ble means of evaluation based on semantic analysis. The use of methods allows you to obtain results, both in quantitative and qualitative form.
**Keywords**: differentiation of access, identification, granting rights to the user, semantic analysis, degree of semantic redundancy.

**Давиденко Анатолій Миколайович**, доктор технічних наук, старший науковий співробітник, провідний науковий співробітник відділу математичного і економетричного моделювання Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, Київ, Україна, професор кафедри безпеки інформаційних технологій Національного авіаційного університету, Київ, Україна.
**Anatolii Davydenko**, Doctor of Technical Sciences, Senior Researcher, Leader Researcher at the Department of Mathematical and Econometric Modeling of the G. E. Pukhov Institute for Modelling in Energy Engineering NAS of Ukraine, Kyiv, Ukraine, professor at the Department of security of information technologies of the National Aviation University, Kyiv, Ukraine.
E-mail: davidenkoan@gmail.com.
Orcid ID: 0000-0001-6466-1690.

**Висоцька Олена Олександрівна** – кандидат технічних наук, доцент кафедри комп'ютеризованих систем захисту інформації Національного авіаційного університету, Київ, Україна.
**Olena Vysotska** – Candidate of Technical Sciences, Associate Professor at the Department of Computerized Information Security Systems of the National Aviation University, Kyiv, Ukraine.
E-mail: lek_vys@ukr.net.
Orcid ID: 0000-0002-9543-1385.

**Пригара Михайло Петрович** – кандидат технічних наук, доцент кафедри технології машинобудування Державного вищого навчального закладу "Ужгородський національний університет", Київ, Україна.
**Mykhailo Prygara** – Candidate of Technical Sciences, Associate Professor at the Department of Mechanical Engineering Technology of the Uzhhorod National University, Kyiv, Ukraine.
E-mail: mykhailo.prygara@uzhnu.edu.ua
Orcid ID: 0000-0002-0954-4480.

**Бичков Володимир В'ячеславович**, старший викладач кафедри безпеки інформаційних технологій Національного авіаційного університету, помічник ректора Державного університету інформаційно-комунікаційних технологій.
**Volodymyr Bychkov**, Senior Lecturer at the Department of Information Technology Security at the National Aviation University, Assistant to the Rector of the State University of Information and Communication Technologies.
E-mail: bychkov.v@duikt.edu.ua.
Orcid ID: 0000-0002-1054-9182.

**DOI: 10.18372/2410-7840.26.18822**
**УДК 336.71:004.056**

# МЕТОД ВИЯВЛЕННЯ НЕПРАВДИВОЇ ІНФОРМАЦІЇ НА ОСНОВІ ЕКСПЕРТНОЇ ОЦІНКИ

***Наталія Лукова-Чуйко, Тетяна Лаптєва***

*У статті удосконалено метод виявлення неправдивої інформації на основі методу експертної оцінки. Експертні методи використовуються для визначення номенклатури показників якості, коефіцієнтів їх вагомості, для вимірювання показників якості і їх оцінки органолептичним методом. Оцінка показників якості вимірювальним, реєстраційним, розрахунковим методами застосовується для визначення комплексних показників якості різних рівнів ієрархії. Експертні методи засновані на ухваленні евристичних рішень, базою для яких є знання і досвід, накопичені експертами в конкретній області у минулому. Базовим методом для удосконалення, був обраний колективній метод експертних оцінок. Тому, що він має безсумнівні переваги в порівнянні з методами, заснованими на звичайній статистичній обробці результатів індивідуальних опитувань. На відміну від існуючого підходу, удосконалений метод дозволяє проводити відбір експертів у групу, а не корегувати відповіді експертів з метою отримання необхідного результату. Особливістю запропонованого методу є те що відбір експертів робиться за рахунок осереднення оцінок. Осереднення оцінок для кожного експерта. Самооцінки експерта та оцінки того ж самого експерта робочою групою. Це дозволяє значно зменшити похибку реальної оцінки експерта. Можливість встановлювати інтервал довіри до оцінки неправої інформації дозволять отримати результати які задовольняють завданню виявлення неправдивої інформації з належною точністю. Але це спонукає до вирішення завдання оптимізації критеріїв оцінки та часу вирішення встановленого завдання. Наукова новизна полягає в обґрунтуванні та оцінюванні порівняльної важливості факторів, що обмежують призначення кожного окремого експерта для виявлення неправдивої інформації за допомогою методу групової експертної оцінки. Напрямком подальших досліджень є завдання оптимізації критеріїв оцінки.*
***Ключові слова:*** *експерт, неправдива інформація, прогнозування, алгоритм, інформаційні технології.*

