УДК 621.391:519.2 **DOI:10.30837/rt.2024.3.218.08**

Є.В. КОТУХ, канд. техн. наук, Г.З. ХАЛІМОВ, д-р техн. наук, І.Є. ДЖУРА

ПРОБЛЕМА ЗНАХОДЖЕННЯ ПЕРІОДИЧНОСТІ В КВАНТОВОМУ КРИПТОАНАЛІЗІ АЛГОРИТМІВ ГРУПОВОЇ КРИПТОГРАФІЇ

Вступ

Алгоритми пошуку квантового періоду є центральним компонентом квантових обчислень, особливо в задачах, де періодичність відіграє ключову роль, наприклад алгоритм Шора (для цілочисельної факторизації) та інші програми, що включають періодичні функції над групами. Ці алгоритми використовують принципи квантової суперпозиції та інтерференції, щоб знайти період даної функції експоненціально швидше, ніж класичні алгоритми. Нижче наведено огляд алгоритму визначення квантового періоду, його теоретичні основи та порівняння з існуючими квантовими та класичними методами. Щоб забезпечити повний аналіз алгоритмів пошуку періоду для різних типів груп, включаючи групи Сузукі, Ерміта та Рі, потрібно спочатку зрозуміти загальну структуру та властивості цих груп у зв'язку з квантовими алгоритмами, зокрема з проблемою знаходження періодичності.

Аналіз літератури

Квантові алгоритми визначення періоду відіграють основоположну роль у квантових обчисленнях і криптоаналізі, зокрема завдяки їх застосуванню в алгоритмі Шора, який дає змогу ефективно розкладати великі цілі числа на множники та обчислювати дискретні логарифми. Ці завдання мають вирішальне значення для безпеки багатьох широко використовуваних криптографічних систем, таких як шифрування RSA. Новаторська робота Пітера Шора в 1994 р. продемонструвала, як квантовий комп'ютер може вирішувати ці проблеми експоненціально швидше, ніж класичні методи, створюючи серйозну проблему для класичної криптографії [1]. Алгоритм Шора використовує квантове перетворення Фур'є (QFT) для ідентифікації періоду даної функції, підхід, який став основою для багатьох квантових алгоритмів, що вирішують криптографічні проблеми. Алгоритм пошуку періоду є ключовим для ефективного вирішення таких проблем, як цілочисельна факторізація, яка є центральною для зламу RSA. Це викликало інтерес до квантово-стійких криптографічних систем [2, 3].

Класичні алгоритми для пошуку періоду, такі як алгоритм Ро Полларда, мають значні обмеження, коли йдеться про обробку великих вхідних даних. Алгоритм Полларда Ро, хоч і ефективний для певних циклічних групових структур, працює з експоненціальною складністю часу, що робить його непрактичним для більших екземплярів [4]. Класичні методи грубої сили також неможливі для великих періодів, оскільки вони вимагають перевірки кожного можливого введення, доки не буде знайдено повторення, зі складністю O(T), де T - період.

З іншого боку, квантові алгоритми, такі як Шор, працюють у поліноміальному часі та пропонують експоненціальне прискорення порівняно з класичними методами. Алгоритм Шора, зокрема, має часову складність O((log N)^3), де N є цілим числом, яке розкладається на множники, порівняно з класичною експоненційною складністю O(exp(log N)^c) [1]. Це різке прискорення робить визначення квантового періоду ключовим інструментом у квантовому криптоаналізі, де його можна застосовувати для ефективного зламу класичних криптографічних систем [5].

Квантове перетворення Фур'є (QFT) є основним для квантових алгоритмів пошуку періоду, включаючи алгоритм Шора. QFT ефективно обчислює частотні компоненти періодичної функції, дозволяючи визначити період у логарифмічному часі відносно розміру вхідних даних. Алгоритм Шора починається з ініціалізації суперпозиції станів, застосовує квантовий оракул для обчислення періодичної функції, а потім використовує QFT для

виділення періоду Nielsen2002. Однак застосування КТП до неабелевих груп значно складніше. У випадках, пов'язаних із неабелевими структурами, такими як групи Сузукі та Рі, квантове перетворення Фур'є є багатовимірним і менш простим, що робить пошук періоду в цих групах відкритою дослідницькою проблемою [6]. Ці групи мають вирішальне значення для вивчення проблем прихованих підгруп (HSP) у квантовій криптографії, де поточні квантові алгоритми не можуть ефективно виділити періодичність [7].

