https://doi.org/10.31891/2307-5732-2025-355-31
УДК 004.056.55

**КОЗУБ НАТАЛІЯ**
Херсонський національний технічний університет
https://orcid.org/0000-0002-0406-0161
e-mail: actinis1@gmail.com
**МЕДИНСЬКИЙ МИКОЛА**
Херсонський національний технічний університет
https://orcid.org/0009-0004-6982-8292
e-mail: nikolassswork@gmail.com

# КРИПТОГРАФІЧНО СТІЙКІ БУЛЕВІ ФУНКЦІЇ: АНАЛІЗ НЕЛІНІЙНОСТІ, СТІЙКОСТІ ТА КОРЕЛЯЦІЙНОЇ ІМУННОСТІ

*Булеві функції є основним елементом криптографічних систем, оскільки впливають на їх безпеку через такі властивості, як нелінійність, збалансованість, стійкість до атак і кореляційну імунність. В даній статті розглядаються теоретичні основи булевих функцій, зокрема їх роль у криптографії, а також криптографічні критерії якості, що включають нелінійність, кореляційну імунність, стійкість та збалансованість. Окремо висвітлюються теоретичні обмеження та конфлікти між властивостями булевих функцій. У статті також наводяться приклади конкретних булевих функцій, таких як бент-функція, XOR-функція та функція Фаулера, з аналізом їх характеристик, що допомагає зрозуміти їх застосування в реальних криптографічних системах. Завершення статті присвячене аналізу цих функцій та визначенню їх придатності для різних криптографічних завдань.*

*Ключові слова: булеві функції, криптографія, нелінійність, кореляційна імунність, стійкість, збалансованість, бент-функція, XOR-функція, функція Фаулера, криптографічні критерії, теоретичні обмеження.*

**KOZUB NATALIIA**
**MEDYNSKYI MYKOLA**
Kherson National Technical University

## CRYPTOGRAPHICALLY STABLE BOOLEAN FUNCTIONS: ANALYSIS OF NONLINEARITY, STABILITY, AND CORRELATIONAL IMMUNITY

*In the modern digital world, where the volume of information transmitted and stored electronically is rapidly increasing, the issue of ensuring the confidentiality, integrity, and authenticity of data has become critically important. Among the numerous areas of cryptography that provide information protection, symmetric encryption systems—specifically stream and block ciphers—hold a special place. One of the fundamental components of such systems is Boolean functions, which serve as the core for constructing cryptographic primitives. Boolean functions, as mappings from binary space to binary values, may seem like simple mathematical objects at first glance. However, in the context of cryptography, they must meet complex and often conflicting requirements. An ideal Boolean function for cryptographic purposes must be nonlinear to prevent linear attacks; stable, meaning balanced and insensitive to fixing a certain number of variables; and correlation immune to withstand correlation attacks based on the analysis of statistical relationships between input and output bits.*

*Unfortunately, achieving all these properties simultaneously is limited by a number of theoretical results, particularly the Zaytsev–Siegel–Chang theorem, which establishes the boundaries of possible coexistence of stability, nonlinearity, and immunity in Boolean functions. This presents a real challenge for cryptographers: to find functions that, while not ideal, provide an acceptable compromise between security and efficiency.*

*The aim of this article is a deep analysis of the main cryptographic properties of Boolean functions — nonlinearity, stability, and correlation immunity. Formal definitions of these characteristics, algorithms for their computation, and examples of functions used in practice are considered. Special attention is paid to the interrelationship of properties and the theoretical limitations that define the boundaries of constructing cryptographically strong Boolean functions.*

*Keywords: boolean functions, cryptography, nonlinearity, correlation immunity, stability, balance, bent function, XOR function, Fowler function, cryptographic criteria, theoretical limitations.*

Стаття надійшла до редакції / Received 03.06.2025
Прийнята до друку / Accepted 26.06.2025

### Теоретичні основи булевих функцій

Булеві функції є фундаментальними об'єктами в дискретній математиці, що знаходять широке застосування у цифровій логіці, теорії обчислень, схемотехніці та, зокрема, у криптографії. Формально булева функція — це відображення $f$: $F_2^n \to F_2$, де $F_2 = \{0,1\}$ - двоелементне поле, а $n$ — кількість змінних. Таким чином, булева функція перетворює $n$-вимірний бінарний вектор на одне бінарне значення.