## ВСТУП

Метод експертних оцінок – це науковий метод, який дозволяє отримати об'єктивну оцінку на основі певної сукупності індивідуальних думок експертів. Слово «експерт» (expertus) у перекладі з латинської мови означає «досвідчений», що, в свою чергу, походить від слова «experire» – досліджувати. Експерт – це особа (спеціаліст), якому довірено висловити думку про якийсь суперечливий чи складний випадок, оскільки людство у складних ситуаціях завжди намагалося врахувати думку висококваліфікованих спеціалістів у різних сферах життєдіяльності [2].

Розрізняють два типи експертних оцінок:

1. Індивідуальні – такі оцінки ґрунтуються на думці одного чи кількох експертів, які працюють окремо один від одного. Рішення, що приймаються таким чином, можуть бути характерними і для колективної експертизи, але в цьому випадку вердикт ґрунтується на висновку лідера думки;

2. Колективні – підсумкова оцінка групи є об'єднаною думкою кількох експертів. Вона формується внаслідок попереднього узгодження всередині колективу.

Експертні методи засновані на ухваленні евристичних рішень, базою для яких є знання і досвід, накопичені експертами в конкретній області у минулому.

Експертним методам властиві певні переваги і недоліки.

Перевагами є те, що вони дозволяють ухвалювати рішення, коли об'єктивні методи неприйнятливі. До інших переваг відноситься їх відновлюваність.

Експертне знання - це поєднання теоретичного розуміння проблеми і набору евристичних правил для її вирішення. Як показує практика, універсальних евристичних прав не існує. Вироблені на основі знань, специфічних для певної предметної сфери, ці правила є, зазвичай, ефективними у відповідних практичних галузях. Експертні оцінки - це якісні оцінки, засновані на інформації неколичественного (якісного) характеру, які можуть бути одержані тільки з допомогою фахівців – експертів. Експерт – висококваліфікований спеціаліст, покладається на свої знання, досвід, інтуїцію та вміння оцінювати складні чинники (явища) і здатний створити власну обґрунтовану (інтуїтивний) модель аналізованого явища (проблеми), якщо він має необхідної для цього вихідною інформацією.

Чим вище кваліфікація, ерудиція, компетентність, креативне мислення експертів, тим обґрунтованій прогноз, а звідси, що вкрай важливо, його практична цінність. Відібрати групу експертів, кожен із яких відповідав би необхідним вимогам, практично неможливо. Задача формування стабільної експертної групи зводиться до визначення розміру і структури групи та оцінки компетентності експертів. Сутність колективного методу експертних оцінок полягає в логіко-інтуїтивному аналізі інформації. Узагальнена думка експертів служить підставою для здійснення висновку про категорії інформації, а саме правдива чи неправдива інформація. Виходячи з проведеного аналізу свідчить, що вивчення існуючих колективних методів експертної оцінки виявлення неправдивої інформації є актуальним науковим завданням.

## ПОСТАНОВКА ПРОБЛЕМИ

Визначення правдивості інформації колективним експертним методом має недоліки, а саме не в повній мірі відображені питання методологічного аналізу факторів визначення компетентності експертів для визначення неправдивої інформації. Тому треба удосконалювати та розробляти нові методи, які дозволять виділити ті критерії у підборі експертів, які дозволять визначати правдивість інформації з більшої ефективністю. Метою даної роботи є вирішення актуального наукового завдання по розробки методу виявлення неправдивої інформації на основі колективної експертної оцінки.

## АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Експертне знання – це поєднання теоретичного розуміння проблеми і набору евристичних правил для її вирішення. Важливою проблемою обрання кваліфікованих фахівців, експертів у всіх, без винятку, сферах життєдіяльності, особливо у галузі виявлення неправдивої інформації є підбір та залучення персоналу для проведення відбору експертів [1].

У роботах [2, 3] розглядаються методи ранжування для відбору спеціалістів з розробки програмного забезпечення. Але основне завдання по відбору експертів, з точки зору авторів, покладеться на керівника проекту. Саме на керівника проекту покладається відповідальність щодо призначення персоналу на виконання робіт проекту. Цей метод має суб'єктивний фактор, та може привести до помилкових призначень. Він може привести до призначення спеціаліста який має більш привабливі соціальні та зовнішні ознаки ніж професіональні. Тому потрібно робити відбір фахівців без впливу суб'єктивних преференцій. Тобто індивідуальний метод ранжування бі-

льш підтверджений прийняттю помилкових рішень.

У роботах [4-6] наведені нові методи відбору фахівців, такий як графологічний метод. Наводяться приклади застосування для відбору персоналу графологічні методи визначення здібностей людини (за його почерком). Мета даного методу - оцінити ступінь відповідності людини пропонованої посади, виділити групи ризику та групи переваги. Переваги методу – безконтактні, оперативність. Оцінювані показники: здатність контролювати свою поведінку; можливість адаптації у колективі; вміння керувати підлеглими; старанність; наполегливість; аналітичне мислення, психічні особливості; здатність до нестандартних рішень. Але метод дуже новий та потрібує подальшого удосконалення.

У роботах [7-9] наводиться метод співбесіди (інтерв'ю) з працівником, який виконує роботу, застосовується для отримання інформації, необхідної для аналізу робочого процесу. Він дає аналітику та працівнику можливість поговорити один з одним. Під час розмови працівник також може задавати аналітику різні питання. Таким чином, аналітик пояснює працівнику, як буде використовуватися отримана інформація. Співбесіда може проводитися з одним працівником, з групою або з начальником, який має відомості про робочому процесі. Використовується зазвичай стандартний набір питань, що дозволяє порівнювати відповіді. Уразливість методу в тому, що інформація може бути неточною.

Тому треба використовувати нові підходи, які дозволять виділити таки критерії у підборі персоналу-експертів, що напряму впливають на реалізацію задач в межах поставленого завдання.

Разом із тим, в цих роботах не в повній мірі відображені питання методологічного аналізу факторів визначення компетентності експертів для визначення неправдивої інформації. Тому треба використовувати нові та удосконалені методи, які дозволять виділити ті критерії у підборі персоналу, що напряму залежать як від кожного окремого співробітника як в межах його ролі так і впливу цих факторів на реалізацію задач в межах цілого проекту. Виходячи з вищевикладеного аналіз факторів визначення компетентності експертів для виявлення неправдивої інформації є актуальним науковим завданням.

## РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Експертне оцінювання базується на кількох методах. Серед найпопулярніших можна виділити:

1. Асоціативний – полягає у вивченні об'єкта, що має подібні характеристики;

2. Парні порівняння – порівнює альтернативи одного рішення з метою вивчення найкращих варіантів розвитку подій;

3. Фокальні об'єкти – метод ґрунтується на перенесенні властивостей та ознак випадково обраних аналогів на об'єкт дослідження;

4. Середня точка – у процесі оцінювання виділяють два шляхи вирішення проблеми: найбільш і найменш переважний. Між ними знаходиться «середня точка» – альтернатива, яка враховує особливості першого та другого варіанта.

Вибір конкретного методу залежить від призначення експертної оцінки.

Експертна група перед остаточним вердиктом перевіряє можливість використання альтернативних варіантів і розглядає об'єкт, що вивчається, з різних сторін. Щоб цей процес пройшов швидше та якісніше, необхідно підготувати інформаційні матеріали, що містять опис проблеми, статистику, довідки, анкети. Чим різноманітні дані, тим більше у експертів матеріалу для аналітики.