Хоча квантові алгоритми показали значний успіх з абелевими групами, неабелевий випадок залишається набагато складнішим. Неабелеві групи, такі як групи Сузукі, Ерміта та Рі, є більш складними через їх багатовимірні представлення та некомутативний характер їхніх елементів. Ці властивості роблять застосування квантових алгоритмів, особливо алгоритмів пошуку періоду, експоненціально складнішим [3].

Наприклад, група Сузукі є неабелевою простою кінцевою групою типу Лі зі скрученою структурою Шевалле. Квантові алгоритми для знаходження періоду борються з цими групами, тому що їхня теорія представлення є набагато більш залученою, і для таких груп не існує ефективної КТП [6]. Подібні проблеми спостерігаються з ермітовими (унітарними) і групами Рі, де періодичність прив'язана до власних значень матриці або скручених автоморфізмів, а поточні квантові методи не пропонують ефективних рішень [8].

Квантовий пошук періоду лежить в основі багатьох криптографічних атак, особливо тих, які загрожують безпеці RSA та криптографії на основі еліптичної кривої. Алгоритм Шора, який використовує пошук періоду для ефективного розкладання цілих чисел, безпосередньо підриває схему шифрування RSA, оскільки безпека RSA залежить від складності розкладання великих цілих чисел [1]. Окрім RSA, визначення квантового періоду також можна застосовувати до таких проблем, як проблема дискретного логарифмування як у скінченних полях, так і в групах еліптичних кривих. Якби були розроблені ефективні квантові алгоритми для неабелевих груп, це могло б призвести до зламу криптографічних систем, які покладаються на жорсткість цих проблем [9]. Незважаючи на прориви, які забезпечують квантові алгоритми визначення періоду, залишаються значні проблеми у застосуванні цих методів до структур неабелевих груп. Продовжуються дослідження щодо розробки ефективних квантових алгоритмів для проблеми прихованих підгруп (HSP) у неабелевих групах, що дозволить квантовим комп'ютерам вирішувати більш широкий спектр криптографічних задач [7]. Розвиток постквантової криптографії, яка спрямована на розробку криптографічних алгоритмів, стійких до квантових атак, є ще одним важливим напрямком поточних досліджень [10, 11].

Метою цієї статті є визначення квантової проблеми знаходження періоду, вивчення її поточного стану щодо неабелевих груп та аналіз критеріїв складності, пов'язаних з найбільш помітними групами, що використовуються в криптографічних програмах.

Результати досліджень

Групи Сузукі, Ерміта та Рі є конкретними прикладами неабелевих груп, що додає значного рівня складності квантовим алгоритмам. Хоча ефективні алгоритми пошуку періоду існують для абелевих груп і деяких неабелевих випадків (такі, як двогранні групи), проблема знаходження періоду залишається складною в цих більш складних групах типу Лі.

Група Сузукі неабелева, проста, скінченна, типу Лі, скручена група Шевалле. Їх позначають як Sz (q), та вона є частиною більшого класу скручених груп Шевалле, що визначаються для полів характеристики 2, де $q = 2^{2n+1}$. Групи Сузукі демонструють високосиметричні, некомутаційні структури. Вони існують для непарних ступенів числа 2 і класифікуються як прості групи (групи без нетривіальних нормальних підгруп). Група має складну внутрішню структуру, яка включає польові автоморфізми та вимагає передових методів теорії Лі та алгебраїчної геометрії для опису. Порядок групи Сузукі дорівнює $Sz(q):\left|Sz(q)\right| = q^2\left(q-1\right)\left(q^2+1\right)$. Періодичність у групах Сузукі надзвичайно важко проаналізувати. Оскільки групи Сузукі є неабелевими, їх теорія представлення набагато складніша, ніж теорія абелевих груп. Квантові алгоритми, які покладаються на перетворення

Фур'є, такі як алгоритм Шора, погано працюють для груп Сузукі, оскільки їх структура призводить до багатовимірних представлень. Квантове перетворення Фур'є (QFT) не є простим, і для груп Сузукі невідомо ефективних алгоритмів пошуку періоду. Отримання інформації про підгрупи в групах Сузукі залишається обчислювально складним. Групи Сузукі вивчаються в контексті скінченних простих груп і груп типу Лі, і розв'язання проблеми HSP для цих груп дасть суттєве розуміння ширшого класу квантових проблем. Відсутність ефективних алгоритмів відображає загальну проблему вирішення проблем знаходження періоду для неабелевих груп.

