УДК 519.21:004.056.55
DOI https://doi.org/10.32782/cusu-pmtp-2026-1-6

ВИКОРИСТАННЯ ІНТЕГРАЛЬНИХ ОЦІНОК ІМОВІРНОСТЕЙ КОЛІЗІЙ У ХЕШ-ФУНКЦІЯХ ПІД ЧАС ПІДГОТОВКИ МАЙБУТНІХ ІТ-ФАХІВЦІВ

Клєопа Ірина Анатоліївна,
доктор філософії (PhD), доцент,
кафедри вищої математики
Вінницького національного технічного університету
ORCID ID: 0000-0001-8408-6515

Тютюнник Оксана Іванівна,
кандидат педагогічних наук, доцент,
кафедри вищої математики
Вінницького національного технічного університету
ORCID ID: 0000-0002-8544-4246

Ковальчук Майя Борисівна,
доктор педагогічних наук, професор,
кафедри вищої математики
Вінницького національного технічного університету
ORCID ID: 0000-0002-1895-1715

У статті обґрунтовано педагогічну доцільність використання методів інтегрального числення для оцінювання ймовірностей колізій у хеш-функціях у процесі підготовки майбутніх ІТ-фахівців. Актуальність дослідження зумовлена потребою в підвищенні якості математичної підготовки майбутніх фахівців з інформаційної безпеки та формуванні в них здатності застосовувати математичні методи для аналізу криптографічної стійкості алгоритмів захисту інформації.

У роботі показано, що традиційні комбінаторні підходи до оцінювання ймовірностей колізій у хеш-функціях часто є складними для сприйняття студентами та не забезпечують належного рівня усвідомлення прикладного змісту математичних моделей. Запропоновано методику навчання, що ґрунтується на використанні інтегральних оцінок, які дають можливість апроксимувати дискретні ймовірнісні процеси неперервними моделями та застосовувати графічну інтерпретацію результатів. Такий підхід сприяє кращому розумінню парадоксу днів народження та його зв'язку з проблемою колізій у хеш-функціях.

З метою оцінювання педагогічної ефективності запропонованого підходу проведено педагогічний експеримент із залученням контрольної та експериментальної груп студентів. В експериментальній групі вивчення теми здійснювалося з використанням інтегральних моделей і графічної інтерпретації імовірностей, тоді як у контрольній групі застосовувалися традиційні комбінаторні методи. Результати тестування продемонстрували підвищення рівня засвоєння матеріалу в експериментальній групі, що підтверджено статистичною перевіркою.

Отримані результати свідчать про доцільність використання інтегралів як ефективного інструменту для аналізу колізій у хеш-функціях та їх педагогічну цінність у навчанні математичних основ криптографії.

Ключові слова: *інтегральне числення, ймовірність колізій, хеш-функції, методика навчання, професійна підготовка студентів, ІТ-освіта, педагогічний експеримент, вища математика.*

Klieopa Iryna, Tiutyunnik Oksana, Kovalchuk Maya. Using integral estimates of collision probability in hash functions during the training of future IT specialists

The article substantiates the pedagogical feasibility of using integral calculus methods to estimate collision probabilities in hash functions in the process of training future IT specialists. The relevance of the study is due to the need to improve the quality of mathematical training of future information security specialists and to form in them the ability to apply mathematical methods to analyze the cryptographic stability of information protection algorithms.

The paper shows that traditional combinatorial approaches to estimating collision probabilities in hash functions are often difficult for students to perceive and do not provide an adequate level of awareness of the applied content of mathematical models. A teaching methodology based on the use of integral estimates is proposed, which allows approximating discrete probabilistic processes by continuous models and applying graphical interpretation of the results. This approach contributes to a better understanding of the birthday paradox and its connection with the problem of collisions in hash functions. In order to assess the pedagogical effectiveness of the proposed approach, a pedagogical experiment involving control and experimental groups of students was conducted. In the experimental group, the study of the topic was carried out using integral models and graphical interpretation of probabilities, while traditional combinatorial methods were applied in the control group. The test results demonstrated an increase in the level of material mastery in the experimental group, which was confirmed by statistical verification.