Процедуру експертного опитування, для виявлення неправдивої інформації можливо виділити в декілька кроків.

*Крок 1.* Формування робочої групи. Завдання робочої групи полягає в організації процедури набору експертів, розробка анкет, обмеження масштабу дослідження.

Відбір фахівців, експертів –складне, багатогранне завдання, успішний результат якого визначає ефективність використовуваних методів та рішень. Експерт повинен мати:

– компетентність у потрібній сфері;

– знання у суміжних областях, які безпосередньо не належать до досліджуваного питання;

– досвід практичної роботи, академічними та науковими досягненнями;

– об'єктивність для формування оцінки;

– здатність нестандартно мислити у випадках, коли це потрібно.

*Крок 2.* Формування експертної групи. Учасників слід ретельно вибирати відповідно до теми, що розглядається. Рекомендується запрошувати змішані групи експертів –представників промисловості академічних кіл, дослідницьких інститутів тощо. Також група повинна бути змішаною та включати в себе представників різної статі та різних вікових груп. Кількість учасників залежить від кількості тем, областей, очікуваної відповіді або рівня участі та інших питань. Якщо проводиться

невелике опитування з використанням комп'ютерів, то число учасників може бути невеликим (10-15). Якщо необхідно провести опитування на національному рівні, то потрібна велика кількість учасників, і часто необхідно отримати до ста відповідей по одній темі.

*Крок 3.* Формулювання питань. Перша анкета може бути повністю безструктурною і допускати будь-які відповіді. Експерти в письмовій формі висловлюють свої думки та ідеї по темі опитування

Після того як прогнози групи повернулися до організаторів, робоча група їх об'єднує, ідентифікує і складає перелік, який стає основою другої анкети [2-4].Таким чином формуються питання анкет для виявлення неправдивої інформації. Тобто на при кінці третього етапу ми отримуємо перелік питань які відселяють саме неправдиву інформації від правдивої.

*Крок 4.* Проведення експертизи. Експертам направляють зведений перелік інформаційних джерел і просять оцінити дані та обґрунтувати своє рішення. Після того як прогнози та оцінки, зроблені членами групи, повернулися до організаторів, аналітична група проводить статистичну обробку отриманих даних: уточнюють перелік подій та аналізують характеристики ряду, тобто розраховують медіани та квартилі. Інакше кажучи, проводять математичну обробку отриманих даних. Тобто на четвертому етапе обирається остаточна кількість експертів, точніше обирається група кваліфікованих експертів, які дійсно зможуть оцінити якість інформації з заданою довірою.

Це робиться методом перебору експертів, після того як переглянуті оцінки, організатор повинен змінити експерта, або експертів які отримали значно зменшили показники довіри оцінки. Надалі підсумувати оцінки групи, розрахувавши нові медіани і нові квартилі, підсумовувати аргументи, подані з обох сторін, і підготувати на цій основі нові питання. Експертиза повторюється до ти пір, поки всі оцінки не будуть знаходитись в визначеної області довіри [10, 11].

*Крок 5.* Аналіз результатів та доведення експертного висновку. На цьому етапі обробляються відомості, одержані в результаті експертизи. Після аналізу приймається рішення по оцінки інформації, яка підлягала експертизі.

Удосконалення методу колективної експертної оцінки полягає у можливості отримувати результати експертної оцінки з заданим результатом довіри до правдивості інформації.

## ПРАКТИЧНЕ ЗАСТОСУВАННЯ МЕТОДУ

В якості розгляду використання запропонованого методу для виявлення неправдивої інформації візьмемо на першому етапі 10 експертів.

Кожному експерту надаємо анкету для оцінки інформації та анкета самооцінки. Особливо хотилось би відмітити, що рівень самооцінки експертів, додатково перевіряються. Додатково визначаються рівень оцінки експертів робочій групою. Остаточно рівень оцінки експерта є середнє значення від самооцінки та оцінки робочий групи. Це дозволяє отримати значно об'єктивнішу оцінку експерта ніж за класичним методом.

