УДК 003.26:621.39:530.145(045)

ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ МЕТОДУ ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ КУТРИТОВИХ ПРОТОКОЛІВ КВАНТОВОЇ КРИПТОГРАФІЇ

Сергій Гнатюк, Тетяна Жмурко, Василь Кінзерявий, Халіча Юбузова

Сьогодні гостро постає питання забезпечення конфіденційності інформації в умовах зростання кількості та якості порушень в кіберпросторі, що постійно вдосконалюються та розвиваються. Надійність традиційних методів забезпечення конфіденційності викликає сумніви з огляду на сучасні загрози. Тому пошук альтернативних методів і способів захисту є актуальним питанням. Значний інтерес викликає квантова криптографія, яка не залежить від обчислювальних чи інших можливостей порушника, використовує специфічні унікальні властивості квантових частинок і ґрунтується на непорушності законів квантової фізики. Однією з найбільш розвинутих технологій квантової криптографії є квантовий прямий безпечний зв'язок, який дозволяє передавати інформацію відкритим каналом напряму (без попереднього її шифрування – проблема розподілу ключів нівелюється), проте вони мають лише асимптотичну стійкість до некогерентних атак і, безумовно, потребують методів підсилення безпеки. У зв'язку з цим розроблено метод забезпечення стійкості протоколів квантової криптографії. Для оцінювання ефективності цього методу було розроблено методику проведення експериментального дослідження, згідно якої виконано порівняння його швидкодії з відомим методом. Відповідно до отриманих результатів, запропонований метод має швидкість у 1,52 разів більшу від аналогів при тому ж рівні стійкості до некогерентних атак.

Ключові слова: *квантова криптографія, квантовий прямий безпечний зв'язок, трит, захист інформації.*

Актуальність. Сьогодні актуальність проблеми кібербезпеки не викликає ніяких сумнівів – щодня кожен громадянин стикається з необхідністю використання інформаційно-комунікаційних технологій (ІКТ) – від використання соціальних мереж та розміщення інформації про свої персональні дані в Інтернеті до користування банкоматами, банківськими рахунками тощо. У зв'язку з цим, гостро постає питання забезпечення конфіденційності в умовах зростання кількості та якості порушень в кіберпросторі, що постійно вдосконалюються та розвиваються на рівні з технологіями, що в свою чергу, ускладнює процес їх виявлення, аналізу і протидії. Надійність традиційних методів забезпечення конфіденційності, яка, як правило, забезпечується методами симетричної та асиметричної криптографії, викликає сумніви з огляду на сучасні загрози. Симетричним методам, зокрема, характерна проблема розподілу секретних ключів, а асиметричні – повільні та потребують значних обчислювальних ресурсів [1, 2, 9]. Крім того, стійкість усіх традиційних криптосистем залежить від обчислювальних можливостей порушника і базується на гіпотетичній неможливості розв'язання певного класу математичних задач за поліноміальний час – пошук у повністю невпорядкованій базі даних, факторизація та логарифмування в дискретних полях великого розміру тощо. Проте, ця гіпотеза може бути спростована за допомогою, наприклад, багатокубітних квантових комп'ютерів (D-Wave 2X), GRID-технологій, HPC та інших сучасних ІКТ [1, 4, 10].

З огляду на це, великий інтерес викликає квантова криптографія (КК), яка не залежить від обчислювальних потужностей порушника, використовує специфічні унікальні властивості квантових частинок і ґрунтується на непорушності законів квантової фізики. Основними перевагами методів КК є можливість точного виявлення порушника і забезпечення, в деяких випадках, теоретико-інформаційної (абсолютної) стійкості. На сьогодні такі методи і системи пройшли складний шлях від теоретичних гіпотез і лабораторних експериментів до повноцінних комерційних рішень [1, 2, 4, 9-10].

Однією з найбільш розвинених технологій КК є квантовий прямий безпечний зв'язок (КПБЗ), який дозволяє передавати інформацію відкритим каналом напряму (без попереднього її шифрування – проблема розподілу ключів нівелюється). На сьогодні запропоновано велику кількість методів КПБЗ [1-3, 6-8], що базуються на різних квантових технологіях і можуть використовуватись як для захищеного передавання інформації (з використанням кубітів або кудитів), так і для розподілу криптографічних ключів.

Проте, вимоги до стійкості протоколів КПБЗ є значно вищими, ніж до стійкості протоколів квантового розподілу ключів, адже в протоколах КПБЗ кожний біт є конфіденційною інформацією і не повинен потрапити до порушника. Таким чином, хоча протоколи КПБЗ повністю знімають проблему розподілу секретних криптографічних ключів, проте вони мають лише асимптотичну

стійкість до некогерентних атак і, безумовно, потребують методів підсилення безпеки [1, 4, 5]. Оскільки імовірність виявити цю атаку при одноразовому контролю підслуховування менше одиниці для всіх відомих протоколів КПБЗ, а крім того помилки в режимі контролю підслуховування будуть створюватися не тільки атакою, але і природним шумом у квантовому каналі зв'язку, то необхідно виконати деяку кількість раундів контролю підслуховування перш, ніж можна буде з упевненістю виявити атаку. Так як режими контролю підслуховування і передачі повідомлення необхідно чергувати випадковим чином, то деяка кількість інформації може бути перехоплена порушником [5]. Очевидно, що необхідно застосовувати додаткові процедури і методи підсилення безпеки. У [1, 7] описані методи підсилення безпеки протоколів КПБЗ, а в [3, 6, 8] авторами був запропонований метод забезпечення стійкості протоколів КПБЗ.

Метою статті є проведення експериментального дослідження методу забезпечення стійкості протоколів квантової криптографії (на прикладі кутритових протоколів) для оцінювання його ефективності.

Для дослідження запропонованого методу забезпечення стійкості протоколів КПБЗ [6, 8] було розроблено методику експериментального дослідження, відповідно до якої виконано порівняння його швидкодії з існуючим методом забезпечення стійкості [1, 2, 7] (на прикладі часткового випадку – застосування тритових протоколів).

Нехай потрібно передавати протоколом КПБЗ (з використанням запропонованого та відомого методів забезпечення стійкості) повідомлення $A \in V_n$ ($V_n = \{0,1,2\}^n$, $n = r \cdot l$, $r \in N$ – розмір блоку даних, а $l \in N$ – кількість таких блоків). Для порівняння швидкодії передачі повідомлення A протоколом КПБЗ (з частотою перемикання в режим підслуховування q) буде проведено оцінку часу виконання кожного конкретного його етапу. Для оцінки часу виконання кожного етапу було введено такі позначення: V_{gen} – швидкість генерування тритових послідовностей; V_{kv} та V_{kl} – швидкість передачі тритових послідовностей квантовим та класичним каналами відповідно; V_x – швидкість виконання арифметичних операцій у полі $GF(3)$.

