Бавицький А. О.,
здобувач вищої освіти спеціальності F3 Комп'ютерні науки
Науковий керівник: Богатєнкова О.Є., асистент кафедри економічної кібернетики, комп'ютерних наук та інформаційних технологій
Миколаївський національний аграрний університет
м. Миколаїв

ЗАСТОСУВАННЯ АЛГОРИТМІЧНОЇ ТЕОРІЇ ЧИСЕЛ У СУЧАСНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ ТА СЕРВІСАХ

У цифрову епоху, коли цілісність та конфіденційність даних визначають безпекові, економічні та соціальні аспекти суспільства, фундаментальні математичні дисципліни стають критичними для технологічного прогресу. Теорія чисел, зокрема її алгоритмічний напрям, становить основу для сучасних криптографічних протоколів, методів захисту інформації та оптимізації обчислювальних процесів. Її застосування забезпечує функціонування фінансових систем, конфіденційність комунікацій та стійкість інформаційної інфраструктури держави до кіберзагроз, що є пріоритетом національної безпеки.

Алгоритмічна теорія чисел є фундаментальною основою для розвитку надійних криптосистем, ефективних обчислювальних методів та стійких інформаційних технологій [5]. Її принципи безпосередньо впливають на створення та захист цифрового середовища [3].

Важливість досліджень у галузі теорії чисел обґрунтовується її фундаментальною роллю в сучасних технологіях. Насамперед, безпека цифрового середовища, зокрема захист комунікацій та фінансових транзакцій, безпосередньо залежить від складних обчислювальних задач, що базуються на цій науці, таких як факторизація великих чисел. По-друге, алгоритмічні підходи, які випливають із теорії чисел, є основою для оптимізації обчислювальних процесів, що критично важливо для ефективності програмування та комп'ютерних наук загалом. По-третє, стрімкий розвиток інноваційних напрямів, зокрема квантових обчислень і блокчейн-технологій, неможливий без поглибленого вивчення та розширення знань у цій математичній дисципліні, оскільки вони створюють нові виклики й вимоги до криптографічних основ.

Дане обґрунтування побудовано на аналізі сучасних наукових праць, навчальних ресурсів та технологічної документації. Методологія дослідження полягає у системному аналізі взаємозв'язків між абстрактними поняттями теорії чисел, такими як модульна арифметика або властивості простих чисел, та їх практичним втіленням у конкретних алгоритмах і протоколах безпеки.

Теорія чисел слугує математичним фундаментом сучасної криптографії, що підтверджується ключовими алгоритмами безпеки. Наприклад, алгоритм RSA [2, 5] покладається на обчислювальну складність факторизації великих цілих чисел на прості множники. Протокол Діффі-Геллмана забезпечує безпечний обмін криптографічними ключами [2, 5], використовуючи важкість задачі дискретного логарифмування. А криптографія на еліптичних кривих

(ECC) досягає високої криптостійкості при значно меншій довжині ключа, базуючись на аналогічній задачі, але в групі точок еліптичної кривої [2, 3].

Крім того, алгоритмічні методи, породжені теорією чисел, мають критичне значення для оптимізації в програмуванні та обчислювальних науках. Це проявляється в ефективних алгоритмах тестування простоти, таких як Міллера-Рабіна, що використовуються для швидкої генерації криптографічних ключів. Арифметика великої точності, реалізована для обробки чисел довільної довжини, є основою для всіх сучасних криптографічних обчислень [6]. Також методи лінійного та цілочислового програмування, які ґрунтуються на теорії чисел, вирішують складні оптимізаційні задачі в розподілі ресурсів і плануванні [1].

Принципи цієї математичної дисципліни глибоко інтегровані в основні технології захисту даних та зв'язку. Цифрові підписи, зокрема алгоритм ECDSA, забезпечують автентифікацію та цілісність даних як в блокчейн-системах, так і в електронному документообігу [2, 5]. Коди виправлення помилок, такі як алгоритм Ріда-Соломона, що працюють на основах полів Галуа, захищають цілісність інформації на оптичних носіях та в мережевих передачах [2]. Нарешті, саме глибоке розуміння математичних основ дозволяє фахівцям з криптоаналізу та кіберфорензики розробляти ефективні методи виявлення вразливостей і протидії атакам на криптографічні системи.

Таким чином, алгоритмічна теорія чисел з абстрактної галузі знань перетворилася на ключовий інструментарій для побудови цифрового суспільства, безпосередньо впливаючи на технологічний суверенітет та обороноздатність держави в кіберпросторі.

Список використаних джерел

1. Андрунік В.А., Висоцька В.А., Пасічник В.В., Чирун Л.Б., Чирун Л.В. Чисельні методи в комп'ютерних науках. Том 2: навч. посібник. Львів: Національний університет «Львівська політехніка». URL: https://ism.lpnu.ua/uk/content/chyselni-metody-v-kompyuternyh-naukah-tom-2
2. Real-Life Applications of Number Theory // GeeksforGeeks. 2023. URL: https://www.geeksforgeeks.org/maths/real-life-applications-of-number-theory/
3. Bowcut S. Why math matters in cybersecurity // CybersecurityGuide.org. 2023. URL: https://cybersecurityguide.org/resources/math-in-cybersecurity/
4. Алгоритмічна теорія чисел // Вікіпедія. 2023. URL: https://uk.wikipedia.org/wiki/Алгоритмічна_теорія_чисел (дата звернення: 05.12.2025)
5. Whitson G.M. Cryptology and number theory in computer security // EBSCO. 2024. URL: https://www.ebsco.com/research-starters/computer-science/cryptology-and-number-theory-computer-security.
6. Числові типи даних – урок. Інформатика, 8 клас НУШ // МійКлас. 2023. URL: https://www.miyklas.com.ua/p/informatica/8-klas/algoritmi-ta-programi-394917/osnovni-tipi-danikh-zminni-virazi-operatciyi-481751/re-adc003a2-539e-4672-8d2e-887bd370e31d