The obtained results indicate the feasibility of using integrals as an effective tool for collision analysis in hash functions and confirm their pedagogical value in teaching the mathematical foundations of cryptography.

Key words: *integral calculus, collision probability, hash functions, teaching methodology, professional training of students, IT education, pedagogical experiment, higher mathematics.*

Вступ. Сучасна підготовка фахівців у галузі інформаційних технологій та кібербезпеки вимагає не лише засвоєння формальних математичних методів, а й формування здатності застосовувати їх для аналізу реальних прикладних задач. Особливе місце серед таких задач посідає проблема колізій у хеш-функціях, яка є ключовою в оцінюванні криптографічної стійкості алгоритмів захисту інформації та безпеки комп'ютерних систем. Традиційне вивчення ймовірностей колізій у курсах вищої математики та криптографії зазвичай ґрунтується на комбінаторних підходах і дискретних моделях, що часто ускладнює сприйняття матеріалу студентами та знижує рівень його практичного розуміння. У підсумку математичні формули розглядаються ізольовано від їхнього прикладного змісту, що не повною мірою сприяє формуванню професійних компетентностей майбутніх фахівців [3].

У зв'язку із цим актуальним є пошук педагогічно доцільних методик навчання, які забезпечують інтеграцію математичного апарату з прикладними задачами криптографії. Одним із таких підходів є використання інтегрального числення для оцінювання ймовірностей колізій у хеш-функціях, що дає можливість наочно моделювати імовірнісні процеси, застосовувати графічну інтерпретацію результатів та формувати у студентів аналітичне й імовірнісне мислення.

Метою статті є обґрунтування й експериментальна перевірка ефективності методики використання інтегралів для оцінювання ймовірностей колізій у хеш-функціях у процесі підготовки майбутніх фахівців ІТ-галузі. Для досягнення поставленої мети розглянуто математичні моделі оцінювання колізій, розроблено навчальні приклади з використанням інтегральних оцінок і графічних моделей, а також проведено педагогічний експеримент з метою порівняння результатів навчання у контрольній та експериментальній групах. Таке дослідження поєднує математичний та педагогічний підходи і спрямоване на підвищення якості професійної підготовки студентів шляхом впровадження наочно орієнтованих і методично обґрунтованих засобів навчання

Використання інтегралів дає змогу перейти від дискретних моделей до неперервних, що спрощує аналітичні оцінки та сприяє кращому розумінню імовірнісної природи колізій. Це особливо важливо для підготовки студентів з інформаційних технологій та кібербезпеки, для яких поєднання вищої математики з криптографічними застосуваннями є необхідним [8].

Аналіз досліджень і публікацій. Проблематика оцінювання ймовірностей колізій у хеш-функціях широко представлена в працях, присвячених теоретичним основам криптографії та

інформаційної безпеки. Класичні підходи до аналізу колізій базуються на комбінаторних імовірнісних моделях, зокрема на аналогії з парадоксом днів народження, який детально розглядається у фундаментальних роботах з криптографії та теорії імовірностей. У таких дослідженнях колізії аналізуються як дискретні випадкові події, що дає можливість отримати точні формули, однак ускладнює їх практичне застосування в разі великих обсягів даних.

У працях вітчизняних науковців значну увагу приділено дослідженню криптографічних засобів захисту інформації та методів хешування даних із метою забезпечення автентичності в комп'ютерних системах і мережах. Зокрема, відповідні питання висвітлювалися в роботах С. П. Євсєєва, А. А. Кузнецова, Т. Ю. Самбурської та інших дослідників. Суттєвий внесок у розвиток теорії та практики криптографічного захисту інформації, що передається через комп'ютерні системи і мережі, зробили зарубіжні науковці. Серед таких авторів слід відзначити Альфреда В. Ахо, Джона Хопкрофта, Джеффрі Д. Ульмана та інших [5].

