УДК 004.056.5 **DOI:10.30837/rt.2023.1.212.05**

Ю.І. ГОРБЕНКО, канд. техн. наук, М.В. ЄСІНА, канд. техн. наук,
В.А. ПОНОМАР, канд. техн. наук, І.Д. ГОРБЕНКО, д-р техн. наук, Є.Ю. КАПТЬОЛ

НАУКОВО-МЕТОДИЧНІ ОСНОВИ АНАЛІЗУ, ОЦІНКИ ТА РЕЗУЛЬТАТИ ПОРІВНЯННЯ ІСНУЮЧИХ ТА ПЕРСПЕКТИВНИХ (ПОСТКВАНТОВИХ) АСИМЕТРИЧНИХ КРИПТОГРАФІЧНИХ ПРИМІТИВІВ ЕЛЕКТРОННОГО ПІДПИСУ, ПРОТОКОЛІВ АСИМЕТРИЧНОГО ШИФРУВАННЯ ТА ПРОТОКОЛІВ ІНКАПСУЛЯЦІЇ КЛЮЧІВ

Вступ

Важливою проблемою в криптології є аналіз шляхів зниження ризиків для вразливих криптографічних систем та стану їх розроблення, прийняття та впровадження на міжнародному та національному рівнях постквантових стандартів асиметричних криптоперетворень електронних підписів (ЕП), асиметричних шифрів (АСШ) та протоколів інкапсуляції ключів (ПІК). Тому процеси зниження ризиків для вразливих існуючих стандартизованих криптографічних систем, визначення напрямків розвитку математичних методів та дослідження перспектив їх застосування в ході створення стандартизованих ЕП, АСШ та ПІК є суттєво значимими. Вони зводяться до обґрунтування та визначення математичних методів та механізмів, які дозволять створити перспективні (постквантові) стандартизовані ЕП, АСШ та ПІК [1 – 23].

Підтвердженням наявності ризиків щодо застосування квантових обчислень для злому існуючих асиметричних стандартів криптографічного захисту інформації є прийняття в США закону в формі «Меморандуму про національну безпеку з просування лідерства США в галузі квантових обчислень при одночасному зниженні ризиків для вразливих криптографічних систем» від 04 травня 2022 р. Однак поряд із потенційними перевагами, квантові обчислення також ймовірно будуть становити для економічної та національної безпеки значні ризики.

В подальшому під перехідним періодом будемо розуміти проміжок часу у майбутньому, коли будуть суттєво вдосконалені класичні методи та засоби криптоаналізу, а також будуть створені та застосовуватись для криптоаналізу квантові комп’ютери з обмеженими потужностями. У цей період можуть бути застосованими існуючі стандарти асиметричних та криптографічних перетворень, але з максимально можливими чи збільшеними довжинами загальносистемних параметрів та ключових даних, обмеженою надійністю функціонування. Постквантовий період пропонується визначити як проміжок часу у майбутньому, коли будуть суттєво удосконалені класичні методи та створені квантові комп’ютери з необхідними для успішного криптоаналізу довжинами регістрів (в кубітах) та необхідне для їх реалізації математичне та програмне забезпечення, Вважається, що у постквантовий період квантові комп’ютери будуть працювати з суттєво збільшеною надійністю, тобто з виправленням помилок.

Мета статті – розроблення науково-методичних основ аналізу, оцінки та порівняння існуючих і перспективних (постквантових) асиметричних криптографічних примітивів АСШ, ПІК та ЕП, а також аналіз отриманих практичних результатів.

1. Аналіз стану застосування квантових комп’ютерів для криптоаналізу

Світова цивілізація робить суттєві кроки в науці та практиці, що пов’язані з квантовими обчисленнями; кроки щодо досягнення конкурентної переваги країн в галузі квантової інформаційної науки та практики впровадження квантових технологій. Наукові та практичні дослідження спрямовані перше за все на зниження ризиків, що пов’язані з квантовими комп’ютерами щодо кібербезпеки, економічної та національної безпеки. Визначаються

конкретні дії, які мають зробити технологічно розвинені держави, що розпочинають багаторічний процес переведення вразливих комп'ютерних систем на квантово-стійку криптографію [1, 2, 12, 13]. Здійснюються спроби стимулювання інновацій економіки у сферах від матеріалознавства та фармацевтики до фінансів та енергетики, кібербезпеки тощо. Хоча повний спектр застосування квантових комп'ютерів ще невідомий, проте очевидно, що подальше технологічне та наукове лідерство держав, принаймні частково, буде залежати від здатності країни підтримувати конкурентну перевагу в галузі квантових обчислень та квантової інформаційної науки [1, 2, 6 – 13].

У зв'язку з прийняттям Меморандуму в галузі квантових обчислень Президент США надав півроку на перехід усіх державних органів на постквантову криптографію. Вважається, що квантові обчислення також будуть становити для економічної та національної безпеки США значні ризики. Зокрема, квантовий комп'ютер достатнього розміру та складності – також відомий як криптоаналітично значущий квантовий комп'ютер (КЗКК) – буде здатний зламати більшу частину існуючих стандартизованих криптографічних перетворень з відкритим ключем – АСШ, ПІК та ЕП [1 – 3], що використовується, наприклад, у цифрових системах США та всього світу. Коли він стане доступним для використання, то зможе поставити під загрозу цивільні та військові комунікації, підірвати системи нагляду та контролю за критичною інфраструктурою, а також зруйнувати протоколи безпеки для більшості фінансових операцій в Інтернеті. Переваги та недоліки фізичних реалізацій квантових комп'ютерів:

• масштабованість, тобто можливість створення та управління все більшими і більшими квантовими пристроями зі все більшою кількістю кубітів з використанням фізичних/інженерних ресурсів та керування ними;

• сумісність з різними обчислювальними моделями та простота їх реалізації;

• типовий час декогерентності (тобто скільки часу залишаються збереженими характеристики та вони використані в працездатному стані, а також можуть бути використані квантові особливості, такі як суперпозиції);

• швидкість і точність, з якою вентилі можуть бути застосовано.

Потрібно згодитись, що є проблеми стосовно обґрунтованого вибору фізичної реалізації квантових комп'ютерів.

Високорівневу класифікацію перспективних фізичних реалізацій квантових комп'ютерів можна представити у такому складі [1, 7, 11, 12]:

• квантова оптика, коли інформація зберігається та захищається в станах квантів світла на основі поляризації або в станах з певним числом фотонів, та може бути реалізована в чіпі за допомогою інтегрованої оптики;

• надпровідні системи, коли інформація зберігається та обробляється (захищається) в електричних ланцюгах, які використовують властивості надпровідних матеріалів;

• топологічні системи, коли інформація зберігається та захищається з використанням деяких топологічних властивостей, тобто властивостей, які залежать від «глобальних» (геометричних) властивостей, нечутливих до «локальних» змін – квантових систем;

• іонні пастки, коли інформація зберігається (захищається) та маніпулюється з використанням властивостей іонів (атомів із незникаючим повним електричним зарядом), які обмежені електромагнітними полями;

• квантові спінові системи, коли інформація зберігається та захищається (маніпулюється) у внутрішньому ступені свободи, який називається квантовим спіном. Такі системи можуть бути реалізовані в кремнії як стандартні мікрочіпи, або в менш звичайних системах як алмази з точковими дефектами, відомі як азотно-заміщена (коротше NV) вакансія;

• гази холодних атомів, де нейтральні атоми (а не іони) охолоджуються до значення близького до абсолютного нуля. У той час як іони відштовхуються один від одного через свій електричний заряд, нейтральні атоми цього не роблять, і можуть бути захоплені і організовані в дуже регулярні масиви за допомогою лазерних променів, що створюють так звані оптичні решітки. Атомами можна керувати аж до рівня окремих ділянок в решітці.

Стан створення квантового комп'ютера та можливості вирішення задач криптоаналізу щодо асиметричних криптоперетворень АСШ, ПІК та ЕП можна оцінити наступним чином [1, 7 – 11]:

- IBM розробила та представила квантовий 127-кубітний процесор Eagle. Він прийшов на зміну 65-кубітному квантовому процесору Hummingbird, що відповідає дорожній карті квантових технологій IBM;
- є відомості про наміри IBM представити 433-кубітний процесор Osprey в 2022 р., а 1121-кубітний процесор Condor – в 2023 р.;
- IBM повідомляє про наміри щодо побудови на основі покращених чіпів нової інтегрованої квантової обчислювальної системи IBM Quantum System Two замість існуючої системи IBM Quantum System One;
- компанія D-Wave, що відома розробками псевдоквантових (гібридних) комп'ютерів з великою загальною кількістю кубітів (понад 2000 та понад 5000 кубітів сьогодні), повідомила про наміри представити машину понад 7000 кубітів (2023 – 2024 рр.).

Наведеним даним можна довіряти, але зрозуміло, що фактичний стан розроблення та застосування потужних квантових комп'ютерів є закритим. З іншої сторони, зрозуміло, що створення квантових комп'ютерів здійснюється в умовах суттєвих інвестицій, з випередженням розробки математичних, логічних та програмних основ.

Певний досвід також свідчить. що потрібні інші підходи до підготовки спеціалістів математиків, фізиків, алгоритмістів та програмістів тощо. Навіть використовуючи класичну математику для розробки криптографічно стійких постквантових стандартів, необхідно застосовувати інші математичні методи для асиметричних криптографічних перетворень. Перелік таких методів може зводитися до використання математичних решіток та математичних кодів, математики ізогеній еліптичних кривих, криптографічних перетворень в квадратичних полях (багатовимірних перетворень в квадратичних полях) тощо.

До основних задач криптоаналізу, які можуть бути вирішені на квантовому комп'ютері, необхідно віднести такі [7 – 9]:

- квантовий алгоритм факторизації Шора;
- квантовий алгоритм Гровера пошуку елемента в несортованій базі;
- квантовий алгоритм Шора для розв'язку дискретного логарифму в скінченному полі;
- квантовий алгоритм розв'язку дискретного логарифму в групі точок ЕК Шора тощо.

Окрім класичної криптографії, яка базується на математичних алгоритмах, нині активно розвивається квантова криптографія. Створення квантових комп'ютерів відкриє принципово нові можливості для людства, але при цьому існуючі методи захисту інформації втратять свою ефективність. Не дивлячись на те, що квантові комп'ютери тільки виходять за межі лабораторій, необхідність у використанні квантово безпечної або, як її ще називають, постквантової криптографії є уже сьогодні.

Безпека сучасних інформаційних систем та технологій ґрунтується на стійкості криптографічних перетворень, які використовуються при криптографічному захисті інформації (КЗІ). Криптографічна стійкість КЗІ базується на складності розв'язку певних математичних задач (факторизації великого цілого числа, розв'язку дискретного алгоритму тощо), для таких задач характерна суб'експоненційна або експоненційна складність розв'язку вказаних задач на сучасних (класичних) комп'ютерах. Проте, використовуючи квантові алгоритми Шора та Гровера, певні математичні задачі можна розв'язувати навіть з поліноміальною складністю.

Ідеї використання потужностей квантового середовища висунули Пауль і Фейман. Важливим стало розроблення у 1992 р. Дойчем та іншими першого квантового алгоритму, можливості якого значно перевищували можливості звичайних комп'ютерів. У випадку появи квантового комп'ютера, на якому може бути запущений квантовий алгоритм криптоаналізу Шора або алгоритм пошуку в неупорядкованій базі даних Гровера, можуть виникнути великі загрози у інформаційній сфері відносно забезпечення криптографічної стійкості як для

асиметричних криптоперетворень, так і для певних симетричних. Важливим є не тільки сам факт побудови такого комп'ютера, а й технічні характеристики, якими володітиме квантовий комп'ютер.

В квантовому комп'ютері ключ шифрування передається за допомогою елементарних часток світла – фотонів, тобто внаслідок реалізації квантового протоколу розподілення ключа. Будь-який прилад, за допомогою якого третя сторона спробує перехопити дані, вплине на стан фотона, і ключ стане недійсним. Передавати фотони можна за допомогою виділених оптоволоконних ліній; на обох кінцях такої лінії необхідні спеціальні шифрувальні пристрої. Недоліком квантової криптографії є те, що вона вимагає великих затрат на інфраструктуру. При цьому поки що ключі вдається передавати реально на відстань (50 – 100 км), швидкість їх генерації досить низька, а на передачу фотонів впливає маса зовнішніх факторів.

