$$

$$Rez\_Bal := M\_Bal \cdot V\_Bal^T$$

$$Rez\_Bal^T = (0.127 \quad 0.124 \quad 0.126 \quad 0.132 \quad 0.127 \quad 0.128 \quad 0.137 \quad 0.137)$$

Рис. 5. Обчислення результуючого вектора пріоритетів

Метод визначення вагових коефіцієнтів та оцінки ЕП на основі числового способу

n – кількість експертів n=5;

m – кількість показників m=8.

Відповідно до правил проведення оцінювання, згідно з визначеним методом побудуємо таблицю для показників (табл. 8). Значення коефіцієнтів обирають із методу на основі шкали Фішберна.

Таблиця 8

Значення вагових коефіцієнтів

Показники / Оцінювання	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8
$x_{i\min}$	0,167	0,111	0,028	0,028	0,028	0,028	0,194	0,083
$x_{i\max}$	0,222	0,167	0,139	0,139	0,111	0,083	0,222	0,194
d_i	0,250	0,333	0,800	0,800	0,750	0,667	0,125	0,571
w_i	0,058	0,078	0,186	0,186	0,175	0,155	0,029	0,133

Аналогічно будуємо таблиці для усіх механізмів ЕП згідно з ДСТУ ISO/IEC 14888-3:2014.

Після проведення оцінювання отримаємо результати, показані на рис. 6.

Далі проведемо аналіз отриманих результатів згідно з рис. 6. Для цього розміщаємо значення Rez_Chisl у міру їх зменшення, тобто:

1. IBS-1 – 0,15; 2. IBS-2 – 0,15; 3. EC-DSA – 0,144; 4. EC-GDSA – 0,141; 5. EC-KCDSA – 0,138; 6. EC-FSDSA – 0,126; 7. EC-SDSA – 0,123; 8. EC-RDSA – 0,109.

У цьому випадку також необхідно зазначити, що отримані результати не можна сприймати як для застосування, найшвидше, це є методика порівняння ЕП. Для реальних використань необхідно у відповідний спосіб вибрати умовні критерії та провести дослідження.

$$M\_Chisl := \begin{pmatrix} 0.065 & 0.075 & 0.131 & 0.196 & 0.131 & 0.229 & 0.075 & 0.098 \\ 0.059 & 0.059 & 0.101 & 0.156 & 0.156 & 0.205 & 0.117 & 0.147 \\ 0.09 & 0.103 & 0.15 & 0.16 & 0.16 & 0.18 & 0.069 & 0.09 \\ 0.166 & 0.147 & 0.166 & 0.055 & 0.055 & 0.055 & 0.178 & 0.178 \\ 0.15 & 0.15 & 0.15 & 0.113 & 0.113 & 0.113 & 0.113 & 0.097 \\ 0.155 & 0.155 & 0.155 & 0.117 & 0.117 & 0.117 & 0.087 & 0.1 \\ 0.095 & 0.05 & 0.158 & 0.18 & 0.21 & 0.168 & 0.032 & 0.108 \\ 0.095 & 0.05 & 0.158 & 0.18 & 0.21 & 0.168 & 0.032 & 0.108 \end{pmatrix}$$

$$V\_Chisl := w\_pokaz4$$

$$V\_Chisl = (0.058 \quad 0.078 \quad 0.186 \quad 0.186 \quad 0.175 \quad 0.155 \quad 0.029 \quad 0.133)$$

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

$$Rez\_Chisl^{T} = (0.144 \quad 0.138 \quad 0.141 \quad 0.109 \quad 0.123 \quad 0.126 \quad 0.15 \quad 0.15)$$

Рис. 6. Обчислення результуючого вектора пріоритетів

Аналіз результатів досліджень ЕП згідно з ДСТУ ISO/IEC 14888-3:2014

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

Можна вважати, що результати оцінювання механізмів ЕП, згідно з ДСТУ ISO/IEC 14888-3:2014, за різними методиками були отримані майже однакові – фактично однаковий порядок розташування механізмів ЕП від найкращого до найгіршого. Числовий розкид значень вагових коефіцієнтів для одного алгоритму є майже незначним, тільки числові значення для механізмів ЕП IBS-1,2 у методі аналізу ієрархій на основі попарних порівнянь відрізняються від значень вагових коефіцієнтів для цих механізмів ЕП за іншими методиками оцінювання, що обґрунтовується сильнішим впливом суб'єктивної думки експертів.

На рис. 7 графічно зображено результати оцінювання механізмів ЕП за різними методами оцінювання.