Водночас аналіз наукових публікацій свідчить, що питання застосування інтегральних методів саме для оцінювання ймовірностей колізій у хеш-функціях залишається недостатньо висвітленим, особливо в аспекті їх дидактичного потенціалу. Наявні роботи переважно не розглядають можливості використання інтегральних моделей і графічної візуалізації як засобів підвищення якості навчання криптографії та вищої математики.

Матеріали та методи. Дослідження виконувалося із застосуванням методів теорії імовірностей, математичного аналізу та криптографії. Теоретичною основою слугували моделі оцінювання ймовірностей колізій у хеш-функціях, що базуються на аналогії з парадоксом днів народження. Для апроксимації дискретних імовірнісних процесів використовувалися методи інтегрального числення, які дали змогу отримати експоненціальні оцінки ймовірності виникнення колізій [1].

Для підвищення ефективності засвоєння студентами теми оцінювання ймовірностей колізій у хеш-функціях було запропоновано інтегральний підхід, що поєднує математичні моделі з наочною педагогічною реалізацією. Методика ґрунтується на використанні інтегрального числення для апроксимації дискретних імовірнісних процесів неперервними моделями та на візуалізації результатів через графічні засоби, що дає змогу студентам глибше усвідомлювати математичну сутність процесу колізій.

На першому етапі студенти опановують традиційні комбінаторні формули для оцінки ймовірності колізій, що забезпечує формування базового теоретичного апарату. Другий етап передбачає введення інтегральних апроксимацій дискретних моделей, які дають можливість спростити обчислення, підвищити наочність аналізу та показати зв'язок між дискретними й неперервними математичними підходами. На третьому етапі використовуються графічні інтерпретації та прикладні задачі з криптографічним змістом, що сприяє формуванню професійних компетентностей студентів та підвищенню їх мотивації до вивчення вищої математики.

Педагогічна ефективність запропонованого підходу оцінювалася шляхом проведення педагогічного експерименту за участю контрольної та експериментальної груп студентів. У контрольній групі застосовувалися класичні комбінаторні формули, тоді як в експериментальній – інтегральні оцінки та графічна інтерпретація результатів. Рівень засвоєння матеріалу визначався за результатами підсумкового тестування з використанням методів математичної статистики для аналізу отриманих даних [4].

Результати. Метою педагогічного експерименту було визначення ефективності запропонованої методики навчання оцінювання ймовірностей колізій у хеш-функціях із використанням інтегральних методів. Експеримент складався з констатувального, формувального та контрольного етапів. На контрольному етапі проводилося підсумкове оцінювання рівня засвоєння матеріалу та сформованості відповідних умінь. Нами було проведено педагогічний експеримент, у якому брали участь дві групи студентів зі спеціальності «Безпека інформаційних і комунікаційних систем»: контрольна група й експериментальна група.

Навчальний процес у контрольній групі здійснювалося з використанням класичних комбінаторних формул без залучення інтегральних оцінок і графічних інтерпретацій. Нижче покажемо основні формули, які використовували для дослідження.

Імовірність відсутності колізій за хешування k різних повідомлень визначається дискретною формулою:

$$P_{посол} \approx \prod_{1=0}^{k-1}\left(1-\frac{i}{N}\right).$$

Проте в разі великих значень k та N безпосереднє використання цієї формули є обчислювально складним. У зв'язку із цим застосовується інтегральне наближення, яке ґрунтується на переході від дискретного добутку до експоненціальної функції.

Зокрема, використовуючи логарифмування й інтегрування, отримуємо асимптотичну оцінку:

$$P \approx \exp\left(-\frac{k^2}{2N}\right).$$

Цей результат отримується шляхом переходу від дискретної добуткової формули до інтегрального наближення, що базується на обчисленні визначеного інтеграла логарифмічної функції.