Ермітові (унітарні) групи є неабелевими, класичними групами. Ермітові групи, також відомі як унітарні групи, складаються з матриць, які зберігають ермітову форму (внутрішній добуток на складні векторні простори). Унітарна група U(n, q) складається з n помножених на n матриць над полем q, де кожна матриця задовольняє умову $U^{\dagger}U = I$ (зберігає ермітову форму). Ермітові групи є неабелевими, коли n > 1, що робить їх частиною класичної групи груп, яка зберігає певні симетрії під час перетворень. Ці групи відіграють важливу роль у квантовій механіці та квантових обчисленнях, оскільки унітарні перетворення керують квантовою еволюцією. Ермітові групи мають складні структури власних значень, періодичність яких пов'язана з властивостями власних значень. Періодичність у ермітових групах пов'язана з поведінкою власних значень. Наприклад, періодичність унітарних матриць включає обертальну симетрію в комплексних векторних просторах. З квантовим перетворенням Фур'є над унітарними групами стає важче працювати через багатовимірну природу представлення, особливо зі збільшенням розміру матриці n. Квантові алгоритми, які включають унітарні матриці (такі як алгоритми quantum walk або алгоритми HSP), повинні мати справу з періодичністю, яка виникає внаслідок складних обертальних симетрій. Для алгоритмів пошуку періоду завдання полягає в ефективному виявленні повторюваних власних значень або шаблонів у перетвореннях матриці, що потребує інтенсивних обчислень і значної постобробки. Ермітові групи тісно пов'язані з проблемами квантової криптографії та квантової корекції помилок, де унітарні операції є фундаментальними. HSP для унітарних груп ще не є ефективно розв'язаним, що відображає ширшу складність вирішення квантових проблем для неабелевих груп. Для виділення періодичності в таких групах часто потрібні методи з теорії представлень і алгебр Лі.

Групи Рі є неабелевими, простими, скрученими групами Шевалле типу Лі. Їх позначають $G_2(q)$ або $F_4(q)$, це кінцеві прості групи, визначені над полями характеристики 3 замість 2 (як це визначено для групи Сузукі). Як і групи Сузукі, вони належать до класу скручених груп Шевалле і виникають із специфічних автоморфізмів алгебраїчних груп. Порядок груп Рі відповідає структурі основної алгебраїчної групи (наприклад, $G_2(q)$ і $F_4(q)$), звичайно може бути описаний за допомогою автоморфізмів скручених полів. Порядок груп Рі дорівнює $G_2(q) = q^3\left(q^3+1\right)\left(q-1\right)$, де $q = 3^n$. Періодичність у групах Рі важко проаналізувати через їхню високосиметричну структуру та складність спотворених автоморфізмів, які їх визначають. Квантові алгоритми борються з неабелевою природою груп Рі. Немає відомого ефективного алгоритму для вирішення проблем пошуку періодів або прихованих підгруп у цих групах. Багатовимірні представлення, які не піддаються ефективному перетворенню Фур'є або алгоритмам quantum walk, ще більше ускладнюють вилучення періодичної інформації. Як і групи Сузукі, групи Рі є частиною класифікації скінченних простих групп. Розуміння того, як вирішити HSP для цих групп, є вирішальним для вдосконалення методів квантових обчислень, що відображає ширшу складність неабелевих груп у квантових алгоритмах. Вирішення проблем знаходження періоду для груп Рі, ймовірно, вимагатиме прориву в теорії квантового представлення та квантової інформаційної науки.

Визначення проблеми

Проблему знаходження квантового періоду можна описати так:

Дано функцію $f:\mathbf{Z}\to G$, де G – деяка група, яка є періодичною з періодом r (тобто $f(x)=f(x+r)$ для всіх $x\in\mathbf{Z}$), завдання полягає в тому, щоб визначити період r.