Постквантова (квантово безпечна) криптографія, як і класична, основана на розв'язку математичних задач. Проте нові алгоритми шифрування повинні бути іншими, щоб їх не могли розв'язати за допустимий час не тільки звичайні, але і квантові комп'ютери.

2. Аналіз стану застосування квантових комп'ютерів для криптоаналізу

Стосовно криптології до основних задач, які можуть бути вирішені на квантовому комп'ютері для криптоаналізу існуючих стандартизованих засобів КЗІ, необхідно, в першу чергу, віднести квантові алгоритми Шора (факторизації, розв'язку дискретного логарифму в скінченному полі та дискретного логарифму в групі точок еліптичних кривих (ЕК)), а також квантовий алгоритм Гровера пошуку елемента в несортованій базі тощо. Нижче наведено їх сутність та складність реалізації.

2.1. Квантовий алгоритм факторизації Шора

Квантовий алгоритм запропонований одним з перших для вирішення задачі факторизації модуля криптоперетворення в кільці, наприклад RSA криптоперетворення. Вирішення вказаної задачі зводиться до факторизації модуля перетворення N, а класичні алгоритми факторизації мають або експоненційну, або суб'експоненційну складність. При цьому вважається, що найкращим за критерієм мінімуму складності факторизації є алгоритм загального решета числового поля та при деяких обмеженнях його модифікації – спеціальні решета числового поля. У той же час алгоритм Шора, що орієнтований на квантовий комп'ютер, має поліноміальну складність. При його застосуванні факторизацію можна здійснити зі складністю

$$O(n^3) \qquad (1)$$

та з використанням $O(n)$ кубітів.

Порівняльний аналіз складності факторизації для класичного та квантового алгоритмів наведено у табл. 1.

Таблиця 1

Порівняльний аналіз класичного та квантового алгоритмів факторизації (RSA)

Розмір модуля N, бітів	Кількість необхідних кубітів $2n$	Складність квантового алгоритму $4n^3$	Складність класичного алгоритму
512	1024	$0.54 \cdot 10^9$	$1.6 \cdot 10^{19}$
3072	6144	$12 \cdot 10^{10}$	$5 \cdot 10^{41}$
15360	30720	$1.5 \cdot 10^{13}$	$9.2 \cdot 10^{80}$

Аналіз даних табл. 1 показує, що для зламу RSA криптосистеми з розміром модуля у 15360 бітів (а це розмір відкритого ключа сертифікату США), необхідно лише $1.5 \cdot 10^{13}$ операцій на квантовому комп'ютері, тоді як з використанням існуючих класичних обчислювальних систем потрібно виконати приблизно 1080 операцій.

Таким чином, якщо з'явиться квантовий комп'ютер з відповідними характеристиками та параметрами, RSA система буде зламана за поліноміальний час.

2.2. Квантовий алгоритм Шора дискретного логарифмування в скінченному полі

Існує декілька методів та алгоритмів дискретного логарифмування в скінченному полі [19]. Вважається, що найкращим класичним алгоритмом дискретного логарифмування в скінченному полі є метод решета числового поля. Для нього складність можна оцінити як суб'експоненційну [19]:

$$O(exp(3^{3/2}(ln(P)ln(ln(P)))^{1/3}). \quad (2)$$

Як слідує із вказаних джерел, класичні методи криптоаналізу дискретного логарифмування в скінченному полі мають суб'експоненційну складність. Алгоритм Шора має поліноміальну складність дискретного логарифмування, що дозволяє вирішити проблему дискретного логарифму в скінченному полі з суттєво меншою складністю [15]. Порівняльний аналіз складності алгоритму дискретного логарифмування в скінченному полі на основі решета числового поля та алгоритму Шора наведено в табл. 2.

Таблиця 2

Порівняльний аналіз класичного і квантового алгоритму дискретного логарифмування в скінченному полі

Розмір модуля перетворення (бітів)	Кількість необхідних кубітів $\approx 3n$	Час квантового алгоритму $\approx n^3$	Час класичного алгоритму
1024	3072	$0.1 \cdot 10^{10}$	$3.3 \cdot 10^{20}$
3072	9216	$2.9 \cdot 10^{10}$	$1.4 \cdot 10^{31}$
15360	46080	$3.6 \cdot 10^{12}$	$5.9 \cdot 10^{56}$

Аналіз даних табл. 2 дозволяє зробити висновок, що збільшення розміру модуля перетворення і, відповідно особистого ключа, при застосуванні квантового алгоритму Шора не забезпечує необхідного збільшення складності дискретного логарифмування в скінченному полі, як при зламі ЕП, так і АСШ (ПІК). Наприклад, для модуля $P \geq 2^{3072}$ складність дискретного логарифмування в скінченному полі складає $1.4 \cdot 10^{31}$, а із застосуванням алгоритму Шора – всього $2.9 \cdot 10^{10}$ операцій. Але, в той же час, при застосуванні квантового алгоритму проблемною є реалізація регістрів зі значним числом кубітів – не менше 9216 кубітів. Очевидно, досягти такого розміру буде ще певний час проблемою.

2.3. Квантовий алгоритм Шора дискретного логарифмування в групі точок еліптичних кривих

Квантовий алгоритм Шора дискретного логарифмування в групі точок еліптичних кривих суттєво схожий за складністю зі складністю алгоритму Шора дискретного логарифмування в скінченному полі. Так, алгоритм Шора для групи точок ЕК має однакові кроки, відмінність в поданні; замість елементів поля потрібно розглядати точки ЕК. Розглянемо їх криптографічну стійкість та зробимо відповідні оцінки для них.

Вважається, що задачі дискретного логарифмування в групі точок еліптичних кривих найбільш ефективно можуть бути вирішені з використанням ρ- та λ-методів Полларда [20, 21]. Для них складність можна оцінити як

$$O(\sqrt{q}), \quad (3)$$

де q – число точок еліптичної кривої.

Визначено, що квантовий алгоритм Шора у загальному випадку має поліноміальну складність вирішення такого класу задач. Він також може бути застосований для розв'язку дискретного логарифмічного рівняння, причому його часова складність може бути оцінена як $O(n^3)$, де n – порядок базової точки ЕК. Деякі оцінки та результати порівняльного аналізу класичних алгоритмів та квантового алгоритму Шора наведено у табл. 3.

Таблиця 3

Порівняльний аналіз складності класичного і квантового алгоритмів дискретного логарифмування групі точок еліптичної кривої (ECC)

Алгоритм розв'язку дискретного логарифмічного рівняння			
Розмір порядку базової точки, бітів	Кількість необхідних кубітів $f(n)=7n+4\log_2 n+10$	Складність квантового алгоритму $360n^3$	Складність класичного алгоритму
163	1210	$1.6\cdot10^9$	$3.4\cdot10^{24}$
256	1834	$6\cdot10^9$	$3.4\cdot10^{38}$
571	4044	$6.7\cdot10^{10}$	$8.8\cdot10^{85}$
1024	7218	$3.8\cdot10^{11}$	$1.3\cdot10^{154}$

Аналіз даних табл. 3 дозволяє зробити висновок, що збільшення розміру порядку базової точки при криптоаналізі з використанням квантового алгоритму не дає суттєвого збільшення криптографічної стійкості криптографічної системи на еліптичних кривих. Також видно, що при збільшенні модуля складність дискретного логарифмування класичними методами в групі точок еліптичної кривої зі збільшенням порядку базової точки збільшується суттєво. Але потрібно взяти до уваги, що реалізація квантового алгоритму пов'язана із застосуванням регістрів з великою кількістю кубітів, яка необхідна для проведення квантової атаки. Наприклад, для базової точки з порядком 2^{571} необхідно використовувати реєстр з довжиною 4016 кубітів. Вважається, що така велика кількість кубітів певний час не може бути реалізована з необхідною надійністю його функціонування.

2.4. Квантовий алгоритм Гровера та його використання

Проблему криптоаналізу, на вирішення якої спрямовано метод Гровера, може бути сформульовано наступним чином. Нехай дано неупорядковану базу даних (список) з N елементів і нехай в ній існує один елемент, що володіє деякою властивістю, яка перевіряється з поліноміальною складністю. Потрібно знайти цей елемент із мінімально можливою складністю і, зрозуміло, за менший час.

Для пошуку скористаємося математичним апаратом узагальненого «парадоксу про день народження». Основними умовами застосування цієї моделі є випадковість та рівноймовірність здійснення запитів, тобто вхідних даних. Тому при виконанні k запитів ймовірностей успіху можна оцінити як k/N [20, 21]. Значить, щоб знайти необхідний елемент з будь-якою наперед заданою ймовірністю, необхідно зробити до бази $O(N)$ запитів. Алгоритм Гровера якраз і дозволяє знайти необхідний елемент з ймовірністю достатньо близькою до 1 за

$$O(\sqrt{N}) \tag{4}$$

кроків, кожен з яких є ітерацією при виконанні процедури. В цілому квантовий комп'ютер дозволяє вирішити цю задачу за

$$O(\sqrt{N}\log N) \tag{5}$$

кроків, використовуючи $\log N$ кубітів, причому $\log N$ кроків необхідно для виконання перетворення Уолша – Адамара [4, 6].

Вирішення цієї задачі може бути виконане з використанням декількох класичних алгоритмів, в яких для підвищення ймовірності успіху процедура повторюється багатократно. При цьому при повторенні такої квантової процедури ймовірність успіху, як правило, збільшується, але після достатньої великої кількості повторень результат знову стає гіршим. Вказане пояснюється тим, що квантова процедура це унітарне перетворення, яке здійснює поворот в комплексному просторі. Внаслідок цього застосування квантового перетворення спочатку, протягом якогось числа ітерацій, можна наближати поточний стан все ближче і ближче до потрібного нам стану, але в подальшому застосування квантового перетворення може оминути потрібний стан і тому віддалити правильне рішення. Для того щоб отримати

при повторюваних квантових перетвореннях результат, що очікується, дуже важливо визначити, коли потрібно зупинитися і провести уточнення.

Наприклад, використовуючи алгоритм Гровера, можна знайти секретний ключ симетричного шифрування чи гешування за $\sqrt{N}$ ітерацій, де N – розмір простору ключів. У якості прикладу в табл. 4 наведено оцінки стійкості симетричних криптографічних систем проти квантового криптоаналізу. Аналіз даних таблиці показує, що стійкість симетричних шифрів при атаці з використанням квантового алгоритму Гровера суттєво зменшується.

Таблиця 4

Стійкість симетричних криптосистем проти квантового криптоаналізу

Вид криптосистеми	Розмір блоку/ключа (біт)	Обсяг пам'яті, яка необхідна для здійснення атаки (блок повідомлення/ключ), кубіт	Стійкість при атаці на	
			блок повідомлення	ключ
AES-128	128/128	128/128	264 (1019,2)	264 (1019,2)
AES-256	128/256	128/256	264 (1019,2)	2128 (1038,4)
DES	64/56	64/56	232 (109,6)	228 (108,4)
TDES	64/168	64/168	232 (109,6)	2134 (1040,2)
ГОСТ-28147	64/256	64/256	232 (109,6)	2128 (1038,4)
Калина-128	128/128	128/128	264 (1019,2)	264 (1019,2)
Калина-512	512/512	512/512	2256 (1076,8)	2256 (1076,8)

Наприклад, алгоритм шифрування DES буде повністю компрометований і не можна говорити про деяку його стійкість, так як оцінка приймає значення 2^{28}. Також із таблиці видно, що навіть для AES-128 та Калина-128 з використанням квантового комп'ютера можна було б знайти секретний ключ за час приблизно 2^{64}. Але значення 2^{64} нині уже може вважатись небезпечним. Видно, що при довжині ключа 256 біт, що стосується AES-256 біт та Калини-2, часова складність роботи алгоритму Гровера становить 2^{128}, що є практично не здійсненним при нинішніх поглядах та можливостях реалізації. Дані відносно шифру ДСТУ 28157-2009 (ГОСТ 28147-89) показують, чому коротка довжина блоку в 64 бітів не може використовуватись, хоча довжина ключа для нього складає 256 бітів, оскільки стійкість на блок повідомлення складає 2^{32}, а при атаці на ключ – 2^{128}. Таким чином, алгоритм Гровера дозволяє реалізувати алгоритм узагальненого парадоксу про день народження.