Розглянемо спочатку відомий метод [1, 2]. Передача повідомлення A від Аліси до Боба (легітимні користувачі) виконується у шість етапів:

Етап 1 – Генерування матриць. Аліса генерує l матриць M_i розміром $r \times r$ трит, $i \in \overline{1,l}$ використовуючи для цього процедуру генерації тритових послідовностей F_{gen} та секретний параметр K (використовується тільки на етапі генерації матриць): $M_i = F_{gen}\left(K, i, r^2\right)$. Час виконання цієї операції буде залежати від швидкості генерації тритових послідовностей V_{gen} із яких формуються матриці, їх кількості l та розмірів $r \times r$. Отже $t_1 = \dfrac{l \cdot r^2}{V_{gen}}$. Зауважимо, що при оцінюванні часу генерації матриць рахуємо, що усі l матриць M_i, $i \in \overline{1,l}$ із першого разу генерувались невиродженими.

Етап 2 – Множення блоків даних. Аліса перемножує блоки даних A_i ($A = \left(A_1, ..., A_l\right)$, $i \in \overline{1,l}$) розміром r трит із отриманими матрицями M_i розміром $r \times r$ трит: $B_i = A_i \cdot M_i$. Час виконання цієї операції буде залежати від швидкості виконання арифметичних операцій у полі $GF(3)$ V_x, кількості блоків даних l та їх розміру r. Тоді $t_2 = \dfrac{l \cdot (2r^2 - r)}{V_x}$.

Етап 3 – Передавання повідомлень квантовим каналом. Відбувається передавання повідомлення B квантовим каналом з використанням протоколів КПБЗ від Аліси до Боба, при цьому з частотою q відбувається перемикання в режим контролю підслуховування для детектування Єви (порушника): $B_i' = F_{kv}\left(B_i, q\right)$. Час виконання цієї операції буде залежати від швидкості передачі тритових послідовностей квантовим каналом V_{kv}, кількості блоків даних l, їх розміру r та частоти перемикання в режим підслуховування q. Отже $t_3 = \left(\dfrac{l \cdot r}{V_{kv}}\right) \cdot (1+q)$.

Етап 4 – Передавання повідомлень відкритим каналом. Якщо на етапі 3 Аліса і Боб не виявили Єву відбувається передавання відкритим каналом від Аліси до Боба матриць M_i $i \in \overline{1,l}$: $M_i' = F_{kl}\left(M_i\right)$. Час виконання цієї операції буде

залежати від швидкості передачі тритових послідовностей класичним каналом V_{kl}, кількості матриць l та їх розміру $r \times r$. Тоді $t_4 = \frac{l \cdot r^2}{V_{kl}}$.

Етап 5 – Обернення матриць. Боб обертає отримані на 4 етапі матриці M_i, $i \in \overline{1,l}$: $\left(M_i'\right)^{-1} = F_{obr}\left(M_i'\right)$. Час виконання цієї операції буде залежати від швидкості виконання арифметичних операцій в полі $GF(3)$ V_x, кількості таких матриць l та їх розміру $r \times r$. Отже $t_5 = \frac{l \cdot (4r^3 - 4r^2)}{V_x}$.

Етап 6 – Відновлення повідомлень. Боб перемножує отримані блоки B_i ($B = \left(B_1, ..., B_l\right)$, $i \in \overline{1,l}$) розміром r тритів із отриманими оберненими матрицями $\left(M_i\right)^{-1}$ розміром $r \times r$ трит та відновлює початкове повідомлення: $A_i' = B_i' \cdot \left(M_i'\right)^{-1}$. Час виконання цієї операції буде залежати від швидкості виконання арифметичних операцій у полі $GF(3)$ V_x, кількості блоків даних l та їх розміру r. Тоді $t_6 = \frac{l \cdot (2r^2 - r)}{V_x}$.

Тоді швидкість передачі повідомлення A протоколом КПБЗ з використанням відомого методу забезпечення стійкості: $V = \frac{r \cdot l}{t}$, загальний час роботи протоколу КПБЗ, $t = \sum_{i=1}^{6} t_i$, t_i – час виконання i-го етапу, $i = \overline{1,6}$.

Тепер розглянемо запропонований метод забезпечення стійкості протоколів КПБЗ [3, 6, 8]. Передавання повідомлення A від Аліси до Боба виконується у вісім етапів:

Етап 1 – Генерування блоків даних. Аліса генерує l блоків k_i розміром r трит, $i \in \overline{1,l}$ використовуючи для цього процедуру генерації тритових послідовностей F_{gen} та секретний параметр K: $k_i = F_{gen}\left(K, i, r\right)$. Час виконання цієї операції буде залежати від швидкості генерації тритових послідовностей V_{gen}, кількості l та розмірів r блоків k_i, $i \in \overline{1,l}$. Отже $t_1 = \frac{l \cdot r}{V_{gen}}$.

Етап 2 – Складання блоків даних. Аліса потритово складає блоки даних A_i ($A = \left(A_1, ..., A_l\right)$, $i \in \overline{1,l}$) із блоками k_i: $B_i = A_i + k_i$. Час виконання цієї операції буде залежати від швидкості виконання арифметичних операцій у полі $Gf(3)$ V_x, кількості блоків даних l та їх розміру r. Тоді $t_2 = \frac{l \cdot r}{V_x}$.

Етап 3 – Перетворення блоків даних. Аліса обчислює хеш-код повідомлення B та перетворює його асиметричною функцією перетворення F_{aka}^{enc} з використанням відкритого секретного параметру Боба: $H = F_{hf}\left(B\right)$, $J = F_{aka}^{enc}\left(H, K_{op}^{B}\right)$. Час виконання цієї операції буде залежати від швидкості виконання арифметичних операцій у полі $GF(3)$ V_x, кількості блоків даних l та їх розміру r. Отже $t_3 = \frac{4 \cdot l \cdot r}{V_x}$.

Етап 4 – Передавання повідомлень квантовим каналом. Відбувається передавання повідомлення $\left(B, J\right)$ квантовим каналом з використанням протоколів КПБЗ від Аліси до Боба, при цьому з частотою q відбувається перемикання в режим контролю підслуховування для детектування Єви: $B_i' = F_{kv}\left(B_i, q\right)$, $J' = F_{kv}\left(J, q\right)$. Час виконання цієї операції буде залежати від швидкості передачі тритових послідовностей квантовим каналом V_{kv}, кількості блоків даних l, їх розміру r, частоти перемикання в режим підслуховування q та довжини зашифрованого хеш-коду J (для простоти обрали його розміром 96 трит). Тоді $t_4 = \left(\frac{l \cdot r + 96}{V_{kv}}\right) \cdot \left(1 + q\right)$.

Етап 5 – Перевірка цілісності. Боб розраховує нове значення хеш коду H' повідомлення B' та виконує зворотне перетворення хеш коду H'' асиметричною функцією F_{aka}^{dec} з використанням свого закритого секретного параметру: $H' = F_{hf}\left(B'\right)$ і $H'' = F_{aka}^{dec}\left(J', K_{cl}^{B}\right)$. Час виконання цієї операції буде залежати від швидкості виконання арифметичних операцій в полі $GF(3)$ V_x, кількості блоків даних l та їх розміру r. Отже $t_5 = \frac{4 \cdot l \cdot r}{V_x}$.

Етап 6 – Передавання повідомлення відкритим каналом. Якщо на етапі 4 Аліса і Боб не виявили Єву і на етапі 5 Боб отримав $H' = H''$, то відбувається передача відкритим каналом від Аліси до Боба секретного параметра K: $K' = F_{kl}(K)$. Час виконання цієї операції буде залежати від швидкості передачі тритових послідовностей класичним каналом V_{kl} та розміру K (для простоти розрахунків обрали його розмір − 96 трит). Тоді $t_6 = \dfrac{96}{V_{kl}}$.