Кроки в алгоритмі пошуку квантового періоду

К р о к 1 *Суперпозиція.* Ініціалізувати квантовий регістр у суперпозиції всіх можливих входів $|x\rangle$, де $x\in\mathbf{Z}$:

$$\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle.$$

К р о к 2. *Оцінка функції.* Застосуйте квантовий оракул для обчислення функції $f(x)$, поєднуючи результат із вхідними даними:

$$\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle|f(x)\rangle.$$

Мета полягає в тому, щоб виміряти r період $f(x)$.

К р о к 3. *Квантове перетворення Фур'є.* Застосуйте QFT до першого регістру (який містить суперпозицію вхідних даних):

$$\frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}e^{2\pi ikx/r}|k\rangle.$$

QFT виявляє частотні компоненти функції, надаючи інформацію про періодичність.

К р о к 4. *Вимірювання.* Після застосування QFT виміряємо стан системи. З високою ймовірністю результат дасть кратне $1/r$, що дозволить визначити період r.

Квантовий алгоритм пошуку періоду працює за поліноміальний час, пропонуючи експоненціальне прискорення порівняно з класичними алгоритмами, які вимагають експоненціального часу в найгіршому випадку для визначення періоду. Це пов'язано з тим, що QFT можна ефективно обчислити в $O(n^2)$ часі, де n – кількість кубітів, які використовуються для представлення вхідного простору. Прикладом вирішення проблеми є існування квантового комп'ютера IBM на 127 кубітів. Проблема знаходження періоду є ядром алгоритму Шора для розкладання великих цілих чисел на множники. Період відповідає порядку числа за модулем N, і знаходження цього періоду дозволяє ефективно розкласти на множники. Пошук періоду тісно пов'язаний з HSP в абелевих групах, де ідентифікація прихованої підгрупи еквівалентна ідентифікації періоду функції.

Існують деякі класичні підходи. Класичні підходи грубої сили для пошуку періоду вимагають багаторазового оцінювання функції для різних вхідних даних, доки не буде знайдено повторення. Складність $O(r)$, де r – період. Цей спосіб стає неможливим протягом тривалого часу. Хоча алгоритм Ро Полларда пропонує швидший підхід для знаходження періодів у певних структурах циклічної групи (наприклад, для дискретних логарифмів або цілочисельної факторизації), він все ще працює в експоненціальному часі відносно розміру вхідних даних.

Як згадувалося раніше, алгоритм Шора використовує пошук квантового періоду як свою основну підпрограму. Він знаходить період модульної функції піднесення до степеня, що призводить до ефективної цілочисельної розкладки. Складність дорівнює $O\left((\log N)^2\right)$ для розкладання N-розрядного цілого числа.

Алгоритм Саймона знаходить період (або приховану маску XOR) функції, яка є періодичною щодо операції XOR. Він працює за поліноміальний час, але вирішує інший тип про-

блеми періодичності порівняно з алгоритмом Шора. Складність дорівнює $O\left(n^2\right)$, де n – кількість бітів у вхідних даних.

Багато квантових алгоритмів для HSP спираються на принципи визначення періоду. Для абелевих груп складність залишається поліноміальною, але для неабелевих груп складність значно зростає (часто стає експоненціальною), оскільки квантове перетворення Фур'є стає важчим для інтерпретації. Хоча алгоритми Шора та Саймона пропонують ефективний пошук періоду для певних типів періодичностей (модульних та XOR відповідно), їхня складність залишається поліноміальною. Однак для неабелевих груп або інших складних структур квантові алгоритми можуть не мати такої переваги.