3. Науково-методичні основи аналізу, оцінки та порівняння існуючих та перспективних (постквантових) стандартизованих асиметричних криптоперетворень

3.1. Призначення та застосування комплексної методики оцінки, аналізу та порівняння криптографічної стійкості та властивостей існуючих та постквантових АСШ, ПІК та ЕП

Комплексна методика безпосередньо призначена для використання при оцінці, аналізі та порівнянні криптографічної стійкості та властивостей існуючих та постквантових АСШ, ПІК та ЕП. Ця методика може бути у явному вигляді застосована при дослідженнях, оцінці та порівнянні існуючих стандартизованих та альтернативних криптографічних примітивів типу АСШ, ПІК та ЕП, включаючи перспективні криптографічні примітиви АСШ, ПІК та ЕП.

Методика аналізу існуючих та постквантових АСШ, ПІК та ЕП є комплексною та визначає три наступні методики оцінки та порівняння:

- криптографічної стійкості існуючих та постквантових АСШ, ПІК та ЕП на основі використання безумовних критеріїв стійкості;
- існуючих та постквантових АСШ, ПІК та ЕП на основі використання умовних критеріїв;
- властивостей існуючих та постквантових АСШ, ПІК та ЕП на основі прагматичних критеріїв.

Ці методики можуть застосовуватись незалежно одна від одної, але основним є застосування їх у вказаній послідовності – спочатку з використанням на основі безумовних критеріїв, потім – на основі умовних критеріїв та при необхідності на основі прагматичних критеріїв.

Методика може бути застосована:

- при обґрунтуванні та розробленні порядку застосування методик оцінки та порівняльного аналізу асиметричних існуючих та перспективних, в тому числі стандартизованих, криптографічних примітивів АСШ, ПІК та ЕП;
- обґрунтуванні та виборі критеріїв та показників оцінки криптографічної стійкості та інших властивостей, в тому числі стандартизованих криптопримітивів типу АСШ, ПІК та ЕП;
- оцінці, аналізі та порівнянні асиметричних існуючих та перспективних постквантових, в тому числі стандартизованих, криптографічних примітивів АСШ, ПІК та ЕП на основі застосування безумовних критеріїв;
- оцінці, аналізі та порівнянні асиметричних існуючих та перспективних, в тому числі стандартизованих, криптопримітивів АСШ, ПІК та ЕП на основі застосування умовних критеріїв;
- оцінці, аналізі та порівнянні асиметричних існуючих та перспективних, в тому числі стандартизованих, криптопримітивів АСШ, ПІК та ЕП на основі застосування прагматичних критеріїв;
- обґрунтуванні та виборі основних методів експертного оцінювання криптографічної стійкості та інших властивостей існуючих та постквантових, в тому числі стандартизованих, криптопримітивів типу АСШ, ПІК та ЕП;
- реалізації методу ієрархій на основі попарних порівнянь та врахуванні особливостей його застосування для оцінки та порівняння властивостей існуючих та постквантових криптографічних примітивів АСШ, ПІК та ЕП;
- обґрунтуванні та виборі для оцінки та порівняльного аналізу існуючих та перспективних криптопримітивів АСШ, ПІК та ЕП, в тому числі стандартизованих, методу вагових коефіцієнтів;
- розробці рекомендації щодо оцінки та порівняння альтернативних криптопримітивів типу АСШ, ПІК та ЕП за прагматичними техніко-економічними та техніко-експлуатаційними критеріями.

3.2. Аналіз стану розроблення та застосування науково-методичних основ комплексної методики оцінки, аналізу

Методики оцінювання та порівняльного аналізу криптопримітивів базуються на використанні системи безумовних та умовних часткових та інтегральних критеріїв, прагматичних критеріїв, а також показників, які дозволяють оцінити ступінь виконання висунутих до криптоперетворення вимог. На наш погляд, основним завданням таких методик є формалізація процесів прийняття рішень відносно виконання висунутих до них вимог, врахування переваг та недоліків криптопримітивів, що є кандидатами на постквантовий стандарт, зменшення впливу суб'єктивних факторів на прийняття рішень, в тому числі несанкціонованого впливу сторонніх організацій тощо. Наприклад, такі методики можуть бути застосованими щодо оцінки та порівняння алгоритмів АСШ, ПІК та ЕП, що є в нашому випадку кандидатами на постквантовий стандарт.

На формальному рівні такі методики оцінки та порівняння алгоритмів АСШ, ПІК та ЕП можуть бути узагальненими (базовими, комплексними). Але, оскільки до названих криптопримітивів висуваються різні вимоги, то для кожного із примітивів вони можуть доповнятись чи спрощуватись та відображати весь спектр висунутих вимог. Також такі методики можуть забезпечити прозорість прийняття рішень, незалежність експертів та допомогти обґрунтувати прийняття відповідних рішень та довіру до них. В подальшому під

методикою для наших досліджень будемо розуміти фіксовану сукупність прийомів практичної діяльності щодо аналізу криптографічної стійкості та властивостей нових, доказовостійких криптоалгоритмів і протоколів, у тому числі у перехідний та постквантовий періоди, що відповідає наведеним вище вимогам та призводить до заздалегідь визначеного результату.

3.3. Обґрунтування та вибір критеріїв та показників оцінки та порівняння рівнів існуючих та перспективних АСШ, ПІК та ЕП на основі комплексної методики

Під критерієм будемо розуміти ознаку, на основі якої здійснюється оцінка, визначення чи класифікація чого-небудь, тобто, будемо розуміти мірило оцінки. Наші попередні дослідження дозволили зробити висновок, що порівняння криптопримітивів можна здійснити з використанням двох сукупностей критеріїв: безумовних та умовних. Такий підхід дозволяє зробити оцінку та порівняння криптопримітивів, що є кандидатами на постквантові стандарти, за частковими та інтегральним умовним критерієм. Такий підхід ґрунтується, в тому числі, і на врахуванні чи використанні експертних оцінок.

На першому етапі перевіряється відповідність криптопримітиву системі часткових безумовних критеріїв, а потім для кожного криптопримітиву на основі часткових обчислюється безумовний інтегральний критерій.

На другому етапі отримуються відповідні оцінки з використанням спочатку системи часткових умовних критеріїв, а потім на їх основі обчислюється інтегральний умовний критерій.

На третьому етапі отримуються відповідні оцінки з використанням системи прагматичних критеріїв.

Такий підхід дозволяє відкинути криптоперетворення, що не відповідають безумовним вимогам, тобто вимогам, які повинні бути виконані безумовно. Причому інтегральний безумовний критерій дозволяє прийняти рішення відносно кожного із криптопримітивів. У нашому випадку це різні криптопримітиви АСШ, ПІК та ЕП.

Застосування часткових умовних критеріїв, а потім на їх основі інтегрального умовного критерію, дозволяє оцінити якість криптопримітиву у широкому сенсі як якість у середньому, а потім і порівняти криптопримітиви, що є кандидатами на постквантовий алгоритм.

До безумовних критеріїв будемо відносити ті, виконання яких для криптопримітиву є обов'язковим. Причому, на наш погляд, для асиметричних криптоперетворень типу АСШ, ПІК та ЕП можна вибрати однакову систему безумовних критеріїв. Але це не виключає можливостей врахування особливостей вимог та відповідно вибору при аналізі та оцінці криптопримітивів додаткових часткових безумовних критеріїв. Розглянемо та виберемо систему часткових безумовних критеріїв, орієнтуючись на вимоги NIST та певні національні нормативно-правові документи.

До безумовних критеріїв оцінки ПІК можна віднести:

1. Практично реалізований рівень моделі безпеки IK-CPA/CCA2.
2. Криптостійкість (складність криптоаналізу) щодо криптоперетворення ЕП – $W_{ЕП}$, що застосовуються в протоколі ПІК.
3. Криптостійкість (складність криптоаналізу) щодо криптоперетворення інкапсуляції – $W_{ПІК}$, та АСШ – $W_{АСШ}$, що застосовуються в протоколі інкапсуляції та асиметричного шифрування.
4. Криптоживучість ключів щодо криптоперетворення АСШ – $G_{АСШ}$ та АСШ – $W_{АСШ}$ (ЕП – $G_{ЕП}$), що застосовуються в протоколі ПІК (ЕП).
5. Криптоживучість ключів, що застосовуються в протоколі ПІК – $G_{ПІК}$.
6. Захищеність криптопротоколу від раніше переданих повідомлень – $W_{рпп}$.
7. Неспростовності криптоперетворень АСШ – $N_{АСШ}$, що встановлені для криптографічного захисту.

8. Неспростовності криптоперетворень ЕП – $N_{ЕП}$, що встановлені для криптографічного захисту.

9. Новизну ключів АСШ (ЕП) – $W_{кл.}$, що застосовуються в протоколі інкапсуляції ПІК та для АСШ (в кращому випадку використання ключів сеансу).

10. Характеристику ступеню нерозрізнюваності для ключів АСШ, ПІК та ЕП.

Аналіз вимог, що висунуті NIST до часткових безумовних критеріїв асиметричних криптоперетворень типу АСШ, ПІК та ЕП, наш досвід розробки й оцінки властивостей криптоперетворень типу АСШ, ПІК та ЕП тощо, досягнуті результати при практичному розв'язку задач криптоаналізу, в тому числі на основі реалізації алгоритмів квантового криптоаналізу, дозволяють вибрати щонайменше безумовні критерії оцінки АСШ, ПІК та ЕП (в табл. 5).

3.4. Безумовні критерії оцінки криптографічних примітивів

У табл. 5 наведено безумовні критерії оцінки та порівняння АСШ, ПІК та ЕП.

У процесі досліджень число безумовних критеріїв може бути розширеним до переліку, що наведений нижче:

1. Надійність, простота та прозорість математичної бази, що застосовується для АСШ, ПІК та ЕП при криптоперетвореннях. Тобто практична відсутність в порушника можливостей здійснювати відносно ЕП атаки типу «універсальне розкриття» за рахунок недосконалості математичного апарату, що застосовується, чи слабкостей, що можуть бути закладені за рахунок специфічних властивостей загальних параметрів і ключів. При цьому критерієм оцінки надійності математичної бази є той факт, що складність атаки «універсальне розкриття» $I_{ур}$ має експоненційний характер, а критерій ненадійності – суб'експоненційну або поліноміальну складність.

2. Практична захищеність криптоперетворень типу АСШ та ПІК при реалізації алгоритму «семантично безпечного шифрування» від відомих класичних та постквантових атак щодо криптоперетворень АСШ та ПІК, доступу криптоаналітика до 2^{64} обраних шифртекстів, але для моделі безпеки IND-CCA2.

3. Реальна захищеність АСШ, ПІК та ЕП від усіх відомих та потенційно можливих криптоаналітичних атак постквантового періоду. Під захищеністю розуміється той факт, що всі відомі криптоаналітичні атаки типу «повне розкриття» мають експоненційну складність $I_{ес}$, а під критерієм незахищеності – суб'експоненційний $I_{се}$ і нижче характер складності атаки «повне розкриття».

4. Теоретична захищеність криптоперетворень типу АСШ, ПІК та ЕП в постквантовий період проти існуючих силових, аналітичних та спеціальних атак для діючих моделей загроз (мінімум модель EUF-CMA для ЕП та IND-CCA2 для АСШ та ПІК) та складність яких менша, ніж складність атаки типу «повне розкриття».

5. Можливість заміни існуючих стандартизованих криптопримітивів на постквантові АСШ, ПІК та ЕП та застосування в діючих криптосистемах та протоколах в певних умовах та обмеженнях.