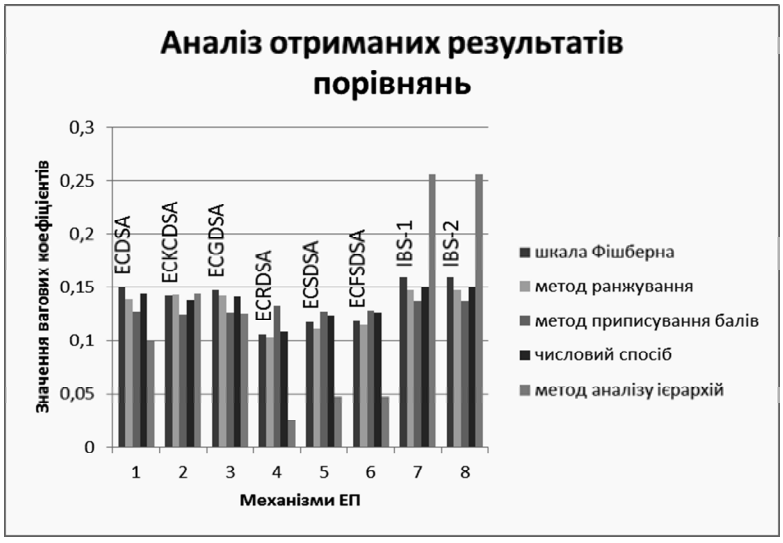

Рис. 7. Результати оцінювання механізмів ЕП за різними методиками

Висновки

1. У зв'язку із специфікою вимог до криптографічних перетворень, зокрема 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 як основний критерій для інтегральної оцінки можна та рекомендується використовувати інтегральний безумовний критерій, який отримують 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 дали змогу зробити висновок, що з погляду об'єктивності оцінювання краще застосовувати метод визначення вагових коефіцієнтів, оскільки в методі аналізу ієрархій на основі попарних порівнянь на результат істотно впливає суб'єктивність експертів.

5. Результати порівняльного аналізу стандартизованих алгоритмів ЕП ДСТУ ISO/IEC 14888-3:2014 дали змогу зробити такі висновки та рекомендації. Максимальне значення умовного інтегрального критерію для ДСТУ ISO/IEC 14888-3:2014 за усіма методами оцінювання досягнуто для алгоритмів IBS-1 та IBS-2.

Результати оцінювання механізмів ЕП згідно з ДСТУ ISO/IEC 14888-3:2014 за різними методиками були отримані майже однакові. Числовий розкид значень вагових коефіцієнтів для одного алгоритму є майже незначним, тільки числові значення для механізмів ЕП IBS-1,2 у методі аналізу ієрархій на основі попарних порівнянь відрізняються від значень коефіцієнтів для цих механізмів ЕП за іншими методиками оцінювання, що зумовлено сильнішим впливом суб'єктивної думки експерта на результат оцінки у визначеному методі.

Згідно з методами оцінювання, на першому місці знаходяться механізми ЕП IBS-1 та IBS-2, а на останньому – механізм ЕП EC-RDSA (тільки для методу визначення вагових коефіцієнтів на основі методу приписування балів на останньому місці розташувався механізм ЕП EC-KCDSA).

Для отримання точніших результатів оцінювання, а також для точного збігу розташування механізмів ЕП за усіма методами оцінювання необхідно виконати процедуру оцінювання кілька разів та ретельно підійти до вибору експертів, що проводитимуть оцінювання.

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 – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms : ISO/IEC 14888-3 (Edition 2 (2006-11-15)) : 2006. – 68 p. 3. Андрейчиков А. В. Анализ, синтез, планирование решений в экономике /А. В. Андрейчиков, О. Н. Андрейчикова. – М. : Финансы и статистика, 2002. – 359 с. 4. Аналитическая иерархическая процедура Саати [Електронний ресурс]. – Режим доступу: http://www.gorskiy.ru/Articles/Dmss/AHP.html. 5. Горбенко Ю. І. Методи побудови та аналізу криптографічних систем: моногр. / Ю. І. Горбенко. – Харків: Форт, 2015. – 959 с. 6. ДСТУ ISO/IEC 9796-3 "Інформаційні технології. Методи захисту. Цифрові підписи, що забезпечують відновлення повідомлення. Частина 2. Механізми, засновані на дискретному логарифмі.", 2016. – 78 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. – (Національні стандарти України). 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 [Електронный ресурс]. – Режим доступу: https://ru.wikipedia.org/wiki/. *11. Методы определения весовых коэффициентов [Електронний ресурс]. – Режим доступу:* http://8v83.tom.ru/. *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// Науковий вісник Національного університету 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. – Науч. изд. 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. – Науч. изд. 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 результатов 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/. *24. Экспертные оценки при разработке решений [Електронний ресурс]. – Режим доступу:* http://books.ifmo.ru/file/pdf/817.pdf.