Таблиця 1

Порівняльний аналіз

Тип групи	**Періодичність**	**Застосування QFT**	**Інші квантові алгоритми**	**Складність**	**Квантова складність**	**Зауваження**
Абелеві	Однозначно існує	Існує ефективна одновимірна QFT	Шор, Саймон, Знахідка періоду	$O(r)$ для фінансування періоду грубої сили	$O\left((\log N)^2\right)$ для алгоритму Шора	Жодних проблем: проста структура, чітка періодичність, легкий QFT.
Циклічні	Чітко визначена періодичність як порядок групи	Ефективний, працює подібно до абелевого випадку	Шор, Саймон	$O(N)$	$O\left((\log N)^2\right)$ для алгоритму Шора	Жодних проблем: більшість проблем можна ефективно вирішити за допомогою QFT
Двогранні	Періодичність включає симетрію як обертання, так і відображення.	Виклик QFT через неабелеву структуру	Субекспоненціальні алгоритми для HSP	$O(r)$	Субекспоненціальний	Проблема: неабелева природа ускладнює пошук підгрупи.
Симетричні	Періодичність на основі перестановок у структурах циклу	Експоненціально складна КТП	Ефективних алгоритмів невідомо	$O(n!)$	Експоненціальний	Завдання: багатовимірна QFT потрібна і залишається відкритою проблемою.
Неабелеві	Складна періодичність, яку часто важко визначити	Багатовимірна QFT, дуже складна	Ефективних алгоритмів невідомо	Експоненціальний	Експоненціальний	Завдання: некомутативна природа груп
Сузукі	Високосиметрична, неабелева, скручена періодичність	Дуже складно, без ефективного QFT	Ефективних алгоритмів невідомо	Експоненціальний	Експоненціальний	Виклик: належить до спотворених груп типу Брехні, важко аналізувати.

Рі	Високо-симетрична, неабелева, скручена періодичність	Дуже складно, без ефективного QFT	Ефективних алгоритмів невідомо	Експонен-ціальний	Експонен-ціальний	Виклик: належить до спотворених груп типу Брехні, важко аналізувати
Ерміта	Періодичність прив'язана до структури власних значень матриці	Складно через пред-ставлення на основі матриці	Ефективних алгоритмів невідомо	Експонен-ціальний	Експонен-ціальний	Завдання: періодичність на основі власних значень і QFT
Вінцевого добутку	Періодичність походить від добутку циклічних та інших груп	Багато-вимірна QFT, дуже складна	Ефективних алгоритмів невідомо	Експонен-ціальний	Експонен-ціальний	Завдання: складне поєднання циклічної та двогранної структур.
Кінцеві прості	Складна періодичність за рахунок структури простих груп	QFT взагалі нездійсненна для неабелевих	Немає ефективних алгоритмів	Експонен-ціальний	Експонен-ціальний	Виклик: те саме для Suzuki, Ree та інших груп
Кінцеві поля	Періодичність легко визначити завдяки добре структурованому полю	Ефективна QFT для абелевих підполів	Алгоритм Шора для скінченних полів	$O(q)$	$O\left((\log q)^2\right)$	Завдання: тільки абелеві підгрупи мають ефективне рішення фінансування періодичності

Висновок

Виявлення квантового періоду є одним із найважливіших проривів у квантових обчисленнях, що дозволяє ефективно розв’язувати проблеми, які класично нерозв’язні. Хоча ці алгоритми працюють виключно добре для абелевих груп, неабелеві групи створюють значні проблеми. Потрібні подальші дослідження, щоб розкрити весь потенціал квантових алгоритмів для неабелевих структур, але наразі квантові алгоритми, такі як Шора та Саймона, залишаються найпотужнішими інструментами для пошуку періоду в абелевих налаштуваннях. Результати порівняльного аналізу представлено в табл. 1.

Основна проблема у застосуванні квантових алгоритмів для проблеми прихованих підгруп (HSP) у неабелевих групах пов’язана зі складністю ефективного вилучення інформації про підгрупи за допомогою квантових перетворень Фур’є. У випадку абелевих груп алгоритм Шора та пов’язані з ним методи досягають успіху завдяки здатності виконувати ефективну квантову вибірку за Фур’є, яка фіксує достатньо інформації для ідентифікації прихованої підгрупи. Однак у неабелевих групах квантове перетворення Фур’є стає значно складнішим, оскільки уявлення груп більше не є одновимірними. Ця складність призводить до труднощів з ефективним обчисленням або інтерпретацією квантових зразків Фур’є, які поширені у просторах вищої розмірності. Як наслідок, існуючим квантовим алгоритмам важко визначити приховані підгрупи в неабелевих групах, особливо коли підгрупа не є нормальною або легко виділяється. Більше того, неабелев HSP включає знамениті складні проблеми, такі як ізоморфізм графів, де проблема прихованих підгруп для симетричних груп, як відомо, є важкою. Спроби узагальнити успішні абелеві методи на неабелеві випадки часто призводять до неповних або неоптимальних рішень, що вимагає нових квантових алгоритмічних методів або розуміння теорії представлень. Крім того, неабелеві групи можуть проявляти більш складну та непередбачувану поведінку під час вибірки квантових станів, що ускладнює зусилля з розробки ефективних алгоритмів.