Етап 7 – Генерування додаткової послідовності. Боб генерує таку ж послідовність k_i розміром r трит, яку генерувала Аліса на етапі 1, $i \in \overline{1,l}$, використовуючи для цього процедуру генерації тритових послідовностей F_{gen} та секретний параметр K, що отримав на етапі 6: $k_i' = F_{gen}(K', i, r)$. Час виконання цієї операції буде залежати від швидкості генерації тритових послідовностей V_{gen}, кількості l та розмірів r блоків k_i, $i \in \overline{1,l}$. Отже $t_7 = \dfrac{l \cdot r}{V_{gen}}$.

Етап 8 – Відновлення повідомлення. Боб потритово віднімає від блоків даних B_i $(B = (B_1, ..., B_l)$, $i \in \overline{1,l})$ блоки k_i та відновлює початкове повідомлення A: $A_i' = B_i' - k_i'$. Час виконання цієї операції буде залежати від швидкості виконання арифметичних операцій в полі $GF(3)$ V_x, кількості блоків даних l та їх розміру r. Тоді $t_8 = \dfrac{l \cdot r}{V_x}$.

Тоді швидкість передавання повідомлення A протоколом КПБЗ з використанням запропонованого методу забезпечення стійкості: $V = \dfrac{r \cdot l}{t}$, загальний час роботи протоколу КПБЗ, $t = \sum_{i=1}^{8} t_i$, t_i – час виконання i-го етапу, $i = \overline{1,8}$.

У табл. 1 наведено основні етапи протоколу КПБЗ із застосування різних методів забезпечення стійкості (відомого та запропонованого) та час їх виконання.

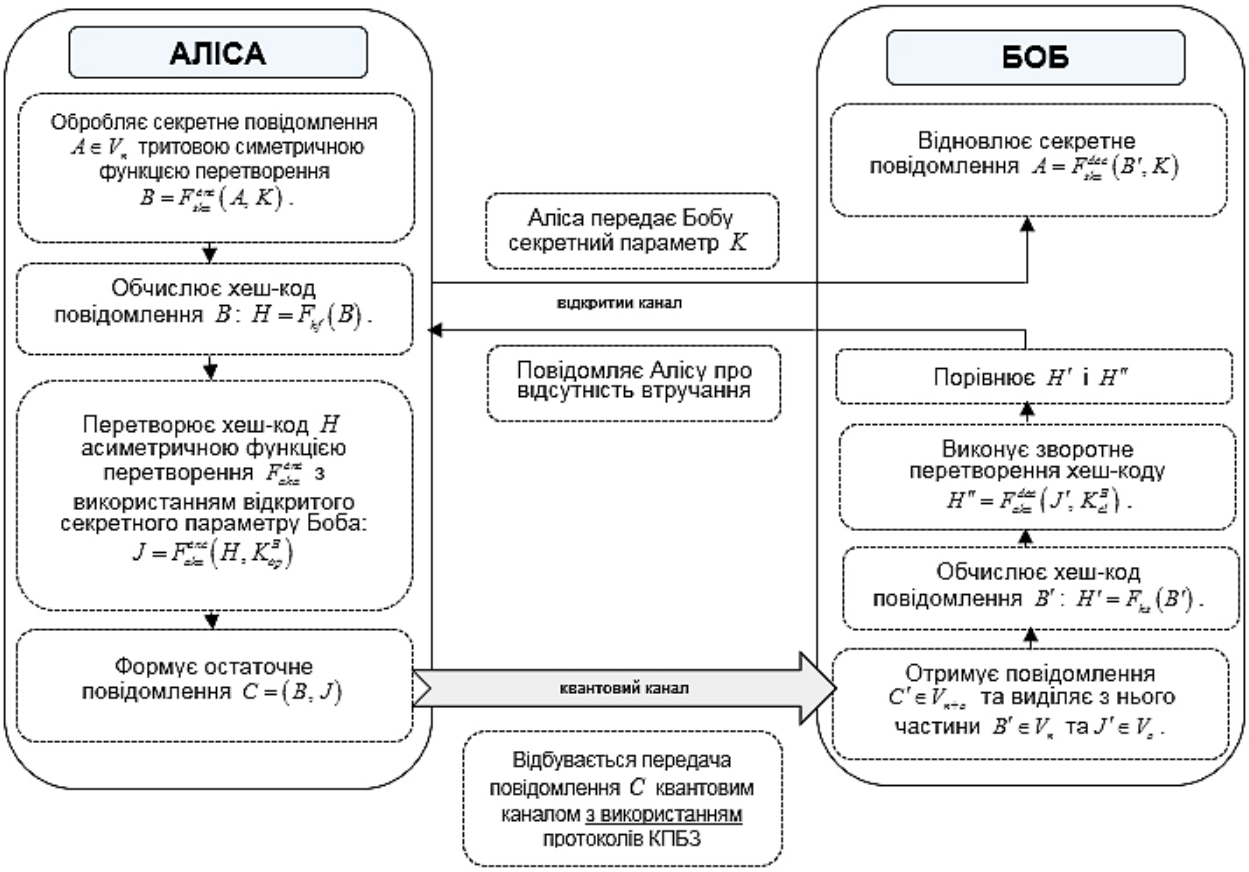

Рис. 1. Схема реалізації методу забезпечення стійкості протоколу КПБЗ [6, 8]

Таблиця 1

Оцінка часу виконання етапів протоколу КПБЗ

№ Ет.	Відомий метод [1, 2, 7]		Запропонований метод [3, 6, 8]	
	Операція	Час виконання, с.	Операція	Час виконання, с.
1	$M_i = F_{gen}\left(K, i, r^2\right)$	$\frac{l \cdot r^2}{V_{gen}}$	$k_i = F_{gen}\left(K, i, r\right)$	$\frac{l \cdot r}{V_{gen}}$
2	$B_i = A_i \cdot M_i$	$\frac{l \cdot (2r^2 - r)}{V_x}$	$B_i = A_i + k_i$	$\frac{l \cdot r}{V_x}$
3	$B_i' = F_{kv}\left(B_i, q\right)$	$\left(\frac{l \cdot r}{V_{kv}}\right) \cdot (1+q)$	$H = F_{hf}\left(B\right)$ $J = F_{aka}^{enc}\left(H, K_{op}^{B}\right)$	$\frac{4 \cdot l \cdot r}{V_x}$
4	$M_i' = F_{kl}\left(M_i\right)$	$\frac{l \cdot r^2}{V_{kl}}$	$B_i' = F_{kv}\left(B_i, q\right)$ $J' = F_{kv}\left(J, q\right)$	$\left(\frac{l \cdot r + 96}{V_{kv}}\right) \cdot (1+q)$
5	$\left(M_i'\right)^{-1} = F_{obr}\left(M_i'\right)$	$\frac{l \cdot (4r^3 - 4r^2)}{V_x}$	$H' = F_{hf}\left(B'\right)$ $H'' = F_{aka}^{dec}\left(J', K_{cl}^{B}\right)$	$\frac{4 \cdot l \cdot r}{V_x}$
6	$A_i' = B_i' \cdot \left(M_i'\right)^{-1}$	$\frac{l \cdot (2r^2 - r)}{V_x}$	$K' = F_{kl}\left(K\right)$	$\frac{96}{V_{kl}}$
7	-	0	$k_i' = F_{gen}\left(K', i, r\right)$	$\frac{l \cdot r}{V_{gen}}$
8	-	0	$A_i' = B_i' - k_i'$	$\frac{l \cdot r}{V_x}$

Експериментальне дослідження. Для дослідження швидкодії зазначених методів забезпечення стійкості протоколів КПБЗ було проведено 7 експериментів при різних параметрах r, l, q, V_{gen}, V_{kv}, V_{kl} та V_x.