Звідси ймовірність виникнення хоча б однієї колізії має вигляд:

$$P_{кол} = 1-\exp\left(-\frac{k^2}{2N}\right).$$

Отримана формула дає можливість ефективно оцінювати ризик колізій без виконання складних комбінаторних обчислень. Вона демонструє нелінійний характер зростання ймовірності колізій і вказує на квадратичну залежність між кількістю повідомлень та розміром простору хеш-значень [3].

Для наочного аналізу було побудовано графіки залежності $P_{col}(k)$ від кількості повідомлень за різних значень параметра N. Аналіз результатів показує, що для малих розмірів хешу (наприклад, $N = 2^{12}$) імовірність колізій швидко наближається до одиниці навіть за відносно невеликої кількості повідомлень. Натомість збільшення розміру хеш-простору до $N = 2^{16}$ істотно знижує ризик колізій у практичному діапазоні значень. Особливу увагу приділено визначенню критичних значень кількості повідомлень, за яких імовірність колізії перевищує заданий поріг α.

Розв'язуючи рівняння: $1-\exp\left(-\frac{k^2}{2N}\right)=\alpha$,
можна отримати оцінки максимально допустимої кількості повідомлень для забезпечення необхідного рівня криптографічної безпеки [6].

В експериментальній групі використовувався інтегральний підхід, який передбачав побудову аналітичних залежностей і їх подальшу візуалізацію у вигляді графіків на конкретних прикладах. Детальніше розберемо на прикладах.

Приклад 1. Опис графіка інтегральної оцінки (одна крива).

На рис. 1 зображено залежність імовірності виникнення колізії від кількості оброблених повідомлень k за фіксованого розміру простору хеш-значень $N = 2^{16}$. Графік побудовано на основі інтегральної апроксимації

$$P_{кол} = 1-\exp\left(-\frac{k^2}{2N}\right),$$

яка є неперервним наближенням дискретної імовірнісної моделі.

На графіку можна побачити, що зі зростанням кількості повідомлень імовірність колізії зростає нелінійно: на початковому етапі зростання є повільним, однак після досягнення певного порогу відбувається різке збільшення ймовірності колізій. Така поведінка узгоджується