Список літератури

1. Shor P. W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer // SIAM Journal on Computing. 1997. No 26(5). P. 1484–1509. https://epubs.siam.org/doi/10.1137/S0097539795293172
2. Nielsen M. A., & Chuang I. L. (2002). Quantum Computation and Quantum Information. Cambridge University Press. https://shorturl.at/09toE
3. Watrous J. Quantum Computational Complexity // Meyers, R. (eds) Encyclopedia of Complexity and Systems Science. Springer, New York, 2009. NY. https://doi.org/10.1007/978-0-387-30440-3_428
4. Pollard J. M. A Monte Carlo method for factorization // BIT Numerical Mathematics. 1975. No 15(3). P. 331–334. https://link.springer.com/article/10.1007/BF01933667
5. Simon D. R. On the Power of Quantum Computation // Proceedings of the 35th Annual Symposium on Foundations of Computer Science, 1994. https://ieeexplore.ieee.org/document/365701
6. Roetteler M., & Beth T. (1998). Polynomial-time solution to the hidden subgroup problem for a class of non-abelian groups. arXiv preprint quant-ph/9812070. https://arxiv.org/abs/quant-ph/9812070
7. Kuperberg G. A subexponential-time quantum algorithm for the dihedral hidden subgroup problem // SIAM Journal on Computing, 2005. No 35(1). P. 170–188. https://epubs.siam.org/doi/10.1137/S0097539703436345
8. Hallgren S., Russell A., & Ta-Shma A. The hidden subgroup problem and quantum computation using group representations // SIAM Journal on Computing, 2003. No 32(4). P. 916–934. https://epubs.siam.org/doi/abs/10.1137/S0097539701391800
9. Bernstein D. J., & Lange T. Post-quantum cryptography // Nature. 2017. No 549(7671). P. 188–194. https://www.nature.com/articles/nature23461
10. Regev O. On lattices, learning with errors, random linear codes, and cryptography // Journal of the ACM. 2005. No 56(6). P. 1–40. https://dl.acm.org/doi/10.1145/1568318.1568324
11. Peikert C. A decade of lattice cryptography // Foundations and Trends in Theoretical Computer Science. 2016. No 10(4). P. 283–424. https://shorturl.at/0CFgn
12. Kotukh Y., Khalimov G. Hard Problems for Non-abelian Group Cryptography // Fifth International Scientific and Technical Conference "Computer and Information systems and technologies". https://doi.org/10.30837/csitic52021232176
13. Kotukh Y., Khalimov G. Towards practical cryptoanalysis of systems based on word problems and logarithmic signatures // INFORMATION SECURITY: PROBLEMS AND PROSPECTS. https://shorturl.at/IaByX
14. Kotukh Y., Khalimov G. Advantages of logarithmic signatures in the implementation of crypto primitives // Challenges and Issues of Modern Science. https://cims.fti.dp.ua/j/article/download/119/158
15. Kotukh Y. Quantum cryptoanalysis of prospective asymmetric cryptosystems // Proceedings of conference “Cybersecurity in energy sector”. https://shorturl.at/1pbcK

Надійшла до редколегії 23.09.2024

Відомості про авторів:

Котух Євген Володимирович – канд. техн. наук, доцент, професор кафедри кібербезпеки; Національний технічний університет «Дніпровська політехніка»; Дніпро, Україна; e-mail: yevgenkotukh@gmail.com; ORCID: https://orcid.org/0000-0003-4997-620X

Халімов Геннадій Зайдулович – д-р техн. наук, професор, завідувач кафедри безпеки інформаційних технологій; Харківський національний університет радіоелектроніки; Харків, Україна; e-mail: hennadii.khalimov@nure.ua; ORCID: https://orcid.org/0000-0002-2054-9186

Джура Ілля Євгенович – студент 4-го курсу, Національний Авіаційний Університет; Київ, Україна; e-mail: illya773823@gmail.com; ORCID: https://orcid.org/0009-0002-5470-4479