6. Статистична безпечність криптоперетворення типу АСШ, ПІК та ЕП. Тобто статистична незалежність результату криптоперетворення (виходу), наприклад АСШ та ПІК (ЕП), від вхідного блоку, що зашифровується (підписується), та особистого ключа, що використовується.

7. Відсутність слабких особистих ключів криптоперетворення типу АСШ та ПІК (ЕП), за яких складність криптоаналітичних атак типу «повне розкриття» та «універсальне розкриття» є меншою, ніж складність атаки «повне розкриття» для інших (не слабких) особистих ключів.

8. Обчислювальна ефективність – складність прямого $I_{пр}$ та зворотного $I_{зв}$ криптоперетворень АСШ, ПІК та ЕП (а також генерування та згортання асиметричних пар ключів) має не вище за поліноміальний характер, а також забезпечення необхідних значень складності

(швидкодії) $I_{пр}$, $I_{зв}$ та $I_{кл}$ при практичному застосуванні в додатках з апаратно-програмною та програмною їх реалізацією.

Таблиця 5

Безумовні критерії оцінки та порівняння АСШ, ПІК та ЕП

Безумовні критерії	Позначення
Надійність, простота та прозорість математичної бази (математичних перетворень), що застосовуються при реалізації постквантових криптоперетворень АСШ, ПІК та ЕП.	W_1
Практична захищеність криптоперетворень типу АСШ та ПІК при реалізації алгоритму «семантично безпечного шифрування» від відомих атак з використанням квантового комп'ютера та доступу криптоаналітика до 2^{64} обраних шифртекстів, але для моделі безпеки IND-CCA2.	W_2
Практична захищеність криптоперетворення типу ЕП від відомих атак з використанням квантового комп'ютера та доступу криптоаналітика до 2^{64} обраних повідомлень, для моделі безпеки EUF-CMA.	W_3
Обґрунтованість реальної стійкості криптоперетворень АСШ, ПІК та ЕП від усіх відомих та потенційно можливих криптоаналітичних атак постквантового періоду на основі використання загальних параметрів та ключів з необхідними розмірами та властивостями (ключі 128 біт квантової безпеки та 256 біт і більше класичної стійкості (безпеки)), включаючи статистичну безпеку.	W_4
Теоретична захищеність криптоперетворень типу АСШ, ПІК та ЕП в постквантовий період проти існуючих силових, аналітичних та спеціальних атак для діючих моделей загроз (мінімум для моделі EUF-CMA для ЕП та IND-CCA2 для АСШ).	W_5
Можливість заміни існуючих стандартизованих криптопримітивів на постквантові та застосування в діючих криптосистемах та протоколах в певних умовах та обмеженнях.	W_6
Обчислювальна ефективність – складність прямого $I_{пр.}$ та зворотного $I_{зв.}$ криптоперетворень АСШ, ПІК та ЕП, а також генерування асиметричних пар ключів $I_{кл.}$ не вище за поліноміальну складність, забезпечення необхідних значень складності (швидкодії) $I_{пр.}$, $I_{зв.}$ та $I_{кл.}$ при практичному застосуванні в додатках з апаратно-програмною та програмною реалізацією.	W_7
Виконання обмежень на мінімальну та максимальну довжини особистих та відкритих ключів, розміри та збитковість шифртексту та ЕП, відсутність слабких особистих ключів для моделей безпеки постквантового періоду EUF-CMA для ЕП та IND-CCA2 для АСШ.	W_8
Обґрунтованість реальної стійкості криптоперетворень АСШ, ПІК та ЕП від усіх відомих та потенційно можливих криптоаналітичних атак постквантового періоду на основі використання загальних параметрів та ключів з необхідними розмірами та властивостями (довжини ключів 256/128, 384/192 та 512/256 біт відповідно класичної стійкості та квантової безпеки (стійкості)).	W_9
Забезпечення захисту від атак на основі сторонніх каналів (наприклад, витоку технічними каналами) та на основі помилок.	W_{10}

9. Виконання обмежень на мінімальну та максимальну довжини особистих та відкритих ключів, розміри та збитковість шифртексту та ЕП, відсутність слабких особистих ключів для моделей безпеки постквантового періоду EUF-CMA для ЕП та IND-CCA2 для АСШ та ПІК.

10. Забезпечення захисту від атак на основі сторонніх каналів (наприклад, вимір складності криптоперетворення, вимір потужності для криптоперетворення, витоку технічними каналами тощо).

11. Забезпечення захисту від атак на основі помилок (наприклад, внесення помилок в процеси прямих та зворотних криптоперетворень, ключів тощо).

Визначається перелік інших безумовних критеріїв, необхідних для дослідження для оцінки АСШ, ПІК та ЕП, наприклад, таких:

$I_{ст.}$ – рівень криптографічної стійкості з використанням безумовних критеріїв;

$l_{в.к.}$ – можливі довжини відкритого ключа;

$l_{о.к.}$ – можливі довжини особистого (секретного) ключа;

$l_{рез.}$ – довжина результату криптоперетворення (збитковість);

$T_{пр.}$ – складність (швидкість) прямого криптоперетворення;

$T_{зв.}$ – складність (швидкість) зворотного криптоперетворення;

$T_{ген.зп.}$ – складність (швидкість) генерування загальних параметрів для відповідного режиму роботи криптоперетворення (у залежності від довжин загальних параметрів та ключів);

$T_{ген.кл.}$ – складність (швидкість) генерування ключа (ключової пари) у залежності від режиму роботи тощо.

З урахуванням наведених вище часткових безумовних критеріїв

$$W_1, W_2, W_3, W_4, W_5, W_6, W_7, W_8, W_9, W_{10}, \quad (6)$$

що наведені в табл. 5, та умови (6) функцію відповідності криптоперетворення вимогам, що викладені вище, запишемо у вигляді інтегрального безумовного критерію:

$$f() = (W_1 \wedge W_2 \wedge W_3 \wedge W_4 \wedge W_5 \wedge W_6 \wedge WW_7 \wedge W_8 \wedge W_9 \wedge W_{10}) \in (1,0), \quad (7)$$

де символ «∧» позначає операцію згідно з (7) кон'юнкції булевих змінних.

Тобто, якість постквантового криптоперетворення АСШ, ПІК та ЕП може бути оцінена з використанням безумовного інтегрального критерію – функції відповідності у вигляді інтегрального безумовного критерію

$$f_{фв}=1, \quad (8)$$

якщо криптоперетворення АСШ, ПІК та ЕП відповідає висунутим вимогам та

$$f_{фв}=0, \quad (9)$$

якщо криптоперетворення АСШ, ПІК та ЕП не відповідає висунутим вимогам.

3.5. Умовні критерії оцінки криптографічних примітивів

Якісну й кількісну оцінку та порівняння криптоперетворень типу АСШ, ПІК та ЕП рекомендується здійснювати з використанням часткових умовних та узагальненого умовного критерію переваги. Розглянемо та визначимо вказані умовні критерії на прикладі АСШ, ПІК та ЕП. У табл. 6 наведено перелік та позначення часткових умовних критеріїв оцінки криптоперетворень типу АСШ, ПІК та ЕП, вимоги до яких висунуті NIST США та ETSI ЄС. Як основні складові узагальненого критерію переваги пропонується використовувати часткові умовні критерії згідно з табл. 6. Ці часткові критерії не є обов'язковими, вони можуть бути змінені, замінені, розширений їх перелік чи взагалі, у залежності від вимог та моделей загроз тощо, відкинуті.

Потрібно підкреслити, що інтегральний умовний критерій є усередним певним чином значенням і ґрунтується на методах експертних оцінок, які розглядаються та обґрунтовуються нижче.

Таблиця 6

Умовні критерії оцінки АСШ, ПІК та ЕП

Умовні критерії	Позначення
Додаткові властивості безпеки: «perfect forward secrecy» (удосконалена пряма безпека); стійкість до атак сторонніми каналами; стійкість до мультиключових атак; стійкість до відмов.	К1
Вимоги до безпеки (стійкості): 1) 128 біт класичної безпеки / 64 біт квантової безпеки (запас стійкості AES-128); 2) 128 біт класичної безпеки / 80 біт квантової безпеки (запас стійкості SHA-256/SHA3-256); 3) 192 біт класичної безпеки / 96 біт квантової безпеки (запас стійкості AES-192); 4) 192 біт класичної безпеки / 128 біт квантової безпеки (запас стійкості SHA-384/SHA3-384); 5) 256 біт класичної безпеки /128 біт квантової безпеки (запас стійкості SHA2-512, SHA3-512).	К2
Додаткові вимоги до стійкості: 1) 512 біт класичної безпеки / 256 біт квантової безпеки (запас стійкості SHA-512/SHA3-512, ДСТУ 7564:2014 – 512 біт); 2) 512 біт класичної безпеки /від 128 до 256 біт квантової безпеки (запас стійкості ДСТУ 7624:2014 (Калина – 512)); 3) 512 біт класичної безпеки / 256 біт квантової безпеки (запас стійкості ДСТУ 7624:2014 (Калина – 512)).	К3

Помилки шифрування. Низький відсоток помилок шифрування ПІК та ЕП.	К4
Можливість багаторазового АСШ, ПІК та ЕП.	К5
Гнучкість: 1) додаткові можливості схеми (оптимізація, неявний обмін ключами тощо); 2) кросплатформеність; 3) можливість розпаралелювання.	К6
Перевірка на коректність. Перевірка правильності опорних та оптимізованих реалізацій.	К7
Перевірка на ефективність: Обчислення часу, що необхідний для генерації ключа, зашифрування, розшифрування, підпису, перевірки підпису, або встановлення ключів (тестування проводиться на оптимізованих версіях).	К8
Умови випробувань: Основні платформи: NIST PQC Reference Platform; Intel x64; Windows або Linux, компілятор GCC. Проведення додаткових тестувань інших умов (8-бітових процесорів, цифрових сигнальних процесорів, виділених CMOS, тощо).	К9
Можливість і умови вільного поширення постквантових криптоперетворень АСШ, ПІК та ЕП.	К10
Рівень довіри до постквантових криптоперетворень АСШ, ПІК та ЕП на різних рівнях застосування.	К11
Перспективність та виправданість застосування постквантових криптоперетворень АСШ, ПІК та ЕП.	К12

3.6. Прагматичні критерії та особливості їх застосування у комплексній методиці

У цьому підрозділі наводиться методика оцінювання за прагматичними критеріями та результати дослідження перспективних стандартизованих криптоперетворень. Вона є третім етапом комплексної методики. Сутність комплексної методики та її третього етапу полягає у наступному.

Відповідно до комплексної методики на перших двох етапах застосовуються умовні методики на основі застосування безумовних та умовних критеріїв. Тобто, на першому етапі спочатку оцінюються та перевіряються криптопримітиви на відповідність системі часткових безумовних критеріїв та на їх основі обчислюється безумовний інтегральний критерій. На другому етапі отримуються оцінки з використанням часткових умовних критеріїв і на їх основі обчислюється інтегральний умовний критерій.

На третьому етапі у залежності від вимог, що висуваються до криптопримітивів, при необхідності потрібно оцінювати та порівнювати альтернативні примітиви за техніко-економічними та техніко-експлуатаційними критеріями (характеристиками). В якості основних рекомендується використовувати такі прагматичні критерії (характеристики) як довжини особистих та відкритих ключів, довжини електронних підписів та довжини блоків, що шифруються, складність (швидкодію) основних прямих та зворотних криптоперетворень ЕП (АСШ, ПІК) тощо, складність генерування (обчислення) ключів та параметрів, а також їх взаємну залежність, у тому числі і у залежності від показників щодо криптостійкості та розмірів параметрів і ключів, а також видів математичних методів, що використовуються для реалізації криптопримітивів тощо. Таким чином, важливістю третього етапу є те, що на ньому здійснюється перевірка відповідності часткових безумовних та умовних критеріїв вимогам, що висунуті щодо них відповідними нормативними документами.