Оцінка експертів буде оцінюватися за шкалою від 0 до 10, а критерій правдивості інформації експерти будуть оцінювати за сто відсотковою шкалою.

Зробимо припущення що до критерія якості, тобто задаємо критерій довіри десять відсотків. Тобто як що рівень відхилень загальної оцінки експертів буде знаходиться в межах десяті відсотків тоді будемо вважати. Що експерти підібрані вірно та їх експертний висновок відповідає дійсності з імовірністю 90 відсотків.

Нехай перший крок завершено, відібрана робоча група, яка виконала свої обов'язки. На другому кроці пройшло співбесіду з робочою групою 15 експертів.

На третьому кроці експерти виявляли ступень правдивості інформації.

Результати зведені у таблицю (табл. 1), результати відбору експертів. У таблиці 1, $X_i$ – середній рівень оцінки експерта. $Y_i$ - оцінка відповідним експертом ступеня правдивості інформації.

На основі даних табл. 1, виконаємо розрахунки. Для цього використаємо наступні вирази. Середньогрупова оцінка:

$$S_{mгр} = \frac{\sum_{i=1}^{n} X_i}{n}, \qquad (1)$$

де Xi – середній рівень оцінки експерта, який складається з самооцінки експерта та його оцінки робочій групою у одиницях з 0 до 10; $n$ – кількість експертів. Для даних таблиці 1 це значення $S_{mгр} = 7{,}82$.

Середнє значення оцінки правдивості інформації:

$$S_{m\_правд} = \frac{\sum_{i=1}^{n} Y_i}{n}, \qquad (2)$$

де Yi – оцінка відповідним експертом ступеня правдивості інформації, у відсотках; *n* – кількість експертів.

Таблиця 1

Результати відбору експертів та їх оцінка правдивості інформації

| № експерта | Рівень оцінки експертів | Оцінка правдивості інформації | |
|---|---|---|---|
| | $X_i$ | $Y_i$ | $Y_i*X_i$ |
| 1 | 7 | 85 | 595 |
| 2 | 8 | 70 | 560 |
| 3 | 9 | 73 | 657 |
| 4 | 8 | 77 | 616 |
| 5 | 8,5 | 87 | 739,5 |
| 6 | 7,9 | 72 | 568,8 |
| 7 | 6,3 | 70 | 441 |
| 8 | 8,1 | 79 | 639,9 |
| 9 | 7,7 | 85 | 654,5 |
| 10 | 6,2 | 84 | 520,8 |
| 11 | 6,5 | 70 | 455 |
| 12 | 8 | 71 | 568 |
| 13 | 9 | 84 | 756 |
| 14 | 9,5 | 79 | 750,5 |
| 15 | 7,6 | 78 | 592,8 |
| Сума | 117,3 | 1164 | 9114,8 |
| Ср.зн. | 7,82 | 77,6 | 607,65 |

Для даних табл. 1 це значення $S_{m\_правд} = 77{,}6$.

Середньозважена оцінка правдивості інформації:

$$S_{m\_оцінка} = \frac{\sum_{i=1}^{n} X_i * Y_i}{\sum_{i=1}^{n} X_i}. \qquad (3)$$

Для даних табл. 1 це значення $S_{m\_оцінка} = 77{,}7$.

Медіана розраховується як середньоарифметичне між серединними, впорядкованими за зростанням чи спаданням оцінками. Для таблиці 1 Me = 77,6.

Квартиль розраховується за виразом:

$$Квартиль = \frac{\max(Y_i) - \min(Y_i)}{4}. \qquad (4)$$

Для даних табл. 1, квартиль буде мати значення 4,25.

Тоді нижня межа області довіри: 70+4,25= 74,25 %, верхня 87-4,25=75,75%. Інтервал довіри знаходиться у проміжку від 74,25% до 75,75%, тобто дорівнює 1,5 %. Це відповідає застосованому критерію, за нашим критерієм інтервал повинен не перевищувати 10%. Нижче наведено графічне зображення результатів розрахунків (рис. 1).