Мета експериментів – дослідити ефективність розробленого методу у порівнянні з відомим та перевіритийого адекватність.

Вхідними параметрами є: швидкість генерування тритових послідовностей (V_{gen}), швидкість передачі тритових послідовностей квантовим каналом (V_{kv}), швидкість передачі тритових послідовностей класичним каналом (V_{kl}), швидкість виконання арифметичних операцій у полі $GF(3)$ (V_x), розмір блоку даних (r), кількість блоків даних (l), частота перемикання в режим підслуховування (q), відомий та запропоновані методи забезпечення стійкості кутритових протоколів КК, розмір кроків зміни кожного параметру.

Вихідні параметри: зібрана статистика швидкостей роботи відомого та запропонованого методів забезпечення стійкості кутритових протоколів КК в залежності від вхідних параметрів.

Послідовність дій при проведені експериментів: Фіксуються базові параметри системи: швидкість генерування тритових послідовностей (V_{gen}), швидкість передачі тритових послідовностей квантовим каналом (V_{kv}), швидкість передачі тритових послідовностей класичним каналом (V_{kl}), швидкість виконання арифметичних операцій у полі $GF(3)$ (V_x), розмір блоку даних (r), кількість блоків даних (l), частота перемикання в режим підслуховування (q). Далі моделюється виконання усіх етапів квантового протоколу за допомогою розробленого програмного забезпечення. Зібрана статистика використовується для аналізу ефективності запропонованого методу забезпечення стійкості кутритових протоколів КК.

Вибір кроку зміни чинників: зміна r від 4 до 100 (з кроком 4). Зміна швидкостей роботи протоколів (V_{gen}, V_{kv}, V_{kl} та V_x) із 1000 до 100000.

Експеримент 1. Нехай $V_x = V_{kl} = 10^6$, $V_{gen} = 10^4$, $V_{kv} = 10^3$, $l = 1000$, $q = 0{,}5$ – для відомого методу забезпечення стійкості протоколів КПБЗ, $q = 0{,}05$ для запропонованого методу.

Ймовірність перемикання у режим контролю підслуховування для запропонованого методу може бути зменшена до мінімуму (із рекомендованого значення 0,5 до 0,05).

На рис. 2. наведено результати експерименту 1 щодо порівняння швидкодії протоколу КПБЗ для різних методів забезпечення його стійкості.

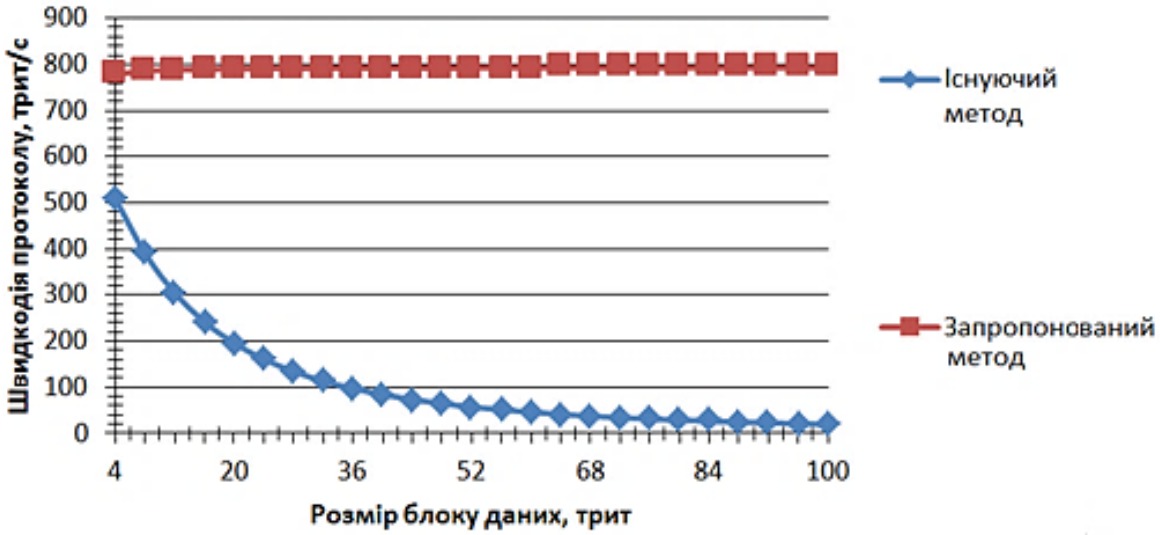

Рис. 2. Порівняння швидкісних характеристик протоколу КПБЗ (результати експерименту 1)

Згідно результатів експерименту, швидкість протоколу КПБЗ із запропонованим методом забезпечення стійкості мінімум у 1,52 раз є більшою за швидкість відомого методу (для $r=4$). Причому при збільшенні r покращення швидкодії буде ще більш показовим. Наприклад, при $r=20$ швидкодія запропонованого методу є кращою у 4,4 рази.

Експеримент 2. Нехай $V_x = V_{kl} = 10^5$, $V_{gen} = 10^4$, $V_{kv} = 10^3$, $l = 1000$, $q = 0{,}5$ – для відомого методу забезпечення стійкості протоколів КПБЗ, $q = 0{,}05$ для запропонованого методу.

На рис. 3 наведено результати експерименту 2 щодо порівняння швидкодії протоколу КПБЗ для різних методів забезпечення його стійкості.