Булеву функцію можна представити кількома способами:

1. табличне подання: перелік усіх можливих вхідних векторів та відповідних значень функції. Це найпростіше подання, зручне для малих $n$, але експоненціально зростає з $n$;
2. алгебра Жегалкіна (поліном над $F_2$): будь-яку булеву функцію можна однозначно подати у вигляді многочлена:

$f(x_1, \dots, x_n) = \bigoplus_{a \in F_2^n} c_a \cdot x_1^{a_1} \cdots x_n^{a_n}$, де $c_a \in F_2$, а $\oplus$ - додавання за модулем 2.

Цей поліном також називається *нормальною формою Жегалкіна*;

3. логічні подання: у вигляді логічних виразів із використанням операцій AND, OR, NOT (або їх еквівалентів у $F_2$: кон'юнкція, диз'юнкція, заперечення, XOR тощо);
4. спектральне подання: розклад функції у базисі Волша—Адамара, що використовується для оцінювання властивостей, таких як нелінійність та кореляційна імунність.

У загальному випадку, для криптографії найбільш цікавими є ті булеві функції, які демонструють високу стійкість до атак і непередбачувану поведінку. У цьому контексті важливими характеристиками функції є:

1. ступінь булевої функції — найвища степінь одночлена у поліномі Жегалкіна. Високий ступінь часто пов'язаний з високою складністю;
2. збалансованість — функція є збалансованою, якщо на $2^n$ можливих вхідних значень вона приймає значення 0 і 1 однакову кількість разів. Це критично важливо для забезпечення відсутності статистичних зрушень у криптографічних застосуваннях;
3. афінна властивість — функція є афінною, якщо її можна подати у вигляді:

$f(x_1, \dots, x_n) = a_0 \oplus a_1 x_1 \oplus \cdots \oplus a_n x_n$, де $a_i \in F_2$. Афінні функції не мають криптографічної сили, оскільки легко передбачувані;

4. лінійність та нелінійність — ступінь відхилення функції від афінної поведінки. Чим вища нелінійність, тим складніше здійснити лінійне наближення або атакувати функцію з використанням лінійного аналізу.

Залежно від значень параметрів, булеві функції поділяють на такі класи:

1. лінійні та афінні функції — найпростіші, непридатні для криптографії;
2. нелінійні функції — містять добутки змінних, мають більшу складність;
3. стійкі функції (resilient functions) - задовольняють умови збалансованості та нечутливості до деякої кількості фіксованих змінних;
4. криптографічні функції - спеціально сконструйовані так, щоб мати високі значення нелінійності, стійкості та кореляційної імунності.

**Приклади булевих функцій та їх характеристик**

**Приклад 1. Однозмінна функція**

Розглянемо булеву функцію $f(x)=x$.

1. Збалансованість: $f(0)=0, f(1)=1 \rightarrow$ збалансована (по одному 0 і 1).
2. Ступінь: 1 (одночлен першого ступеня).
3. Афінна: так, оскільки має вигляд $f(x)=x$.
4. Нелінійність: 0 (є афінною функцією, тож не має відхилення від афінності).

**Приклад 2. Двозмінна функція**

Розглянемо $f(x_1,x_2)=x_1 \cdot x_2$ (кон'юнкція).

| $x_1$ | $x_2$ | $f(x_1,x_2)$ |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 0 |
| 1 | 0 | 0 |
| 1 | 1 | 1 |

1. Збалансованість: 1 значення «1» і 3 нулі → незбалансована.
2. Ступінь: 2 (добуток двох змінних).
3. Афінна: ні.
4. Нелінійність:
   a) найближча афінна функція — наприклад, $fa(x_1,x_2)=0$ або $x_1 \oplus x_2$.
   b) відстань Гемінга до $f$: 1 → нелінійність = 1.