Послідовність оцінювання та порівняння криптопримітивів проводиться у такій послідовності:

1. Аналізу та порівнянню підлягають тільки криптоперетворення, що успішно пройшли тестування згідно з вимогами третього етапу, тобто згідно з безумовними частковими та безумовним інтегральним критеріями.
2. Подальший аналіз проводиться з використанням умовних часткових та інтегрального умовного критеріїв щодо усіх криптопримітивів, що пройшли відбір згідно з безумовними критеріями.
3. Визначається перелік прагматичних критеріїв щодо кожного класу проєктів криптоперетворень – АСШ, ПІК та ЕП.

4. На основі, як правило, експериментальних та в меншій мірі теоретичних оцінок визначаються основні показники щодо техніко-економічних та техніко-експлуатаційних характеристик:

$I_{ст.}$ – рівень криптографічної стійкості АСШ, ПІК (ЕП);

$l_{в.к.}$ – довжина відкритого ключа АСШ, ПІК (ЕП);

$l_{о.к.}$ – довжина особистого ключа АСШ, ПІК (ЕП);

$l_{рез.}$ – довжина АСШ, ПІК (ЕП);

$T_{пр.}$ – складність (швидкість) обчислення АСШ, ПІК (ЕП);

$T_{зв.}$ – складність (швидкість) перевірки АСШ, ПІК (ЕП);

$T_{ген.зп.}$ – складність (швидкість) генерування загальних параметрів АСШ, ПІК (ЕП);

$T_{ген.кл.}$ – складність (швидкість) генерування ключа (ключової пари) АСШ, ПІК (ЕП) тощо з урахуванням особливостей.

5. На основі, як правило, експериментальних та в меншій мірі теоретичних оцінок визначаються залежності необхідних показників між собою щодо їх техніко-економічних та техніко-експлуатаційних характеристик, але з урахуванням криптографічної стійкості.

6. На основі аналізу значень показників, їх залежностей між собою та значень умовних та безумовних критеріїв, що отримані на першому та другому етапах, приймаються рішення про переваги певних кандидатів та розробляються рекомендації щодо прийняття в якості стандартів тих чи інших кандидатів, що підлягали випробовуванням.

7. Наприклад, визначаються:

- залежність довжини відкритого ключа від довжини особистого (закритого) ключа у залежності від математичного методу, який застосовується при побудові асиметричної пари ключа для АСШ, ПІК та ЕП окремо;
- залежність складності генерування відкритого ключа від складності генерування особистого ключа у залежності від математичного методу, який застосовується при побудові асиметричної пари ключа для АСШ, ПІК та ЕП окремо;
- залежність складності генерування загальних параметрів від математичного методу, який застосовується (для АСШ, ПІК та ЕП окремо);
- залежність довжини ЕП від математичного методу, який застосовується при побудові асиметричної пари ключа (для ЕП);
- залежність збитковості АСШ, ПІК від математичного методу, який застосовується (окремо для АСШ та ПІК);
- залежність наведених вище залежностей від виду реалізації (програмна, програмно-апаратна, апаратна тощо).

Очевидно, застосування прагматичної методики необхідне у випадках, коли необхідно забезпечити виконання вимог ТЗ та ТТЗ щодо розмірів ключів та параметрів, складності виконання АСШ, ПІК та ЕП, у залежності від математичного методу та розмірів загальних параметрів та ключів тощо.

Практичні приклади методик з використанням прагматичних критеріїв та показників, та їх використання наведені нижче.

3.7. Приклади критеріїв та вимог NIST.IR 8413 та IT Grundschutz Compedium

Приклади критеріїв та вимог згідно з NIST.IR 8413 [4]:

1. Відповідність моделі безпеки: для АСШ, ПІК – IND-CPA та IND-CCA2; для ЕП – EUF-CMA.
2. Відповідність наборів параметрів категоріям безпеки 1, 2, 3 та 5.
3. Гнучкість, простота та адаптація (відсутність факторів, які могли б перешкодити адаптації) криптоперетворення.
4. Стійкість до атак бічними каналами.
5. Патентна незалежність.
6. Залежність показників криптоперетворення від використовуваного процесора.
7. Розміри параметрів та основних перетворень досліджуваного криптоперетворення.

Приклади критеріїв та вимог згідно з IT Grundschutz Compendium [18]:

1. Забезпечення реалізації захисту від несанкціонованого доступу до ІТ-систем при застосуванні обраного криптографічного алгоритму.

2. Забезпечення реалізації захисту від вразливостей програмного забезпечення або помилок при застосуванні обраного криптографічного алгоритму.

3. Забезпечення запобігання неправильного використання дозволу (авторизації) при застосуванні обраного криптографічного алгоритму.

4. Забезпечення запобігання заперечення (відмови) дій при застосуванні обраного криптографічного алгоритму.

5. Забезпечення реалізації захисту від застосування зловмисного програмного забезпечення при застосуванні обраного криптографічного алгоритму.

6. Забезпечення запобігання відмови в обслуговуванні при застосуванні обраного криптографічного алгоритму.

7. Забезпечення запобігання втрати цілісності конфіденційної інформації при застосуванні обраного криптографічного алгоритму.

8. Забезпечення реалізації визначеної криптографічної концепції при застосуванні обраного криптографічного алгоритму.

9. Забезпечення захисту даних при застосуванні обраного криптографічного алгоритму.

10. Забезпечення використання хмари (при необхідності) при застосуванні обраного криптографічного алгоритму.

11. Забезпечення реалізації механізму виявлення подій, що стосуються безпеки, при застосуванні обраного криптографічного алгоритму.

3.8. Обґрунтування та вибір методів експертного оцінювання та порівняння існуючих та перспективних (постквантових) АСШ, ПІК та ЕП

Під експертними оцінками розуміють метод пошуку і результат застосування методу, що отриманий на основі використання персональної думки експерта або колективної думки групи експертів, а також комплекс логічних і математичних процедур, направлених на отримання інформації від спеціалістів, її аналіз та узагальнення з метою підготовки та вироблення раціональних рішень (рис. 1).

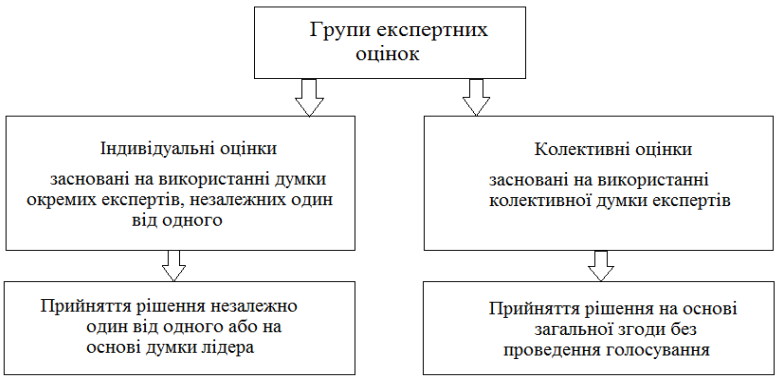

Рис. 1. Схема аналізу груп експертних оцінок

Методи експертних оцінок – це методи організації роботи зі спеціалістами-експертами та обробки думок експертів.

Сутність методів експертних оцінок полягає у покладанні думки спеціаліста або колективу спеціалістів, що заснована на їх знаннях і практичному професійному досвіді, в основу прийнятого рішення, прогнозу, висновку.

Отримали розповсюдження методи експертних оцінок, що виробляються на основі:

- колективних та індивідуальних думок експертів;
- індивідуальних думок експертів;
- колективної роботи групи експертів.

Обґрунтування, вибір та застосування методів експертних оцінок наводяться нижче.

Як правило експертне оцінювання здійснюється у такі етапи:

1) постановка мети дослідження;
2) вибір форми дослідження, визначення бюджету проєкту;
3) підготовка інформаційних матеріалів, бланків анкет, модератора процедури;
4) підбір експертів;
5) проведення експертизи;
6) аналіз результатів (обробка експертних оцінок);
7) підготовка звіту з результатами експертного оцінювання.

В цілому на основі їх аналізу можна зробити висновок, що спільна думка володіє більшою точністю, ніж індивідуальна думка кожного з фахівців. Даний метод застосовують для одержання кількісних оцінок якісних характеристик та вивчення властивостей.

4. Приклади та результати оцінки та порівняння існуючих та перспективних стандартизованих ЕП

4.1. Результати порівняння перспективних механізмів ЕП, що засновані на перетвореннях на алгебраїчних решітках

У табл. 7 наведено характеристики обраних для порівняння алгоритмів (значення швидкості криптоперетворень та генерації ключів наведено в тактах).

Таблиця 7

Характеристики алгоритмів ЕП, що засновані на перетвореннях на алгебраїчних решітках

Алгоритми	$I_{ст.}$	$l_{в.к.}$	$l_{о.к.}$	$l_{рез.}$	$T_{пр.}$	$T_{зв.}$	$T_{гк.}$
Dilithium_round3_sec2	2	1 312	3 504	2 420	259 172	118 412	124 031
Dilithium_round3_sec3	3	1 952	3 856	3 293	428 587	179 424	256 403
Dilithium_round3_sec5	5	2 592	5 792	4595	538 986	279 936	298 050
Вершина_128	3	1 472	3 488	2 693	133 340	109 818	90 328
Вершина_256	5	2 624	5 792	5 345	259 103	233 712	229 669
Вершина_384	7	4 528	9 088	6762	411 040	398 029	317 324
Вершина_512	9	5 824	11 008	10708	643 744	620 989	485 471
Сокіл_128	3	897	4097	666	655 672	139 620	33 696 000
Сокіл_256	5	1 793	8193	1 280	1 338 825	285 714	107 055 000
Сокіл_512	9	3 585	5121	2 515	2 600 053	265 416	28 493 603 229

В порівнянні брали участь проєкти стандартів «Вершина» та «Сокіл», а також алгоритм Dilithium, який за попередніми дослідженнями мав кращі результати серед постквантових алгоритмів підпису, що засновані на перетвореннях на алгебраїчних решітках. Стійкість алгоритмів «Вершини» 128 біт відповідає 3-му рівню стійкості NIST, 256 – 5-му, тому пропорційно для виконання порівняння згідно зі шкалою оцінок попарного порівняння параметрам 384 був наданий 7-й рівень, а 512 – 9-й.

Таблиця 8

Відносна перевага алгоритмів ЕП за кожною з характеристик

Алгоритми	$I_{ст.}$	$l_{в.к.}$	$l_{о.к.}$	$l_{рез.}$	$T_{пр.}$	$T_{зв.}$	$T_{гк.}$
Dilithium_round3_sec2	0,0198	0,1770	0,1816	0,1131	0,1583	0,1857	0,2090
Dilithium_round3_sec3	0,0299	0,0965	0,1475	0,0606	0,0849	0,0984	0,1082
Dilithium_round3_sec5	0,0697	0,0655	0,0768	0,0507	0,0666	0,0506	0,0915
Вершина_128	0,0299	0,1395	0,1816	0,0800	0,3006	0,2195	0,2696
Вершина_256	0,0697	0,0655	0,0768	0,0339	0,1583	0,0716	0,1388
Вершина_384	0,1453	0,0327	0,0407	0,0261	0,0975	0,0348	0,0797
Вершина_512	0,2681	0,0233	0,0296	0,0173	0,0479	0,0218	0,0608
Сокіл_128	0,0299	0,2487	0,1212	0,3211	0,0479	0,1466	0,0192
Сокіл _256	0,0697	0,1108	0,0467	0,1989	0,0238	0,1130	0,0146
Сокіл _512	0,2681	0,0406	0,0973	0,0984	0,0143	0,0581	0,0086

У табл. 8 наведено результати досліджень – відносна перевага алгоритмів ЕП, що отримана методом попарних порівнянь за кожною з характеристик.

На рис. 2 зображено гістограму загальної відносної переваги алгоритмів ЕП з урахуванням вагових коефіцієнтів характеристик.

Як видно, найбільшу перевагу має алгоритм «Вершина» з параметрами стійкості 128 біт.