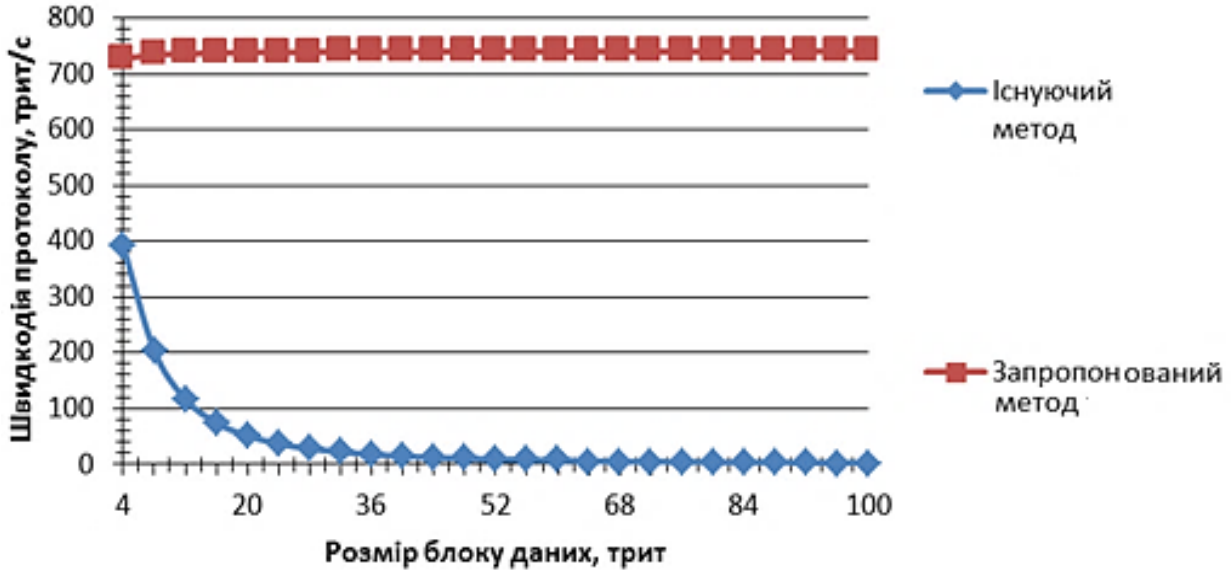

Рис. 3. Порівняння швидкісних характеристик протоколу КПБЗ (результати експерименту 2)

Згідно результатів експерименту, швидкість протоколу КПБЗ із застосуванням запропонованого методу забезпечення стійкості мінімум у 1,86 раз є більшою за швидкість відомого методу (для $r=4$). Причому при збільшенні r покращення швидкодії буде ще більш показовим. Наприклад, при $r=20$ швидкодія запропонованого методу краща у 14,5 рази.

Експеримент 3. Нехай $V_x = V_{kl} = V_{gen} = 10^5$, $V_{kv} = 10^3$, $l = 1000$, $q = 0{,}5$ – для відомого методу

забезпечення стійкості протоколів КПБЗ, $q = 0,05$ для запропонованого методу.

На рис. 4 наведено результати експерименту 3 щодо порівняння швидкодії протоколу КПБЗ для різних методів забезпечення його стійкості.

Згідно результатів експерименту, швидкість протоколу КПБЗ із застосуванням запропонованого методу забезпечення стійкості мінімум у 1,84 раз краща за швидкість відомого методу (для $r = 4$). Причому при збільшенні r покращення швидкодії буде ще більш показовим. Наприклад, при $r = 20$ швидкодія запропонованого методу є більшою у 15,21 рази.

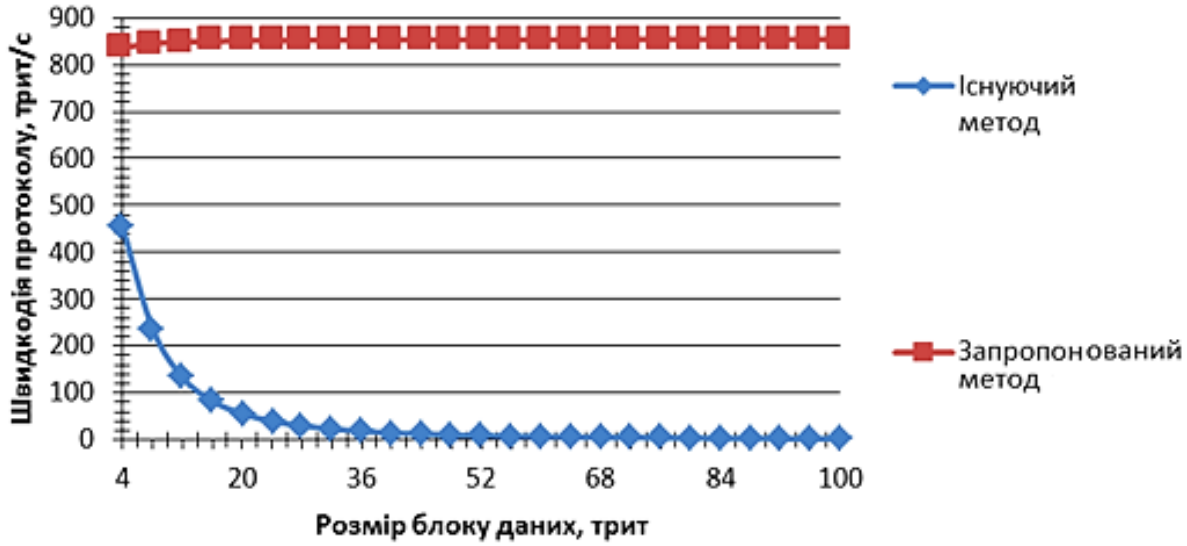

Рис. 4. Порівняння швидкісних характеристик протоколу КПБЗ (результати експерименту 3)

Експеримент 4. Нехай $V_x = V_{kl} = V_{gen} = 10^5$, $V_{kv} = 10^4$, $l = 1000$, $q = 0,5$ – для відомого методу забезпечення стійкості протоколів КПБЗ, $q = 0,05$ для запропонованого методу.

На рис. 5 наведено результати експерименту 4 щодо порівняння швидкодії протоколу КПБЗ для різних методів забезпечення його стійкості.

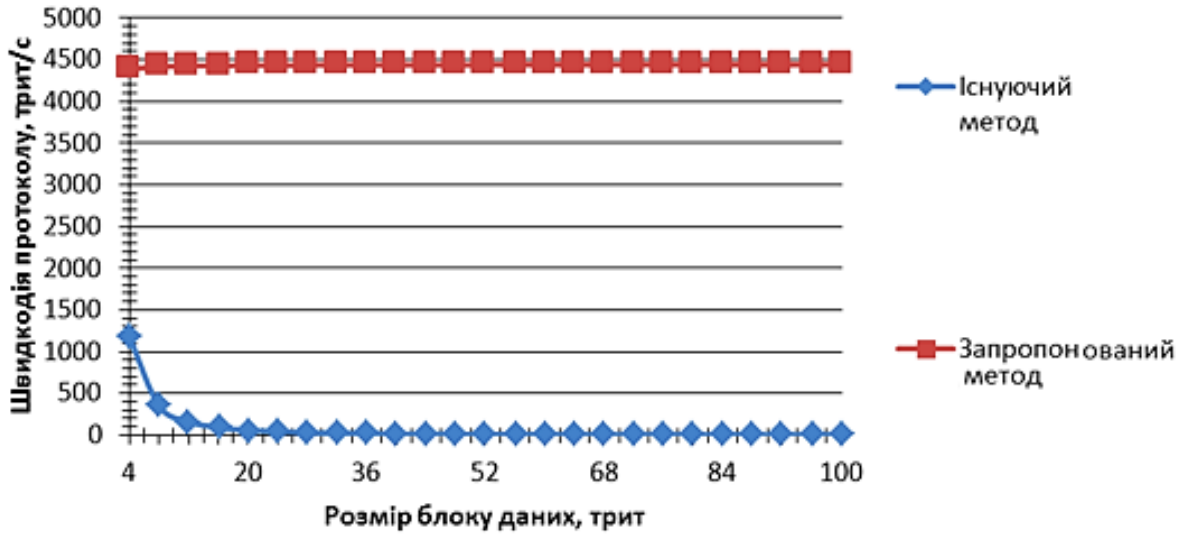

Рис. 5. Порівняння швидкісних характеристик протоколу КПБЗ (результати експерименту 4)

Згідно результатів експерименту, швидкість протоколу КПБЗ із застосуванням запропонованого методу забезпечення стійкості мінімум у 3,73 раз є більшою за швидкість відомого методу (для $r = 4$). Причому при збільшенні r покращення швидкодії буде ще більш показовим. Наприклад, при $r = 20$ швидкодія запропонованого методу краща у 73,29 раз.