**Приклад 3. Трьохзмінна функція**

Розглянемо функцію $f(x_1,x_2,x_3)=x_1x_2 \oplus x_2x_3 \oplus x_1$.

1. поліном Жегалкіна: уже заданий.
2. збалансованість: створимо таблицю істинності [1]:

Таблиця 1

**Трьохзмінна функція** $f(x_1,x_2,x_3)=x_1x_2 \oplus x_2x_3 \oplus x_1$

| $x_1$ | $x_2$ | $x_3$ | $f$ |
|---|---|---|---|
| 0 | 0 | 0 | 0⊕0⊕0=0 |
| 0 | 0 | 1 | 0⊕0⊕0=0 |
| 0 | 1 | 0 | 0⊕0⊕0=0 |
| 0 | 1 | 1 | 0⊕1⊕0=1 |
| 1 | 0 | 0 | 0⊕0⊕1=1 |
| 1 | 0 | 1 | 0⊕0⊕1=1 |
| 1 | 1 | 0 | 1⊕0⊕1=0 |
| 1 | 1 | 1 | 1⊕1⊕1=1 |

3. ступінь: 2.

4. нелінійність:

для $n=3$, максимальна можлива нелінійність — 4,

обчислення спектру Волша дозволяє встановити відстань до найближчої афінної функції, *результат:* нелінійність = 4 (максимальна для $n=3$).

Ці приклади демонструють, як навіть прості булеві функції можуть мати важливі властивості, що впливають на їх криптографічну якість. Далі, формально опишемо ці властивості з позицій криптографічної безпеки.

**Криптографічні критерії якості булевих функцій**

У сучасній криптографії булеві функції відіграють ключову роль при проєктуванні симетричних шифрів, хеш-функцій та генераторів випадкових послідовностей. Від їхніх властивостей залежать такі параметри, як стійкість до атак, складність відновлення ключа, здатність до генерації статистично якісних бітів тощо. Для оцінювання ефективності булевих функцій у криптографічному контексті використовують низку критеріїв. Найважливішими серед них є *нелінійність, стійкість, кореляційна імунність, пропагативна здатність, а також збалансованість.*

Нелінійність булевої функції $f$: $F_2^n \rightarrow F_2$— це мінімальна відстань Гемінга між $f$ і множиною всіх афінних функцій. Вона визначає здатність функції протистояти лінійному криптоаналізу [5].

Формально: $NL(f)=min\ d_H(f, g),\ g \in A_n$, де $A_n$ — множина всіх афінних функцій, а $d_H$ — відстань Гемінга.

Максимальна можлива нелінійність: для $n$ змінних вона обмежена зверху: $NL(f) \leq 2^{n-1} - 2^{n/2-1}$, якщо n парне.

Функції з максимальною нелінійністю називають бент-функціями. Вони мають виняткові властивості, але ніколи не бувають збалансованими, тому не застосовуються безпосередньо в шифруванні, але корисні при конструюванні S-блоків.

Стійка булева функція — це така, яка залишається збалансованою, навіть якщо зафіксувати будь-яку підмножину з $t$ змінних. Стійкість визначає захищеність функції від атаки на основі підстановок (correlation attacks), коли криптоаналітик намагається спростити вхідний потік, фіксуючи деякі змінні.

Формально, $f$ є $t$-стійкою, якщо: вона збалансована, всі її $t$-значні фіксовані проєкції також збалансовані. Існує зв'язок між стійкістю, ступенем та кількістю змінних: $t+deg(f) \leq n-1$.

Кореляційна імунність булевої функції — це її здатність до протистояння атакам на основі статистичних залежностей між вхідними змінними і вихідним значенням. Функція $f$ має кореляційну імунність порядку $m$, якщо її спектр Волша $W_f(\omega)=0$ для всіх $\omega \in F_2^n$, де ваговий вектор $wt(\omega) \leq m$.