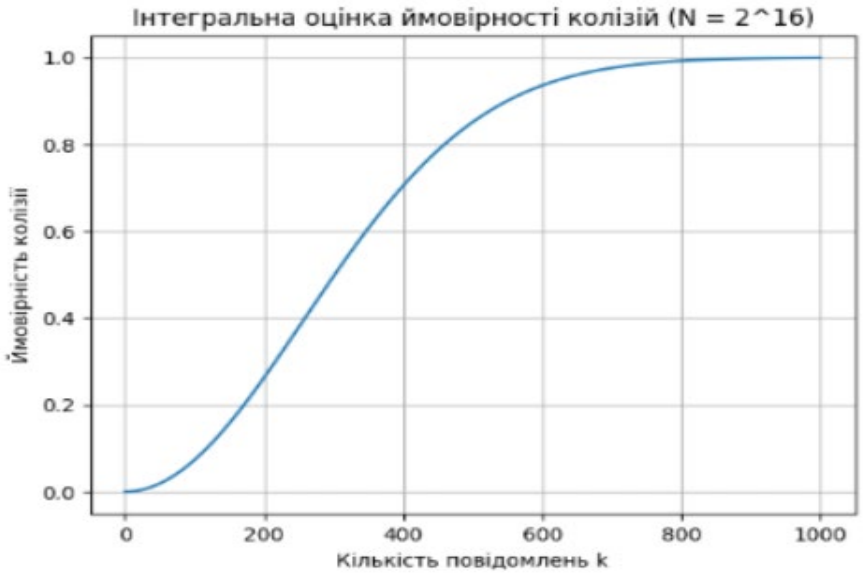

Рис. 1. Інтегральна оцінка ймовірності колізій

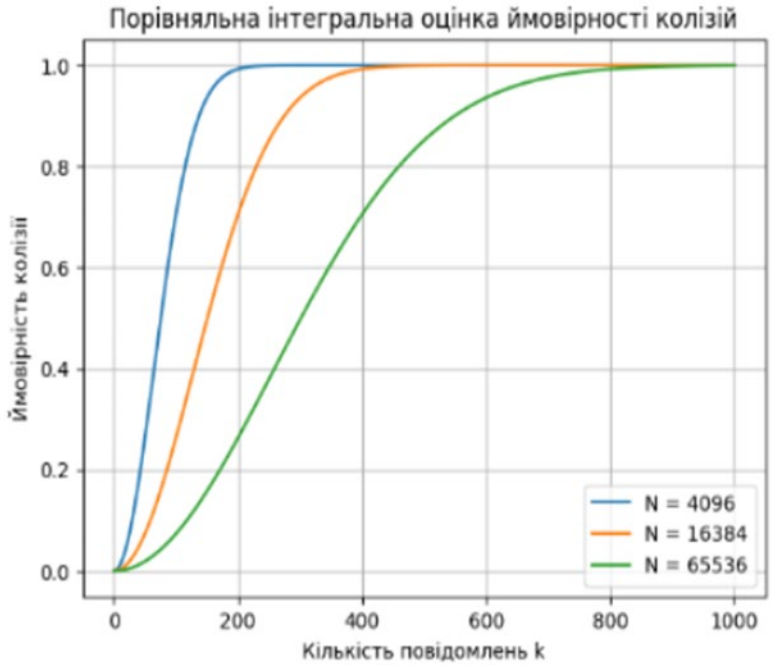

Рис. 2. Порівняльна інтегральна оцінка ймовірності колізій для різних значень *N*

з парадоксом днів народження та підтверджує доцільність використання інтегральних оцінок для аналізу властивостей хеш-функцій.

Візуалізація інтегральної моделі дає змогу наочно продемонструвати студентам імовірнісну природу колізій та сприяє кращому розумінню взаємозв'язку між параметрами хеш-функцій і рівнем криптографічної стійкості.

Приклад 2. Порівняльний графік для різних розмірів хешу.

На графіку зображено кілька кривих для різних розмірів простору хеш-значень (наприклад, $N = 2^{12}, 2^{14}, 2^{16}$). Аналіз графіка показує, що зі збільшенням N крива зсувається вправо, тобто для досягнення однакової імовірності колізій потрібна значно більша кількість повідомлень.

Це підтверджує важливість вибору достатньої довжини хешу для забезпечення криптографічної стійкості.

Порівняльний аналіз графіків для різних розмірів простору хеш-значень продемонстрував суттєвий вплив параметра N на криптографічну стійкість хеш-функцій. Зі збільшенням N криві ймовірності колізій зсуваються вправо, що означає зменшення ризику колізій за фіксованої кількості повідомлень. Це узгоджується з теоретичними положеннями криптографії та підтверджує доцільність використання довших хеш-значень у практичних системах захисту інформації.

Крім того, застосування інтегрального підходу та графічної візуалізації має важливе методичне значення. Побудовані графіки дають можливість студентам і дослідникам інтуїтивно зрозуміти природу колізій у хеш-функціях, поєднуючи строгі математичні моделі з наочною інтерпретацією результатів.

У таблиці 1 показано результати навчальних досягнень контрольної та експериментальної груп.

Таблиця 1

Результати навчальних досягнень

Група	Кількість студентів	Середній бал
Контрольна	26	72,1
Експериментальна	27	83,4

Для перевірки статистичної значущості відмінностей між результатами контрольної та експериментальної груп було використано критерій Стьюдента для незалежних вибірок за рівня значущості $\alpha = 0{,}05$. Отримані результати підтвердили статистично значущу перевагу експериментальної методики. Отримані результати підтверджують ефективність використання інтегральних моделей для оцінювання ймовірностей колізій у хеш-функціях як з математичного, так і з педагогічного погляду [9].