Експеримент 5. Нехай $V_x = V_{kl} = V_{gen} = V_{kv} = 10^5$, $l = 1000$, $q = 0,5$ – для відомого методу забезпечення стійкості протоколів КПБЗ, $q = 0,05$ для запропонованого методу.

На рис. 6 наведено результати експерименту 5 щодо порівняння швидкодії протоколу КПБЗ для різних методів забезпечення його стійкості.

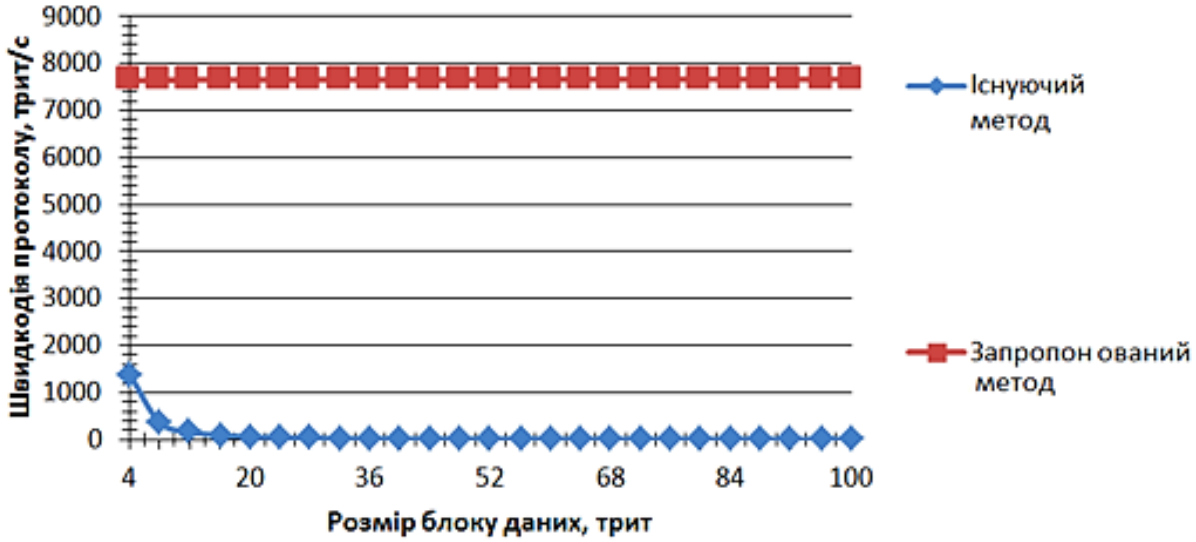

Рис. 6. Порівняння швидкісних характеристик протоколу КПБЗ (результати експерименту 5)

Згідно результатів експерименту, швидкість протоколу КПБЗ із застосуванням запропонованого методу забезпечення стійкості мінімум у 5,45 раз краща за швидкість відомого методу (для $r = 4$). Причому, при збільшенні r покращення швидкодії буде ще більш показовим. Наприклад, при $r = 20$ швидкодія запропонованого методу краща у 125,53 раз.

Експеримент 6. Нехай $V_x = 10^6$, $V_{kl} = 10^5$, $V_{gen} = 10^4$, $V_{kv} = 10^3$, $l = 1000$, $q = 0,5$ – для відомого методу забезпечення стійкості протоколів КПБЗ, $q = 0,05$ для запропонованого методу.

На рис. 7 наведено результати експерименту 6 порівняння швидкодії протоколу КПБЗ для різних методів забезпечення його стійкості.

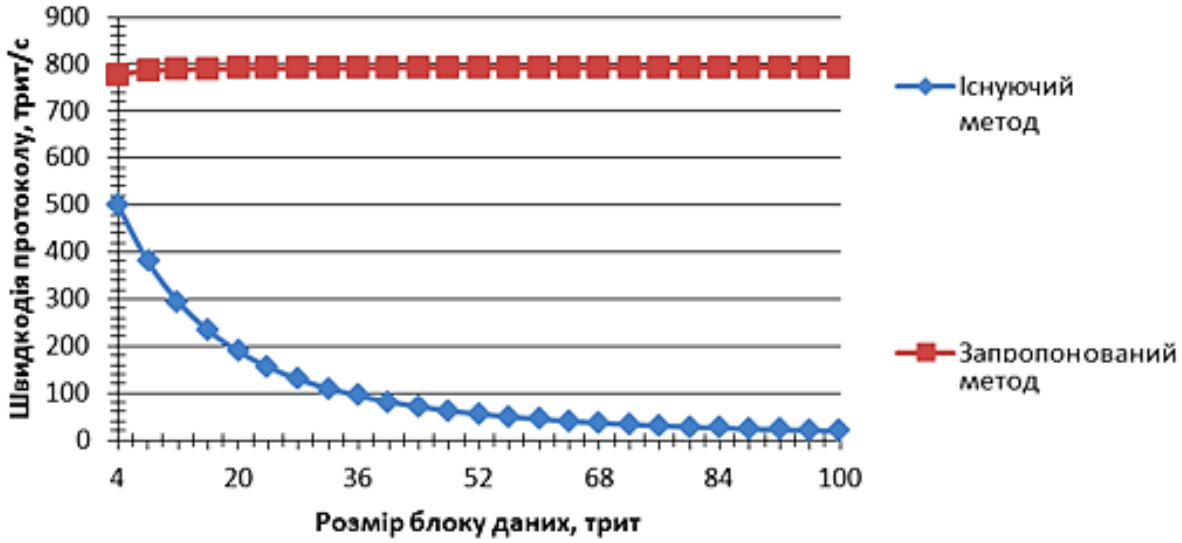

Рис. 7. Порівняння швидкісних характеристик протоколу КПБЗ (результати експерименту 6)

Згідно результатів експерименту, швидкість протоколу КПБЗ із застосуванням запропонованого методу забезпечення стійкості мінімум у 1,55 раз є більшою за швидкість відомого методу (для $r = 4$). Причому при збільшенні r покращення швидкодії буде ще більш показовим. Наприклад, при $r = 20$ швидкодія запропонованого методу краща у 4,18 рази.

Експеримент 7. Нехай $V_x = 10^5$, $V_{kl} = 10^6$, $V_{gen} = 10^4$, $V_{kv} = 10^3$, $l = 1000$, $q = 0,5$ – для відомого методу забезпечення стійкості протоколів КПБЗ, $q = 0,05$ для запропонованого методу.

На рис. 8 наведено результати експерименту 7 із порівняння швидкодії протоколу КПБЗ для різних методів забезпечення його стійкості.