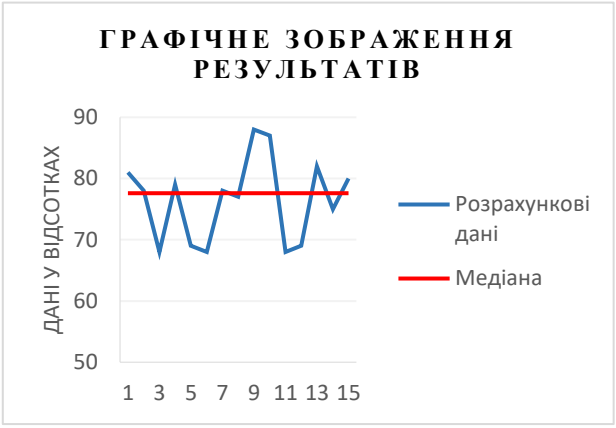


Рис.1. Графічне зображення результатів розрахунків для першої групи експертів

Аналіз графічних результатів рис.1, для даних наведених у таблиці 1, доводить вірний вибір експертів, робочий групою. Інтервал довіри при експертної оцінки набраною групи експертів задовольняє заданому критерію.

Тобто група експертів яка виконує оцінку правдивості інформації, робить її з інтервалом довіри 1,5%, що задовольняє запропонованому нами критерію оцінки. Ми задали критерій оцінки 10%.

Таким чином на відміну від існуючих методів запропоновано відбір експертів. Експертів які роблять оцінку правдивої інформації за встановленим критерієм довіри.

## ВИСНОВКИ

Удосконалено метод виявлення неправдивої інформації на основі методу експертної оцінки. Запропонований метод експертних оцінок має безсумнівні переваги в порівнянні з методами, заснованими на звичайній статистичній обробці результатів індивідуальних опитувань. На відміну від існуючого підходу, удосконалений метод дозволяє проводити ретельний відбір експертів. За допомогою двох критеріїв: самооцінки експерта та оцінки експерта робочою групою. Це дозволяє значно зменшити похибку оцінки експерта.

Отримання об'єктивної правдивої інформації досягається можливістю встановлювати інтервал довіри до оцінки інформації. Проте удосконалений метод має і ряд недоліків. Серед них, вирі-

шення проблеми оптимізації завдання, якщо інтервал довіри буде загально великим, тоді часу на завершення оцінки треба менше, але при цьому точність буде значно менше і навпаки коли інтервал довіри до оцінки буде малим, треба багато часу, що теж не є сприятливим. Тобто напрямком подальших досліджень є завдання оптимізації критеріїв оцінки.

## ЛІТЕРАТУРА


[1]. Лаптєва Т. О., Лукова-Чуйко Н.В. Удосконалення методу виявлення неправдивої інформації на основі методу експертної оцінки «Дельфі». Наукоємні технології. Том 55 № 3 (2022) С. 193-199. DOI: 10.18372 / 2310-5461. 55.16901.

[2]. Гнатієнко Г.М., Снитюк В.Є. Експертні технології прийняття рішень, Київ.: McLaut, 2008. 444 с.

[3]. Schefer-Wenzl, S., Strembeck, M. Modeling support for role-based delegation in process-aware information systems. Business and Information Systems Engineering. 6 (4). 2014. pp. 215-237. DOI: 10.1007 /s12599-014-0343-3.

[4]. Тетяна Лаптєва. Алгоритм визначення міри існування недостовірної інформації в умовах інформаційного протиборства. Кібербезпека: освіта, наука, техніка. No 2 (14), 2021, С. 15-25. DOI 10. 28925 / 2663-4023. 2021. 14. 1525, ISSN 2663-4023.

[5]. V. Savchenko, O. Laptiev, O. Kolos, R. Lisnevskyi, V. Ivannikova, I. Ablazov. Hidden Transmitter Localization Accuracy Model Based on Multi-Position Range Measurement. 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020) Conference Proceedings Kyiv, Ukraine, November 25-27. 2020. pp. 246-251.