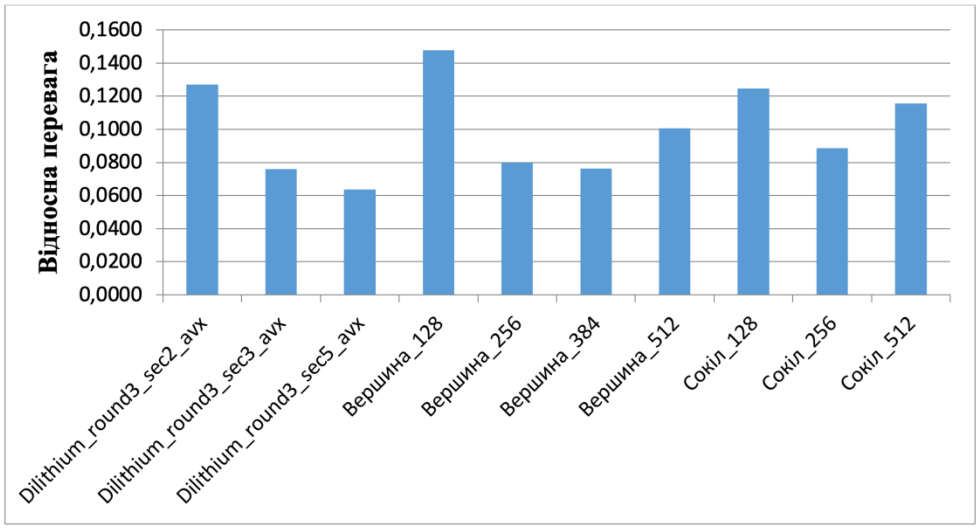

Рис. 2. Переваги алгоритмів ЕП

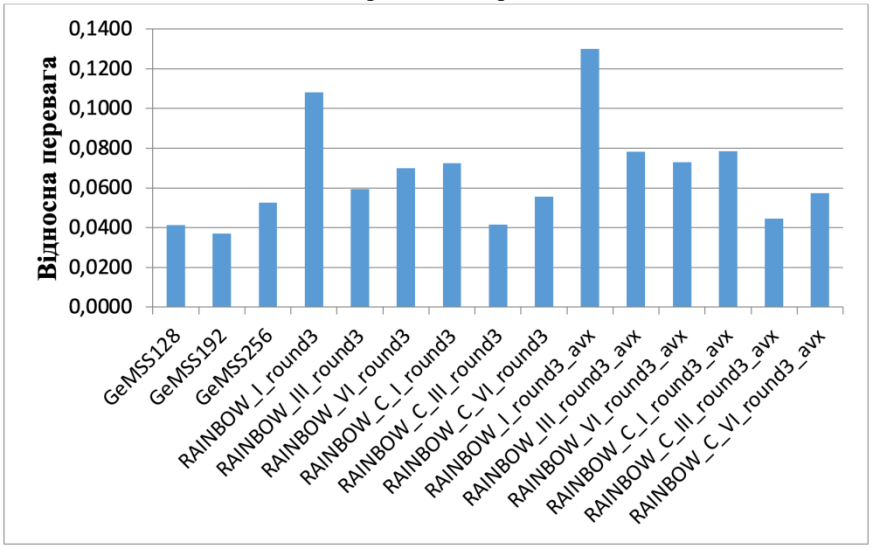

Рис. 3. Переваги алгоритмів ЕП

4.2. Результати кінцевого порівняння перспективних механізмів ЕП

У подальшому порівнювалися алгоритми, що показали кращі результати на попередньому етапі – SPHINCS+_s, «Вершина» та «Сокіл» (через те, що для різних рівнів стійкості перевага у різних алгоритмів), а також Rainbow (оптимізована реалізація зі стандартними параметрами).

У табл. 9 наведено результати досліджень – відносна перевага алгоритмів ЕП, що отримана методом попарних порівнянь за кожною з характеристик.

На рис. 4 відображено гістограму загальної відносної переваги алгоритмів ЕП з урахуванням вагових коефіцієнтів характеристик.

Серед усіх алгоритмів кращий результат у RAINBOW_I_round3_avx (за рахунок малої довжини підпису та великої швидкодії). Але при використані параметрів, що гарантують більшу стійкість, цей алгоритм вже на останньому місці. Якщо ж брати всі можливі параметри алгоритмів, то на першому місці «Вершина» (який в порівнянні з алгоритмами, що засновані на інших математичних апаратах, за сукупністю оцінок обійшов «Сокіл»).

Таблиця 9

Відносна перевага алгоритмів ЕП за кожною з характеристик

Алгоритми	$I_{ст.}$	$l_{в.к.}$	$l_{о.к.}$	$l_{рез.}$	$T_{пр.}$	$T_{зв.}$	$T_{гк.}$
SPHINCS+_128s	0,0155	0,2658	0,2675	0,0189	0,0090	0,0117	0,0164
SPHINCS+_192s	0,0331	0,2289	0,2304	0,0107	0,0090	0,0102	0,0139
SPHINCS+_256s	0,0794	0,1953	0,1984	0,0082	0,0090	0,0079	0,0101
Вершина_128	0,0331	0,0599	0,0664	0,0385	0,2036	0,1525	0,2908
Вершина_256	0,0794	0,0416	0,0433	0,0240	0,1340	0,0713	0,2232
Вершина_512	0,2596	0,0279	0,0274	0,0142	0,0619	0,0305	0,1712
RAINBOW_I_round3_avx	0,0155	0,0117	0,0120	0,2924	0,2864	0,2913	0,0960
RAINBOW_III_round3_avx	0,0331	0,0082	0,0082	0,2043	0,1148	0,1229	0,0500
RAINBOW_VI_round3_avx	0,0794	0,0064	0,0064	0,1746	0,0494	0,0438	0,0263
Сокіл_128	0,0331	0,0770	0,0578	0,1007	0,0619	0,1095	0,0622
Сокіл_256	0,0794	0,0495	0,0337	0,0683	0,0363	0,0898	0,0341
Сокіл_512	0,2596	0,0279	0,0486	0,0451	0,0247	0,0586	0,0057

Тобто, якщо необхідний мінімально задовільний рівень захисту, то кращі результати у Rainbow, а в якості універсального алгоритму краще «Вершина». До того ж, для «Вершини» не були представлені параметри для 1-2 рівнів NIST. Тобто, якщо б були представлені параметри для даних рівнів, то можливо такі параметри обійшли б і Rainbow.

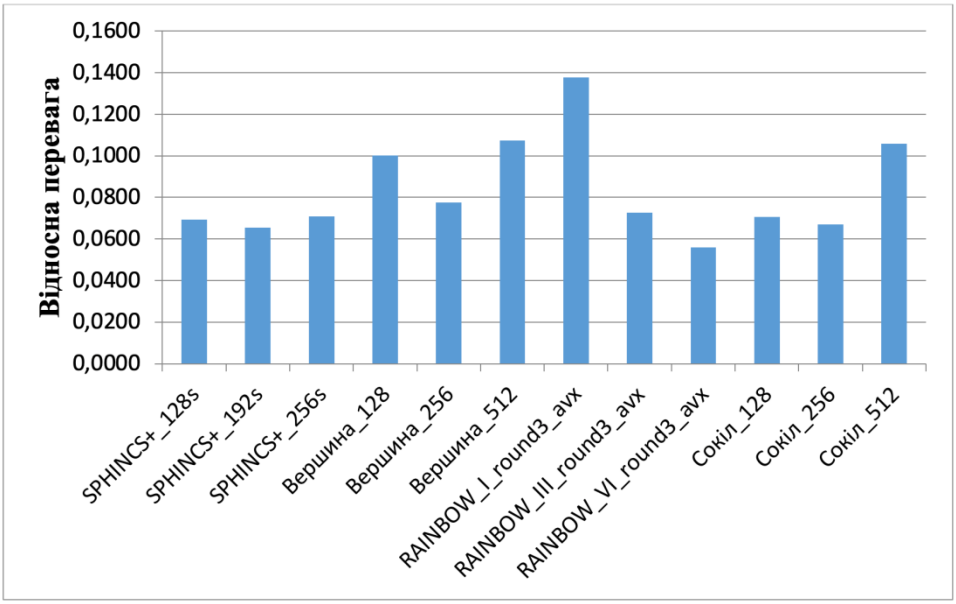

Рис. 4. Переваги алгоритмів ЕП

4.3. Результати повторного порівняння перспективних механізмів ЕП з використанням методу ранжування

Для порівняння методом ранжування варіанти реалізації алгоритмів за їхніми параметрами були розбиті на дві групи рівнів захисту: група параметрів середнього (3-4 рівні) та високого.

На рис. 5 відображено гістограму загальної відносної переваги алгоритмів ЕП (з параметрами високого рівня захисту) з урахуванням вагових коефіцієнтів характеристик з використанням методу ранжування.

При порівнянні методом ранжування з'ясувалося, що кращий результат мають алгоритми, які побудовані на основі перетворень в решеті числового поля.

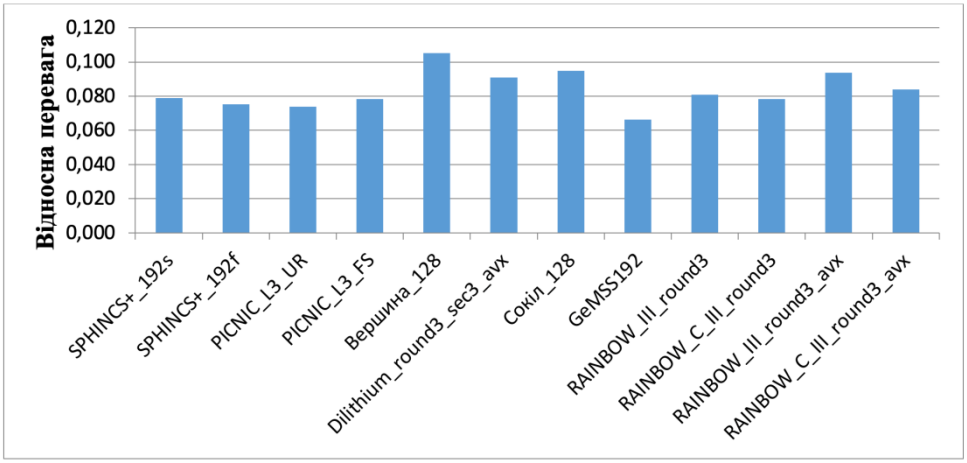

Рис. 5. Переваги алгоритмів ЕП середнього рівня захисту коефіцієнтів характеристик з використанням методу ранжування

4.4. Опис та результати дослідження механізмів ЕП за сукупністю прагматичних

Згідно з комплексною методикою на перших двох етапах застосовуються методики на основі застосування безумовних та умовних критеріїв оцінки ЕП. На третьому етапі залежності від вимог, що висуваються до криптопримітивів, при необхідності потрібно оцінювати та порівнювати альтернативні примітиви за техніко-економічними та техніко-експлуатаційними критеріями (характеристиками) ЕП тощо, які носять локальний характер. В якості основних потрібно використовувати такі критерії (характеристики) як довжини особистих та відкритих ключів ЕП, довжини ЕП, складність (швидкодію) основних – прямих та зворотних криптоперетворень ЕП тощо, складність генерування (обчислення) ключів та параметрів ЕП, а також їх взаємну залежність, у тому числі і у залежності від показників щодо криптостійкості та розмірів параметрів і ключів, а також видами математичних методів ЕП, що використовуються для реалізації криптопримітивів ЕП тощо. Таким чином, важливістю третього етапу комплексної методики оцінки та порівняння ЕП є те, що на ньому здійснюється перевірка щодо відповідності часткових безумовних та умовних критеріїв вимогам, що висунуті щодо них відповідними нормативними документами.

У якості криптопримітивів ЕП виберемо кандидати, що пройшли перший етап відбору. Він є найбільш узагальненим щодо оцінки та порівняння існуючих і перспективних ЕП. На цьому етапі оцінюються можливості виконання прагматичних вимог на основі використання певних математичних методів при криптоперетвореннях ЕП, що пройшли на третій етап міжнародних досліджень.

Послідовність оцінювання та порівняння криптопримітивів ЕП враховують вимоги, а оцінки і порівняння проводяться у наступній послідовності:

1. Аналізу та порівнянню підлягають тільки криптоперетворення ЕП, що успішно пройшли тестування згідно з вимогами другого етапу відповідно до безумовних часткових та безумовного інтегрального критеріїв.