Згідно результатів експерименту, швидкість протоколу КПБЗ із запропонованим методом забезпечення стійкості мінімум у 1,83 раз є більшою за швидкість відомого методу (для $r = 4$). Причому, при збільшенні r покращення швидкодії буде ще більш показовим. Наприклад, при $r = 20$ швидкодія запропонованого методу краща у 14,39 раз.

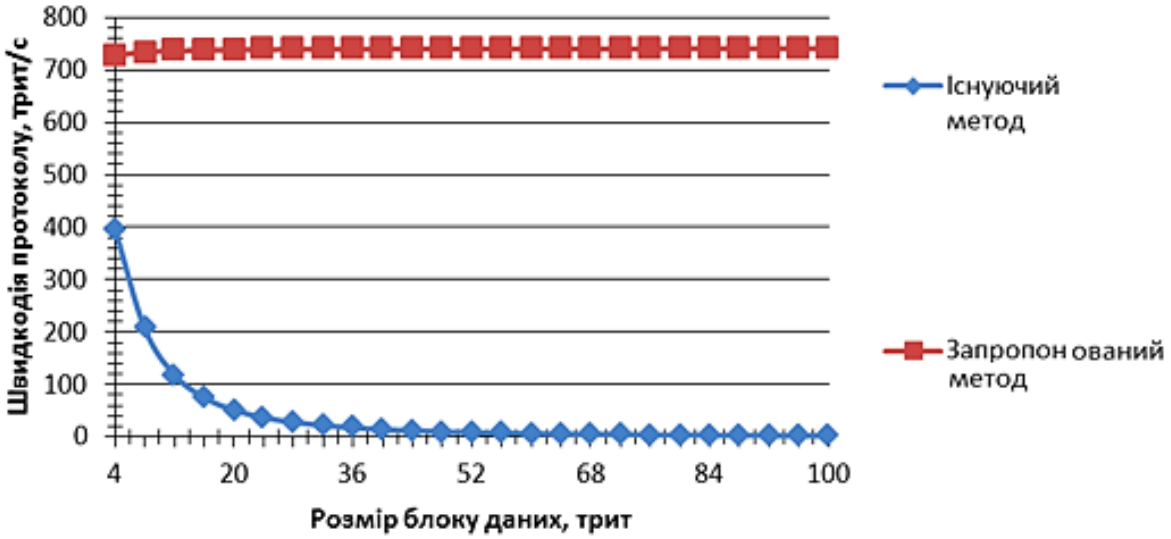

Рис. 8. Порівняння швидкісних характеристик протоколу КПБЗ (результати експерименту 7)

Отже, згідно з результатами експериментів, швидкість протоколу КПБЗ із застосуванням запропонованого методу забезпечення стійкості мінімум у 1,52 раз є більшою за швидкість відомого методу. Проте варто зауважити, що такі результати отримано для $r = 4$. У роботі [6] зазначається, що легітимні користувачі можуть підібрати параметри протоколу (розмір блоку r, ймовірність перемикання в режим контролю підслуховування q та інші параметри) так, щоб ймовірність успішної некогерентної атаки Єви після передачі одного блоку розміром r була нехтовно малою величиною. Можна зробити висновок, що для ефективного використання відомого та запропонованого методів забезпечення стійкості протоколів КК рекомендований розмір $r \geq 20$, в такому випадку швидкодія запропонованого методу мінімум краща у 4,4 рази.

Висновки. Проведено моделювання роботи протоколу КПБЗ із запропонованим та відомим методом забезпечення стійкості протоколів КК до некогерентних атак. Згідно з результатами, швидкість протоколу КПБЗ із запропонованим методом забезпечення стійкості мінімум у 1,52 раз при $r = 4$ більша ніж швидкість відомого методу, а оскільки у КК рекомендований розмір $r \geq 20$, в такому випадку швидкодія запропонованого методу як мінімум більша у 4,4 рази.

ЛІТЕРАТУРА

[1]. Василиу Е.В. Безопасные системы передачи конфиденциальной информации на основе протоколов квантовой криптографии : монография / Е.В. Василиу, В.Я. Мильчевич, С.В. Николаенко, А.В. Мильчевич. – Харьков: Цифровая типография № 1, 2013. – 168 с.

[2]. Василиу Е.В. Синтез основанной на пинг-понг протоколе квантовой связи безопасной системы прямой передачи сообщений / Е.В. Василиу, С.В. Николаенко // Наукові праці ОНАЗ ім. О.С. Попова. – 2009, № 1. – С. 83-91.

[3]. Гнатюк С.О. Метод підвищення захищеності систем захисту інформації на базі квантових технологій / С.О. Гнатюк, Т.О. Жмурко, А.Д. Стояновіч, Н.А. Сейлова // Стан та удосконалення безпеки інформаційно-комунікаційних систем (SITS'2015) – Миколаїв: 2015. – С. 93-96.

[4]. Корченко О.Г. Сучасні квантові технології захисту інформації / О.Г. Корченко, Є.В. Васіліу, С.О. Гнатюк // Захист інформації. – 2010. – № 1. – С. 77–89.

[5]. Методы перехвата информации в информационно-коммуникационных системах на основе

квантових технологий / А.Г. Корченко, Е.В. Василиу, Т.А. Жмурко, С.А. Гнатюк // Информационные технологии и системы в управлении, образовании, науке: Монография [под. ред. В.С. Пономаренко]. – Харків: Цифрова друкарня № 1, 2013. – С. 98-110.

[6]. Новий метод підсилення секретності пінг-понг протоколу з парами переплутаних кутритів / В.М. Кінзерявий, Є.В. Васіліу, С.О. Гнатюк, Т.О. Жмурко// Захист інформації. – 2012. – №2 (55). – С. 5-13.

[7]. Vasiliu Ye. Security amplification of the ping-pong protocol with many-qubit Greenberger-Horne-Zeilinger states / Ye. Vasiliu, S. Gnatyuk, S. Nikolayenko, T. Zhmurko// Безпека інформації. – 2012. – Т. 18. – № 2. – С. 84-88.

[8]. Gnatyuk S. Efficiency increasing method for quantum secure direct communication protocols / S. Gnatyuk, T. Zhmurko, P. Falat // Proceedings of the 2015 IEEE 8th International Conference on «Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications» (IDAACS'2015), Warsaw, Poland, September 24-26, 2015: Vol. 1. – P. 468-472.

[9]. Korchenko O. Modern quantum technologies of information security against cyber-terrorist attacks / O. Korchenko, Y. Vasiliu, S. Gnatyuk // Aviation. Vilnius : Technika. – 2010. – Vol. 14, Iss. 2. – P. 58-69.

[10]. Korchenko O. Quantum Secure Telecommunication Systems / Korchenko O., Vasiliu Ye., Gnatyuk S. et al. // Telecommunications Networks – Current Status and Future Trends (ed. by J.H. Ortiz). – InTech, 2012. – P. 211-236.

REFERENCES

[1]. Vasiliu Ye. Secured systems for transmission of confidential information on the basis of the quantum cryptography protocols: monograph / Ye.Vasiliu, V. Milchevich, S. Nikolayenko, A. Milchevich. – Kharkiv: Tsyfrovaya Typography № 1, 2013, 168 p.