[6]. Valentyn Sobchuk, Volodymyr Pichkur, Oleg Barabash, Oleksandr Laptiev, Kovalchuk Igor, Amina Zidan. Algorithm of control of functionally stable manufacturing processes of enterprises. 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020) Conference Proceedings Kyiv, Ukraine, November 25-27. pp. 206-211.

[7]. O. Svynchuk, O. Barabash, J. Nikodem, R. Kochan, O. Laptiev. Image compression using fractal functions. Fractal and Fractional, 5(2), 31. 2021. pp.1-14 DOI:10.3390/fractalfract5020031. 14 Apr 2021.

[8]. Sherstiuk, O., Kolesnikov, O., Lukianov, D. Team Behaviour Model as a Tool for Determining the Project Development Trajectory. 2019 IEEE International Conference on Advanced Trends in Information Theory, ATIT 2019, Proceedings, 2019, pp. 496-500.

[9]. Лаптєва Т.О. Методика виявлення неправдивої інформації для безпеки Держави. Всеукраїнській науково-практичній конференції студентів, аспірантів та молодих вчених «Об'єднані наукою: перспективи міждисциплінарних досліджень» 23-24 листопада 2023 р. Київ. Україна. С.131-132.

[10]. Наталія Лукова-Чуйко, Тетяна Лаптєва. Виділення та відбір ознак для визначення неправдивої інформації. V Міжнародна науково-практична конференція. "Проблеми кібербезпеки інформаційно-телекомунікаційних систем" (PCSITS)"27-28 жовтня 2022 р. Київ, Україна. Збірник матеріалів доповідей та тез. С 13-15.

[11]. Наталія Лукова-Чуйко, Тетяна Лаптєва. Удосконалення методу виявлення неправдивої інформації за допомогою байесовского класифікатора. Безпека інформації. НАУ. Том 28 № 3 (2022): Безпека інформації, 2022, С. 119-126.

[12]. Лаптєв О.А., Степаненко В.І., Тихонов Ю.О. Формальні математичні моделі для забезпечення безпеки інформації. Сучасний захист інформації: науково-технічний журнал. К.: ДУТ, 2019. № 1. С. 59-64.

[13]. Лаптєва Т.О., Лукова-Чуйко Н.В., Собчук А.В. Дослідження основних загроз і оцінка безпеки інформаційних систем. Математика. Інформаційні технології. Освіта. 2022 рік: збірка тез допов. учасник. XI Міжнар. наук.-практ. конф., 3-5 червня 2022 р. Луцьк-Світязь: СНУ імені Лесі Українки, 2022. С. 101-103.

[14]. Лаптев О.А., Собчук В.В., Саланди И.П., Сачук Ю.В. Математична модель структури інформаційної сеті на основі нестационарної ієрархічної та стаціонарної гиперсети. Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. К.: ВІКНУ, Вип. 64, 2019. С. 124-132.


## METHOD OF DETECTING FALSE INFORMATION BASED ON EXPERT ASSESSMENT


The article improves the method of detecting false information based on the method of expert evaluation. Expert methods are used to determine the nomenclature of quality indicators, their weighting coefficients, to measure quality indicators and evaluate them by the organoleptic method. The assessment of quality indicators by measuring, registration, and calculation methods is used to determine complex quality indicators at different levels of the hierarchy. Expert methods are based on making heuristic decisions based on the knowledge and experience accumulated by experts in a specific field in the past. The collective method of expert evaluations was chosen as the basic method for improvement. Because it has undoubted advantages compared to methods based on the usual statistical processing of the results of individual surveys. In contrast to the existing approach, the improved method allows for the selection of experts in a group, and not for correcting the answers of experts in order to obtain the required result. The peculiarity of the proposed method is that the selection of experts is done by averaging the scores. Averaging scores for each expert. Self-assessments of the expert and assessments of the same expert by the working group. This makes it possible to significantly reduce the error of the expert's real assessment. The abil-

ity to set a confidence interval for the assessment of false information will allow to obtain results that satisfy the task of detecting false information with appropriate accuracy. But this leads to solving the task of optimizing the evaluation criteria and the time to solve the set task. The scientific novelty consists in substantiating and evaluating the comparative importance of factors that limit the appointment of each individual expert to identify false information using the group expert evaluation method.
The direction of further research is the task of optimizing evaluation criteria.
**Keywords**: expert, false information, forecasting, algorithm, information technologies.