2. Подальший аналіз проводиться з використанням умовних часткових та інтегрального умовного критеріїв щодо усіх криптопримітивів ЕП, що пройшли відбір відповідно до безумовних критеріїв.

3. Визначається перелік необхідних прагматичних критеріїв щодо ЕП. На основі, як правило, експериментальних та в меншій мірі теоретичних оцінок, визначаються основні показники щодо техніко-економічних та техніко-експлуатаційних характеристик, в тому числі з урахуванням NIST.IR 8413 та IT Grundschutz [4, 18]:

$I_{ст.}$ – рівень криптографічної стійкості ЕП;

$l_{в.к.}$ – довжина відкритого ключа ЕП;

$l_{о.к.}$ – довжина особистого ключа ЕП;

$l_{рез.}$ – довжина ЕП;

$T_{пр.}$ – складність (швидкість) обчислення ЕП;

$T_{зв.}$ – складність (швидкість) перевірки ЕП;

$T_{ген.зп.}$ – складність (швидкість) генерування загальних параметрів ЕП;

$T_{ген.кл.}$ – складність (швидкість) генерування ключа (ключової пари) ЕП тощо з урахуванням особливостей.

4. На основі, як правило, експериментальних та в меншій мірі теоретичних оцінок, визначаються залежності необхідних показників між собою щодо їх техніко-економічних та техніко-експлуатаційних характеристик ЕП, але з урахуванням, що вони успішно пройшли перший та другий етапи оцінки та досліджень.

5. На основі аналізу значень показників ЕП, їх залежностей між собою та значень умовних та безумовних критеріїв, що отримані на першому та другому етапах, приймаються рішення про переваги певних кандидатів ЕП.

6. Наприклад, визначаються:

- залежність довжини відкритого ключа ЕП від довжини особистого (закритого) від математичного методу, який застосовується при побудові асиметричної пари ключа для ЕП;
- залежність складності генерування відкритого ключа ЕП від складності генерування особистого ключа у залежності від математичного методу, який застосовується при побудові асиметричної пари ключа для ЕП;
- залежність складності генерування загальних параметрів ЕП від математичного методу, який застосовується;
- залежність збитковості ЕП від математичного методу, який застосовується;
- залежність від виду реалізації (програмна, програмно-апаратна та апаратна тощо).

Очевидно застосування прагматичної методики необхідне у випадках, коли необхідно забезпечити виконання вимог щодо розмірів ключів та параметрів, складності виконання ЕП, у залежності від математичного методу та розмірів загальних параметрів та ключів тощо. Конкретно вони визначаються вимогами до техніко-економічних та техніко-експлуатаційних вимог тощо.

4.5. Дослідження прагматичних оцінок алгоритмів ЕП, що засновані на перетвореннях на алгебраїчних решітках

Для дослідження прагматичних критеріїв було обрано алгоритми, що базуються на криптоперетвореннях на алгебраїчних решітках – Dilithium, «Вершина» та «Сокіл».

На рис. 6 показано залежність довжини відкритого ключа від довжини особистого ключа. Оскільки алгоритм «Вершина» базується на алгоритмі Dilithium, то їх графіки майже співпадають, тільки у «Вершини» він довший за рахунок наявності параметрів, що забезпечує більш високий рівень стійкості. Для алгоритму «Сокіл» графік нерівномірний через особливості кодування особистого ключа для параметрів Сокіл_256 – для цих параметрів особистий ключ довший за інші.

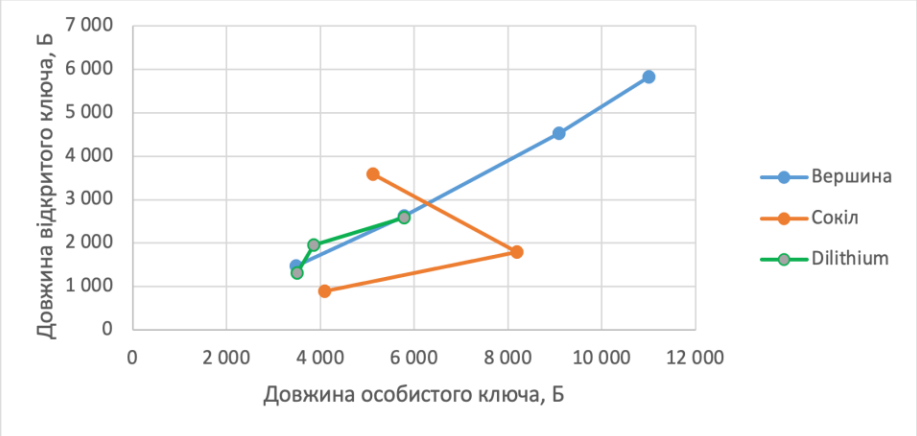

Рис. 6. Залежність довжини відкритого ключа від довжини особистого ключа

На рис. 7 показано залежність довжини підпису від довжини особистого ключа. Залежність та сама, що й для відкритого ключа.

На рис. 8 показано залежність часу підпису від довжини особистого ключа. Графік «Вершини» має як і раніше той же вигляд, що й Dilithium, але за рахунок оптимізацій має більш низькі значення.

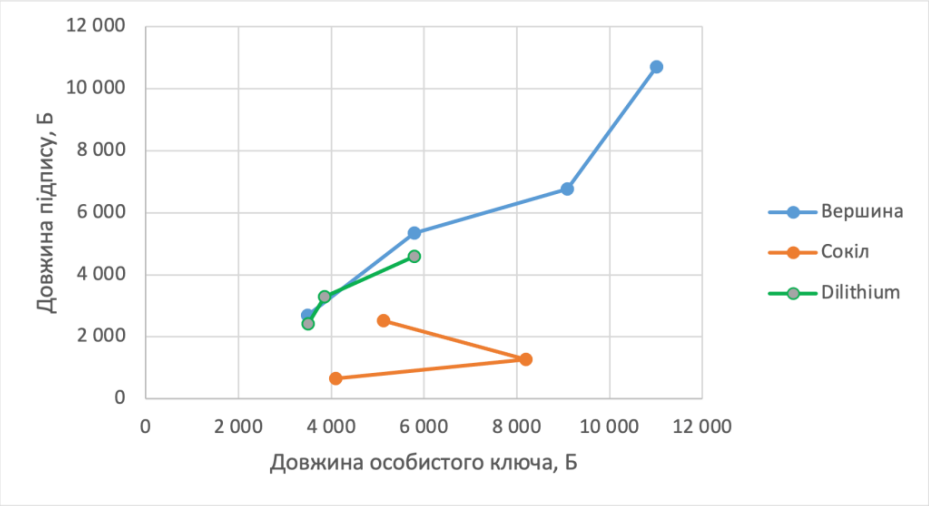

Рис. 7. Залежність довжини повідомлення від довжини особистого ключа

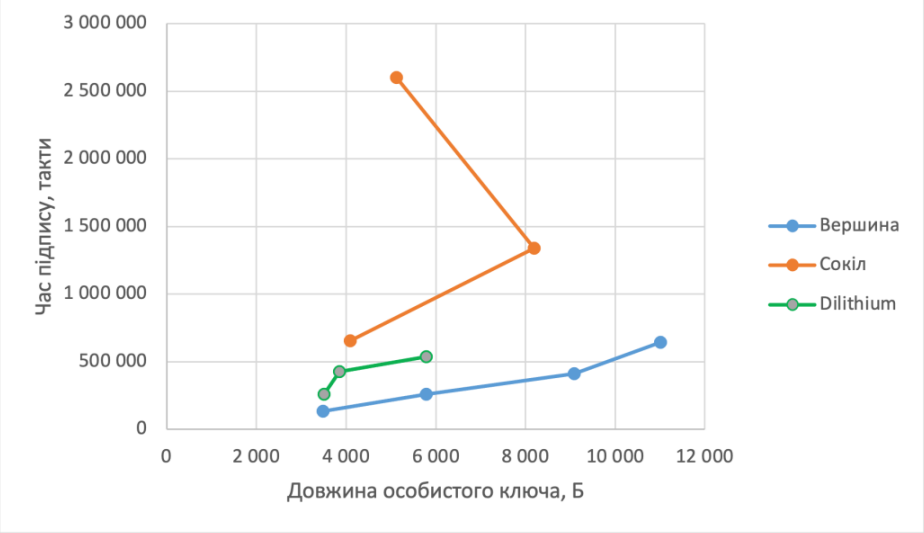

Рис. 8. Залежність часу підпису від довжини особистого ключа

На рис. 9 показано залежність часу перевірки підпису від довжини відкритого ключа.

На рис. 10 показано залежність часу генерації ключів від довжини особистого ключа. Через велику різниці між значеннями було вирішено для наглядності цієї оцінки використовувати в цьому графіку логарифмічну шкалу оцінки (значення вісей мають степені 2, в показниковій прогресії).

За графіками видно, що залежності «Вершини» мають той самий вигляд, що й Dilithium – для розмірів ключів і підпису на рівнях, що відповідають третьому та п’ятому рівням захисту, вони співпадають, а для швидкодії Dilithium має менші значення за рахунок оптимізації. Алгоритм «Сокіл» має кращі показники розмірів ключів, підпису та часу перевірки підпису, але значно програє в швидкодії по самому підпису та генерації ключів. Тому рекомендується використовувати ЕП «Сокіл» в системах, де будуть використовуватися довгострокові ключі, а також кількість операції перевірки підпису буде значно більшою за операції накладання підпису.

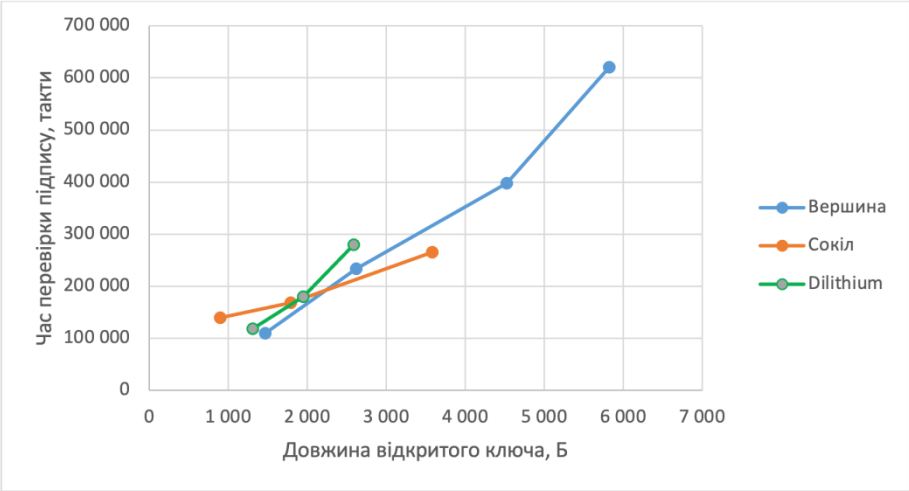

Рис. 9. Залежність часу перевірки підпису від довжини відкритого ключа

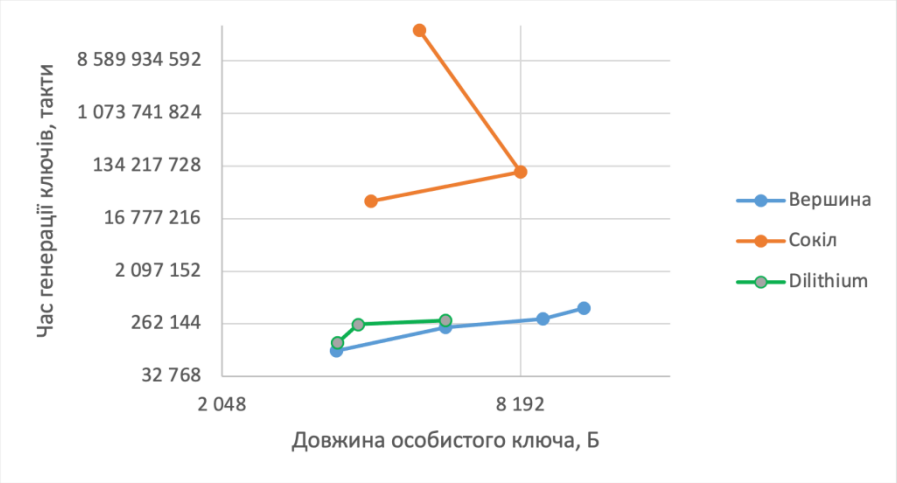

Рис. 10. Залежність часу генерації ключів від довжини особистого ключа

Висновки

1. На міжнародному та національному рівнях суттєво жорсткіші вимоги висунуті стосовно безпеки інформації, техніко-економічних та техніко-експлуатаційних характеристик до інформаційно-комунікаційних систем та інформаційних технологій КЗІ. Це вимоги до надання користувачам в критичних технологіях послуг, цілісності, доступності, конфіденційності, неспростовності відправника та отримувача, криптографічної живучості та санкціонування користувачам дозволу на обмін та обробку інформації взагалі та у критичних технологіях засобом обов'язкового застосування КЗІ.