[2]. Vasiliu Ye. Synthesis based on the ping-pong protocol of quantum secure direct communication messaging / Vasiliu Ye, Nikolayenko S.// Scientific works of ONAT named after O.S. Popov, 2009, № 1, P. 83-91.

[3]. Gnatyuk S. Method for increasing the security of information security systems based on quantum technologies / Gnatyuk S, Zhmurko T., Stoyanovich A., Seylova N. // SITS'2015, Mykolayiv: 2015, P. 93-96.

[4]. Korchenko O. Modern quantum information security technologies / O. Korchenko, Y. Vasiliu, S. Gnatyuk // Ukrainian information security research journal., 2010, № 1, P. 77-89.

[5]. Methods of information interception in information and communication technologies based on quantum systems / Korchenko O., Vasiliu Ye., Gnatyuk S, Zhmurko T.// Information Technologies and Systems in Management, Education, Science: Monograph [under. ed. V.S. Ponomarenko]. – Kharkiv: Tsyfrovaya Typography № 1, 2013, P. 98-110.

[6]. New method for amplification secrecy of ping-pong protocol with pairs of entangled qutrits / V. Kinzeryavyy, Ye. Vasiliu, S. Gnatyuk, T. Zhmurko // Ukrainian information security research journal., 2012, №2 (55), P. 5-13.

[7]. Vasiliu Ye. Security amplification of the ping-pong protocol with many-qubit Greenberger-Horne-Zeilinger states / Ye. Vasiliu, S. Gnatyuk, S. Nikolayenko, T. Zhmurko// Ukrainian scientific journal of information security, 2012, I. 18, № 2, P. 84-88.

[8]. Gnatyuk S. Efficiency increasing method for quantum secure direct communication protocols / S. Gnatyuk, T. Zhmurko, P. Falat // Proceedings of the 2015 IEEE 8th International Conference on «Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications» (IDAACS'2015), Warsaw, Poland, September 24-26, 2015: Vol. 1, P. 468-472.

[9]. Korchenko O. Modern quantum technologies of information security against cyberterrorist attacks / O. Korchenko, Y. Vasiliu, S. Gnatyuk // Aviation. Vilnius : Technika., 2010, Vol. 14, Iss. 2, P. 58-69.

[10]. Korchenko O. Quantum Secure Telecommunication Systems / Korchenko O., Vasiliu Ye., Gnatyuk S. et al. // Telecom-munications Networks – Current Status and Future Trends (ed. by J.H. Ortiz)., InTech, 2012, P. 211-236.

ЭКСПЕРИМЕНТАЛЬНОЕ ИССЛЕДОВАНИЕ МЕТОДА ОБЕСПЕЧЕНИЯ СТОЙКОСТИ КУРТИТОВЫХ ПРОТОКОЛОВ КВАНТОВОЙ КРИПТОГРАФИИ

Сегодня остро стоит вопрос обеспечения конфиденциальности информации в условиях роста количества и качества нарушений в киберпространстве, которые постоянно совершенствуются и развиваются. Надежность традиционных методов обеспечения конфиденциальности вызывает сомнения учитывая современные угрозы. Поэтому поиск альтернативных методов и способов защиты является актуальным вопросом. Значительный интерес вызывает квантовая криптография, которая не зависит от вычислительных или иных возможностей нарушителя, использует специфические уникальные свойства квантовых частиц и основывается на незыблемости законов квантовой физики. Одной из наиболее развитых технологий квантовой криптографии является квантовая прямая безопасная связь, которая позволяет передавать информацию открытым каналом напрямую (без предварительного ее

шифрования – проблема распределения ключей нивелируется), однако они имеют лишm асимптотическую устойчивость к некогерентным атакам и, безусловно, нуждаются в методах повышения безопасности. В связи с этим разработан метод обеспечения устойчивости протоколов квантовой криптографии. Для оценки эффективности этого метода была разработана методика проведения экспериментального исследования, согласно которой выполнено сравнение его быстродействия с известным методом. Согласно полученным результатам, предложенный метод имеет скорость в 1,52 раза больше чем аналоги при том же уровне устойчивости к некогерентным атакам.
Ключевые слова: квантовая криптография, квантовая прямая безопасная связь, трит, защита информации.

EXPERIMENTAL RESEARCH OF EFFICIENCY INCREASING METHOD FOR QUTRITS QUANTUM CRYPTOGRAPHY PROTOCOLS

Today acutely raises the issue of providing information confidentiality in conditions of growth quantity and quality of violations in cyberspace that are constantly improving and developing. Reliability of traditional methods for ensuring confidentiality is questionable taking into account contemporary threats. So look for alternative methods and means of security is urgent issue. Significant interest causes quantum cryptography, which do not depend on computing or other capabilities of offender, uses specific unique properties of quantum particles, and based on the inviolability of the laws of quantum physics. One of the most advanced technology of quantum cryptography is quantum secure direct communication, which can transmit information directly by open channel (without encryption – in this case there is no key distribution problem), but they have only asymptotic resistance to noncoherent attacks and, certainly requires some methods for amplification security. In this regard, developed a method of ensuring the stability of quantum cryptography protocols. To evaluate the effectiveness of this method was developed a methodology for conducting experimental research, according to which it is made comparing of its performance with known method. According to the obtained results, the proposed method has a speed in 1.52 times faster against analogs at the same level of resistance to noncoherent attacks.
Keywords: quantum cryptography, quantum secure direct communication, trit, information security.

Гнатюк Сергій Олександрович, кандидат технічних наук, доцент, доцент кафедри безпеки іфнормаційних технологій Національного авіаційного університету.
E-mail: s.gnatyuk@nau.edu.ua.
Гнатюк Сергей Александрович, кандидат технических наук, доцент, доцент кафедры безопасности информационных технологий Национального авиационного университета.
Gnatyuk Sergiy, PhD in Eng, Associate Professor of IT-Security Academic Department, National Aviation University.

Жмурко Тетяна Олександрівна, кандидат технічних наук, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету.
E-mail: taniazhm@gmail.com.
Жмурко Татьяна Александровна, кандидат технических наук, доцент кафедры безопасности информационных технологий Национального авиационного университета.
Zhmurko Tetiana, PhD in Eng., Associate Professor of IT-Security Academic Department, National Aviation University.

Кінзерявий Василь Миколайович, кандидат технічних наук, доцент кафедри безпеки іфнормаційних технологій Національного авіаційного університету.
E-mail: v.kinzeryavyy@gmail.com.
Кинзерявый Василий Николаевич, кандидат технических наук, доцент кафедры безопасности информационных технологий, Национальный авиационный университет.
Kinzeryavyy Vasyl, PhD in Eng., Associate Professor of IT-Security Academic Department, National Aviation University.

Юбузова Халіча Ібрагімівна, старший викладач кафедри інформаційної безпеки Казахського національного дослідницького технічного університету ім. К.І. Сатпаева (Алмати, Казахстан).
E-mail: hali4a@mail.ru.
Юбузова Халича Ибрагимовна, старший преподаватель кафедры информационная безопасность Казахского национального исследовательского технического университета им. К.И. Сатпаева (Алматы, Казахстан).
Yubuzova Khalicha, Senior Lecturer of Information Security Academic Department, Kazakh National Research Technical University named after K.I. Satpayev (Almaty, Republic of Kazakhstan).