**Лукова-Чуйко Наталія Вікторівна**, доктор технічних наук, професор, завідувачка кафедри кібербезпеки та захисту інформації Факультету інформаційних технологій, Київський національний університет імені Тараса Шевченка, Київ, Україна.

**Nataliya Lukova-Chuiko**, Doctor of technical sciences, professor, Head of the Department of cyber security and information protection, Faculty of Information Technologies, Taras Shevchenko National University of Kyiv, Ukraine
E-mail: lukova@knu.ua.
Orcid ID: 0000-0003-3224-4061.

**Лаптєва Тетяна Олександрівна**, аспірантка кафедри кібербезпеки та захисту інформації, Факультет інформаційних технологій, Київський національний університет імені Тараса Шевченка, Київ, Україна

**Tetiana Laptieva**, PhD-student, Department of Cyber Security and Information Protection Faculty of information technology, Taras Shevchenko National University of Kyiv, Ukraine.
E-mail: tetiana1986@ukr.net.
Orcid ID: 0000-0002-5223-9078.

**DOI: 10.18372/2410-7840.26.18825**
**УДК 004.056.55**

# АРИФМЕТИКА АСИМЕТРИЧНИХ КРИПТОСИСТЕМ В ПОЛІ КОМПЛЕКСНИХ ЧИСЕЛ

***Андрій Алілуйко, Михайло Касянчук***

*На сучасному етапі розвитку інформаційних технологій виникає необхідність у вдосконаленні існуючих і розробці нових методів і засобів підвищення продуктивності асиметричних криптоалгоритмів. У статті наведено теоретичні основи модулярних обчислень та асиметричної криптографії в комплексній числовій області. Зокрема, розглянуто метод визначення комплексного та дійсного залишку за комплексним модулем. Розглянуто алгоритм Евкліда та його наслідок для пошуку оберненого елемента в комплексній числовій області. Здійснено порівняння складності алгоритму Евкліда для знаходження оберненого елементи при знаходженні найменших додатних та абсолютно найменших залишків. Проведено пошук аналогу функції Ейлера в комплексній числовій області та використано цю функцію для знаходження оберненого елемента до комплексного числа. Продемонстровано відновлення комплексного числа з допомогою китайської теореми про остачі. Розглянуті модулярні обчислення в області комплексних чисел можна використати при побудові нових підходів до асиметричного шифрування.*
***Ключові слова**: асиметрична криптосистема, комплексне число, алгоритм Евкліда, функція Ейлера, система залишкових класів.*

## ВСТУП

На сучасному етапі розвитку інформаційних технологій виникає ряд проблем та науково-технічних задач, пов'язаних з підвищенням стійкості комп'ютерних систем до різного виду атак [2, 4], швидкодії алгоритмів шифрування/ розшифрування/аутентифікації [1, 5], оптимізацією обчислень над багаторозрядними числами [8], зменшенням часових складностей виконання базових операцій в асиметричних криптоалгоритмах [9] та створенням засобів захисту інформаційних потоків. Такі задачі опрацювання інформаційних потоків в сучасних комп'ютерних системах розв'язуються на основі використання відомих алгоритмів шифрування, факторизації, дискретного логарифмування, модулярних та інших операцій.

Слід зазначити, що в сучасній асиметричній криптографії, яка функціонує в позиційних системах числення, постає завдання вирішення трудомістких обчислювальних науково-практичних задач з необхідністю виконання значних обсягів обчислень в реальному часі [3]. Переважна більшість таких криптоалгоритмів ґрунтуються на цілочисельній модулярній арифметиці. Зокрема, в основі асиметричної криптосистеми RSA лежить пошук найбільшого спільного дільника (НСД) двох чисел (як правило, за допомогою алгоритму Евкліда), пошук оберненого елемента за модулем (переважно, за допомогою наслідку з