Аналіз результатів педагогічного експерименту дав змогу оцінити ефективність запропонованої методики використання інтегралів для оцінювання ймовірностей колізій у хеш-функціях у процесі підготовки майбутніх фахівців ІТ-галузі. Основна увага приділялася не лише кількісним показникам успішності, а і якісним змінам у характері засвоєння навчального матеріалу студентами.

У контрольній групі вивчення теми здійснювалося з використанням класичних комбінаторних формул і дискретних моделей, що потребували значної кількості формальних обчислень і часто сприймалися студентами як абстрактні. В експериментальній групі навчання базувалося на інтегральних оцінках і графічній інтерпретації імовірностей, що дало можливість наочно продемонструвати залежність імовірності колізій від кількості повідомлень та розміру простору хеш-значень [7].

Результати підсумкового тестування показали вищий рівень засвоєння матеріалу в експериментальній групі. Студенти цієї групи краще виконували завдання, пов’язані з аналізом криптографічної стійкості хеш-функцій, демонстрували здатність інтерпретувати отримані числові оцінки та переносити математичні моделі у прикладний професійний контекст. Це свідчить про формування у них аналітичного та ймовірнісного мислення, необхідного для подальшої професійної діяльності у сфері інформаційної безпеки та програмної інженерії.

Важливим результатом є також підвищення навчальної мотивації студентів експериментальної групи. Використання графіків і комп’ютерного моделювання сприяло кращому розумінню сутності парадокса днів народження та його зв’язку з проблемою колізій у хеш-функціях, що зменшувало формалізм у вивченні теми та підвищувало інтерес до математичних методів аналізу криптографічних алгоритмів.

Статистична обробка результатів тестування підтвердила наявність значущої різниці між показниками контрольної та експериментальної груп, що дає змогу зробити висновок про ефективність запропонованої методики. Отримані дані засвідчують доцільність використання інтегральних моделей не лише як математичного інструменту, а і як ефективного педагогічного засобу для формування професійних компетентностей майбутніх фахівців [2].

Таким чином, результати дослідження підтверджують, що інтеграція методів інтегрального числення з прикладними задачами криптографії забезпечує більш глибоке засвоєння навчального матеріалу та сприяє підвищенню якості підготовки студентів у галузі інформаційних технологій.

Висновки. Запропонований підхід до навчання оцінювання ймовірностей колізій у хеш-функціях із використанням інтегрального числення є ефективним засобом формування професійних компетентностей студентів ІТ-спеціальностей. Результати педагогічного експерименту підтверджують доцільність упровадження інтегральних методів і графічних інтерпретацій у курсах вищої математики з прикладною спрямованістю.

Результати проведеного дослідження показали, що методи інтегрального числення є ефективним інструментом для оцінювання ймовірностей колізій у хеш-функціях. Перехід від дискретних імовірнісних моделей до неперервних інтегральних наближень дає можливість суттєво спростити аналітичний апарат зі збереженням достатньої точності оцінок, особливо у випадках великих розмірів простору хеш-значень.

Отримані інтегральні формули демонструють тісний зв'язок між класичним парадоксом днів народження та криптографічними властивостями хеш-функцій. Використання експоненціальної апроксимації імовірності колізій дає змогу не лише кількісно оцінювати ризик збігів, але й здійснювати їх наочну графічну інтерпретацію.

Аналіз побудованих графіків показав, що інтегральна апроксимація адекватно відображає характер зростання ймовірності колізій залежно від кількості оброблених повідомлень. Зокрема, спостерігається нелінійний характер зростання, який не завжди є очевидним у разі використання лише дискретних комбінаторних формул.

Педагогічний експеримент підтвердив, що застосування інтегральних моделей і візуалізацій у навчальному процесі сприяє глибшому розумінню студентами імовірнісної природи хеш-функцій. Статистична перевірка результатів засвідчила підвищення рівня навчальних досягнень в експериментальній групі, що свідчить про доцільність інтеграції методів математичного аналізу у викладання дисциплін криптографічного спрямування.