2. Згідно з суттєво посиленими вимогами системи КЗІ повинні забезпечувати вже захист від класичних, квантових, на основі помилок та атак сторонніми каналами від порушника (криптоаналітика) третього рівня, для якого практично не існує матеріально-технічних та фінансових обмежень, та їх використання на практиці в процесі здійснення кібератак.

3. Під комплексною методикою аналізу криптографічної стійкості існуючих та перспективних (постквантових) АСШ, ПІК та ЕП, у тому числі у перехідний та постквантовий періоди, розуміється фіксована сукупність прийомів практичної діяльності щодо аналізу криптографічної стійкості та властивостей існуючих та перспективних (постквантових) АСШ, ПІК та ЕП, у тому числі у перехідний та постквантовий періоди, шо відповідає вимогам.

4. Методики можуть застосовуватись незалежно одна від одної, але основним є їх застосування у вказаній послідовності – спочатку з використанням на основі безумовних критеріїв, потім – на основі умовних критеріїв та при необхідності – на основі прагматичних критеріїв.

5. Основним завданням комплексної методики є формалізація процесів прийняття рішень відносно виконання висунутих до них вимог, врахування переваг та недоліків криптопримітивів, що є кандидатами на постквантовий стандарт, зменшення впливу суб'єктивних факторів на прийняття рішень, в тому числі несанкціонованого впливу сторонніх організацій тощо. Наприклад, такі методики можуть бути застосованими щодо оцінки та порівняння алгоритмів АСШ, ПІК та ЕП, що є в нашому випадку кандидатами на постквантовий стандарт.

6. До безумовних критеріїв, як мінімум, необхідно віднести:

$I_{ст.}$ – рівень криптостійкості з використанням безумовних критеріїв;

$l_{в.к.}$ – можливі довжини відкритого ключа;

$l_{о.к.}$ – можливі довжини особистого (секретного) ключа;

$l_{рез.}$ – довжину результату криптоперетворення (збитковість);

$T_{пр.}$ – складність (швидкість) прямого криптоперетворення;

$T_{зв.}$ – складність (швидкість) зворотного криптоперетворення;

$T_{ген.зп.}$ – складність (швидкість) генерування загальних параметрів для відповідного режиму роботи криптоперетворення (у залежності від довжин загальних параметрів та ключів);

$T_{ген.кл.}$ – складність (швидкість) генерування ключа (ключової пари) у залежності від режиму роботи тощо.

7. У якості основних рекомендується використовувати такі прагматичні критерії (характеристики) як довжини особистих та відкритих ключів, довжини електронних підписів та довжини блоків, що шифруються, складність (швидкодію) основних прямих та зворотних криптоперетворень АСШ, ПІК та ЕП тощо, складність генерування (обчислення) ключів та параметрів, а також їх взаємну залежність, у тому числі і у залежності від показників щодо криптостійкості та розмірів параметрів і ключів, а також види математичних методів, що використовуються для реалізації криптопримітивів тощо.

8. На основі, як правило, експериментальних та в меншій мірі теоретичних оцінок, визначаються залежності необхідних показників між собою щодо їх техніко-економічних та техніко-експлуатаційних характеристик, але з урахуванням, що вони успішно пройшли перший та другий етапи оцінки та досліджень.

9. Застосування прагматичної методики необхідне у випадках, коли необхідно забезпечити виконання вимог щодо розмірів ключів та параметрів, складності виконання АСШ, ПІК та ЕП у залежності від математичного методу та розмірів загальних параметрів та ключів тощо. Конкретно вони визначаються вимогами до техніко-економічних та техніко-експлуатаційних вимог тощо, наприклад, з урахуванням NIST.IR 8413 та IT Grundschutz.

Список літератури:

1. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 4 червня 2020 року N 681-IX. Режим доступу: https://ips.ligazakon.net/document/z008000?an=4779&ed=2020_06_04.

2. Crystals-Kyber. [Електронний ресурс]. Режим доступу: https://pq-crystals.org/kyber/.

3. Crystals-Dilithium. [Електронний ресурс]. Режим доступу: https://pq-crystals.org/dilithium/index.shtml.

4. NIST IR 8413 Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process / Gorjan Alagic, Daniel Apon, David Cooper, Quynh Dang, Thinh Dang, John Kelsey, Jacob Lichtinger, Carl Miller, Dustin Moody, Rene Peralta, Ray Perlner, Angela Robinson, Daniel Smith-Tone, Yi-Kai Liu. Режим доступу: https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8413.pdf.

5. ДСТУ 7624:2014 Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення. Режим доступу: https://www.twirpx.com/file/2878521/.

6. ДСТУ 7564:2014 Інформаційні технології. Криптографічний захист інформації. Функція гешування. Режим доступу: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc.66229.

7. ДСТУ 8961:2019 Інформаційні технології. Криптографічний захист інформації. Алгоритми асиметричного шифрування та інкапсуляції ключів. Режим доступу: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=88056.

8. ДСТУ 8845:2019 Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного потокового перетворення. Режим доступу: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=82494.

9. NIST Special Publication 800-208 Recommendation for Stateful Hash-Based Signature Schemes / David A. Cooper, Daniel C. Apon, Quynh H. Dang, Michael S. Davidson, Morris J. Dworkin, Carl A. Miller. Режим доступу: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-208.pdf.

10 Горбенко І. Д., Горбенко Ю. І. Прикладна криптологія : підручник. 2-ге вид. Харків : Форт, 2013. 878 с.

11. Горбенко Ю.І. Методи побудування та аналізу криптографічних систем : монографія. Харків : Форт, 2015. 959 с.

12. ДСТУ ISO/IEC 14888-3:2014 Інформаційні технології – Методи захисту – Цифрові підписи з доповненням. Ч. 3. Механізми, що ґрунтуються на дискретному логарифмі (ISO/IEC 14888-3:2008, IDT). 113 с.

13. ДСТУ 4145-2002 Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка. К. : Держстандарт України, 2003. 35 с.

14. ДСТУ ISO/IEC 10118-3:2005 Інформаційні технології. Методи захисту. Геш-функції. Ч. 3: Спеціалізовані геш-функції. Режим доступу: https://dnaop.com/html/61829/docA3_ISO_IEC_10118-3_2005.

15. Gorbenko I. D. Algorithms of asymmetric encryption and encapsulation of keys of post-quantum period of 5-7 levels of stability and their application / I. D. Gorbenko, O. G. Kachko, O. M. Aleksiychuk, O. O. Kuznetsov, Yu. I. Gorbenko, V. V. Onoprienko, M. V. Yesina, S. O. Kandy // Радіотехніка. 2019. Вип. 198. С. 5 – 18.

16. Горбенко І. Д. Методи обчислення системних параметрів для електронного підпису «Crystals-Dilithium» 128, 256, 384 та 512 біт рівнів безпеки / І. Д. Горбенко, А. М. Олексійчук, О. Г. Качко, Ю. І. Горбенко, М. В. Єсіна, С. О. Кандій // Радіотехніка. 2020. Вип. 202. С. 5 – 27.

17. Gorbenko I. D. Generation of general system parameters for Falcon cryptosystem for 256, 384, and 512 security bits / I. D. Gorbenko, S. O. Kandy, M. V. Yesina, Ye. V. Ostryanska // Telecommunications and Radio Engineering, 2022. Vol. 81, Is. 2. P. 49 – 59.

18. IT-Grundschutz-Compendium. Final Draft, 1 February 2022 // Federal Office for Information Security. Germany. Режим доступу: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi_it_gs_comp_2022.pdf?__blob=publicationFile&v=2.

19. Горбенко І. Д. Методи, методика та результати порівняльного аналізу електронних підписів згідно з ДСТУ ISO/IEC 14888-3:2014 / І. Д. Горбенко, М. В. Єсіна // Вісник Нац. ун-ту "Львівська політехніка". Сер. "Автоматика, вимірювання та керування". Львів : Нац. ун-т "Львівська політехніка", 2016. № 852. С. 9 – 22.

20. Олексійчук А. М. Обґрунтування перспективного постквантового національного стандарту електронного підпису на основі решіток / А. М. Олексійчук, В. А. Кулібаба, М. В. Єсіна, С. О. Кандій, Є. В. Острянська, І. Д. Горбенко // Радіотехніка. 2020. Вип. 200. С. 5 – 14.

21. Горбенко І. Д. Основні положення та результати порівняння властивостей електронних підписів постквантового періоду на алгебраїчних решітках / І. Д. Горбенко, О. Г. Качко, О. В. Потій, А. М. Олексійчук, Ю. І. Горбенко, М. В. Єсіна, І. В. Стельник, В. А. Пономар // Радіотехніка. 2021. Вип. 205. С. 5 – 21.

22. Gorbenko I. D. Calculation of general parameters for NTRU Prime Ukraine of 6-7 levels of stability / I. D. Gorbenko, A. N. Alekseychuk, O. G. Kachko, M. V. Yesina, I. V. Stelnik, S. O. Kandy, V. A. Bobukh, V. A. Ponomar // Telecommunications and Radio Engineering. 2019. Vol. 78, Is. 4. P. 327 – 340. DOI: 10.1615/TelecomRadEng.v78.i4.40.

23. Gorbenko I.D. Methods of building general parameters and keys for NTRU Prime Ukraine of 5th–7th levels of stability. Product form / I.D. Gorbenko, O.G. Kachko, Yu.I. Gorbenko, I.V. Stelnik, S.O. Kandyi, M.V. Yesina // Telecommunications and Radio Engineering. 2019. Vol. 78, Is. 7. P. 579 – 594. DOI: 10.1615/TelecomRadEng.v78.i7.30.

Надійшла до редколегії 10.02.2023

Відомості про авторів:

Горбенко Юрій Іванович – канд. техн. наук, АТ "Інститут Інформаційних Технологій", перший заступник головного конструктора, Україна; e-mail: jsciitua@gmail.com; ORCID: https://orcid.org/0000-0003-0073-9107

Єсіна Марина Віталіївна – канд. техн. наук, Харківський національний університет імені В.Н. Каразіна, доцент кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук; науковий співробітник-консультант АТ «Інститут Інформаційних Технологій»; Україна; e-mail: m.v.yesina@karazin.ua; ORCID: https://orcid.org/0000-0002-1252-7606

Пономар Володимир Андрійович – канд. техн. наук, Харківський національний університет імені В.Н. Каразіна, науковий співробітник кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук; інженер-конструктор АТ «Інститут інформаційних технологій»; Україна; e-mail: Laedaa@gmail.com; ORCID: https://orcid.org/0000-0001-5271-2251

Горбенко Іван Дмитрович – д-р техн. наук, професор, Харківський національний університет імені В. Н. Каразіна, професор кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, АТ "Інститут Інформаційних Технологій", головний конструктор, Україна; e-mail: i.d.gorbenko@karazin.ua; ORCID: https://orcid.org/0000-0003-4616-3449

Каптьол Євген Юрійович – Харківський національний університет імені В. Н. Каразіна, аспірант факультету комп'ютерних наук; співробітник АТ "Інститут Інформаційних Технологій", Україна, e-mail: kaptevg@gmail.com.