Запропонована методика не лише підвищує рівень засвоєння навчального матеріалу, але й сприяє формуванню професійно орієнтованого мислення студентів, що є важливою складовою підготовки конкурентоспроможних фахівців у галузі інформаційних технологій та кібербезпеки.

Література:

1. Бедратюк Л. П., Бедратюк Г. І. Використання системи комп'ютерної алгебри Maple в елементарній теорії чисел. *Східноєвропейський журнал передових технологій.* 2013. № 6 (4). С. 10–13. https://doi.org/10.15587/1729-4061.2013.18892.

2. Ковальчук М. Б., Клєопа І. А., Коломієць А. А., Тютюнник О. І., Добранюк Ю. В. Алгоритмічні прийоми розумової діяльності як технологія розвитку когнітивних здібностей студентів у вивченні математики. *Педагогічна академія: наукові записки*. 2025. № 15. https://doi.org/10.5281/zenodo.14987960.

3. Клєопа І. А. Лавренюк Д. С. Парадокси теорії ймовірностей: інтуіція проти математичних розрахунків. *Матеріали LIV науково-технічної конференції підрозділів ВНТУ.* Вінниця. 2025.

4. Клєопа І. А., Тютюнник О. І., Крупський Я. В., Добранюк Ю. В. Особливості використання сучасних інформаційнокомунікаційних технологій у вищій математичній освіті. *Інформаційні технології та інноваційні методики навчання в закладах вищої освіти.* 2024. Вип. 72. С. 113–124. https://doi.org/10.31652/2412-1142-2024-72-113-124.

5. Клювак О. В. Криптографічна стійкість комбінаційного хешування автентифікаційних даних в інтернет-платіжних системах. *Соціально-економічні проблеми сучасного періоду України*. 2013. Вип. 1. С. 531–538.

6. Маліновська О. О. Вимоги до криптографічної системи захисту інформації / О. О. Маліновська, О. І. Зінченко ; наук. кер. Я. Ю. Усов. *Новітні технології у науковій діяльності і навчальному процесі* : *матеріали тез доп. Всеукр. наук.-практ. конф. студентів, аспірантів та молодих учених.* Чернігів : ЧНТУ, 2019. С. 113–116.

7. Михалевич В. М., Майданевич Л. О. Використання системи Maple в математичних задачах криптографії. Елементарна теорія чисел. *Інформаційні технології та комп`ютерна інженерія*. 2024. Т. 59, № 1. С. 105–118.

8. Сидоренко В. М., Кирилаха Н. Г. Дидактико-методичні аспекти викладання теорії ймовірностей та математичної статистики студентам ІТ напряму. *Інженерні та освітні технології*. 2023. Т. 11. № 3. С. 17–23. https://doi.org/10.32782/2307-9770.2023.11.03.02.

9. Сидоренко В. М., Садовнича С. А., Долударєва Є. В. Оптимізація структури тестових завдань навчальних онлайн-курсів на основі ймовірнісної моделі. *Інженерні та освітні технології*. 2022. Т. 10. № 2. С. 27–36.

10. Фаур Е. В., Щерба А. І., Рудницький В. М. Метод та критерій оцінювання якості послідовностей випадкових чисел. *Кібернетика та системний аналіз*. 2020. Т. 52. № 2.

References:

1. Bedratiuk, L.P., & Bedratiuk, H.I. (2013). Vykorystannia systemy kompiuternoi alhebry Maple v elementarnii teorii chysel [Use of the Maple computer algebra system in elementary number theory]. *Skhidnoievropeiskyi zhurnal peredovykh tekhnolohii*, *6* (4 (66)), 10–13. https://doi.org/10.15587/1729-4061.2013.18892 [in Ukrainian].

2. Kovalchuk, M.B., Klieopa, I.A.,Kolomiiets, A.A., Tiutiunnyk, O.I., & Dobraniuk, Yu.V. (2025). Alhorytmichni pryiomy rozumovoi diialnosti yak tekhnolohiia rozvytku kohnityvnykh zdibnostei studentiv u vyvchenni matematyky [Algorithmic techniques of mental activity as a technology for developing students' cognitive abilities in studying mathematics]. Pedahohichna Akademiia: naukovi zapysky, *(15).* https://doi.org/10.5281/zenodo.14987960 [in Ukrainian].

3. Klieopa, I.A., & Lavreniuk, D.S. (2025). Paradoksy teorii ymovirnostei: intuitsiia proty matematychnykh rozrakhunkiv [Paradoxes of probability theory: intuition versus mathematical calculations]. In Materialy LIV naukovo-tekhnichnoi konferentsii pidrozdiliv VNTU. Vinnytsia [in Ukrainian].

4. Klieopa, I.A., Tiutiunnyk, O.I., Krupskyi, Ya.V., & Dobraniuk, Yu.V. (2024). Osoblyvosti vykorystannia suchasnykh informatsiino-komunikatsiinykh tekhnolohii u vyshchii matematychnii osviti [Features of using modern information and communication technologies in higher mathematical education]. Informatsiini tekhnolohii ta innovatsiini metodyky navchannia v zakladakh vyshchoi osvity, *(72),* 113–124. https://doi.org/10.31652/2412-1142-2024-72-113-124 [in Ukrainian].

5. Kliuvak, O.V. (2013). Kryptohrafichna stiikist kombinatsiinoho kheshuvannia avtentyfikatsiinykh danykh v Internet-platizhnykh systemakh [Cryptographic strength of combinational hashing of authentication data in Internet payment systems]. Sotsialno-ekonomichni problemy suchasnoho periodu Ukrainy, *(1),* 531–538 [in Ukrainian].

6. Malinovska, O.O., & Zinchenko, O.I. (2019). Vymohy do kryptohrafichnoi systemy zakhystu informatsii [Requirements for a cryptographic information protection system]. In Novitni tekhnolohii u naukovii diialnosti i navchalnomu protsesi: materialy tez dopovidei Vseukrainskoi naukovo-praktychnoi konferentsii studentiv, aspirantiv ta molodykh uchenykh (pp. 113–116). Chernihiv, Ukraine: ChNTU [in Ukrainian].

7. Mykhalevych, V.M., & Maidanevych, L.O. (2024). Vykorystannia systemy Maple v matematychnykh zadachakh kryptohrafii. Povidomlennia 1. Elementarna teoriia chysel [Use of the Maple system in mathematical problems of cryptography. Report 1. Elementary number theory]. Informatsiini tekhnolohii ta kompiuterna inzheneriia, *59* (1), 105–118 [in Ukrainian].

8. Sydorenko, V.M., & Kyrylaha, N.H. (2023). Dydaktyko-metodychni aspekty vykladannia teorii ymovirnostei ta matematychnoi statystyky studentam IT napriamu [Didactic and methodological aspects of teaching probability theory and mathematical statistics to IT students]. Inzhenerni ta osvitni tekhnolohii, *11* (3), 17–23. https://doi.org/10.32782/2307-9770.2023.11.03.02 [in Ukrainian].

9. Sydorenko, V.M., Sadovnycha, S.A., & Doludarieva, Ye.V. (2022). Optymizatsiia struktury testovykh zavdan navchalnykh onlain-kursiv na osnovi ymovirnisnoi modeli [Optimization of the structure of test tasks in online courses based on a probabilistic model]. Inzhenerni ta osvitni tekhnolohii, *10* (2), 27–36 [in Ukrainian].

10. Faur, E.V., Shcherba, A.I., & Rudnytskyi, V.M. (2020). Metod ta kryterii otsiniuvannia yakosti poslidovnostei vypadkovykh chysel [Method and criterion for evaluating the quality of random number sequences]. Kibernetyka ta systemnyi analiz, *52* (2) [in Ukrainian].

Дата першого надходження статті до видання: 28.01.2026

Дата прийняття статті до друку після рецензування: 20.02.2026

Дата публікації (оприлюднення) статті: 21.04.2026