Висока кореляційна імунність потрібна в генераторах потокових шифрів, але вона часто знижує можливу нелінійність, бо існує компроміс між цими критеріями. Пропагативна здатність (Propagation Criterion, PC) характеризує здатність булевої функції реагувати на зміну вхідного біта зміною вихідного результату. Вона вимірює криптографічну дифузію, критично важливу для шифрів блочного типу.

PC-1: функція змінює своє значення при зміні одного біта на вході з ймовірністю близько 0.5. Функція задовольняє критерій PC порядку $k$, якщо будь-яка зміна не більше ніж $k$ вхідних бітів призводить до зміни виходу з імовірністю 50%.

Як зазначали вище, збалансованою є булева функція, в якій кількість одиниць і нулів серед значень на всіх входах однакова: $wt(f)=2^{n-1}$. Збалансованість гарантує відсутність статистичної асиметрії в потоці шифрування. У незбалансованих функцій з'являється бітова перевага, що дає змогу атакувальнику знайти шаблони.

**Компроміси між критеріями**

Проблема проектування якісних булевих функцій полягає в неможливості одночасно досягти максимальних значень для всіх криптографічних критеріїв. Наприклад:

1) бент-функції мають максимальну нелінійність, але не є збалансованими;
2) стійкі функції часто мають нижчий ступінь і обмежену нелінійність;
3) висока кореляційна імунність суперечить високій нелінійності через обмеження спектру Волша.

Тому при проектуванні криптографічних алгоритмів важливо вибирати функції з оптимальним компромісом, залежно від типу атаки, проти якої необхідно забезпечити захист [3; 6].

**Конфлікт властивостей: теореми обмежень**

Проектування булевих функцій для криптографічних застосувань пов'язане з численними компромісами між різними властивостями функцій. Однієї з головних проблем є те, що не всі важливі криптографічні властивості можуть бути досягнуті одночасно.

**Компроміси при проектуванні**

При проектуванні криптографічних систем, що використовують булеві функції, потрібно враховувати обмеження на властивості. Наприклад, бажання максимізувати нелінійність може призвести до втрати стійкості або збалансованості функції. Ось кілька важливих моментів:

1) бент-функції мають максимальну нелінійність, але вони не збалансовані. Вони можуть бути використані в специфічних контекстах, таких як різні структури блочних шифрів, але не підходять для функцій, де необхідно зберігати збалансованість (наприклад, у генераторах псевдовипадкових послідовностей) [2];

2) стійкі функції, що добре захищені від атак, можуть мати нижчий ступінь нелінійності, що робить їх менш ефективними в контексті криптографічної безпеки, якщо максимальна нелінійність є критичною вимогою;
3) кореляційно-імунні функції не можуть мати одночасно високу нелінійність, що також обмежує їх застосування в певних типах шифрів.

Дослідження Carlet [3] підкреслює важливість побудови булевих функцій, які одночасно задовольняють кілька криптографічних вимог.

**Практичні рекомендації для вибору булевих функцій**

Коли криптографи вибирають булеві функції для конкретного застосування, вони орієнтуються на компроміси між різними властивостями:

1) для генераторів випадкових послідовностей і хеш-функцій важливими є властивості нелінійності та кореляційної імунності;
2) для блочних шифрів важливими є стійкість і пропагативна здатність;
3) для криптографічних конструкцій, які потребують балансу між різними властивостями, можуть бути обрані функції з поміркованими значеннями нелінійності і стійкості.

Загалом, проектування криптографічних функцій вимагає глибокого розуміння цих теоретичних обмежень і обрання відповідних компромісів, щоб забезпечити максимальну безпеку системи.

**Приклади та аналіз булевих функцій**

Наведемо декілька класичних прикладів булевих функцій, які використовуються в криптографії, а також проведемо їх аналіз згідно з важливими криптографічними критеріями, такими як нелінійність, кореляційна імунність, стійкість та збалансованість.

**Приклад 1. Бент-функції**

Бент-функція - це булева функція $f: \{0,1\}^n \to \{0,1\}$, яка має максимально можливу нелінійність. Вона визначена тільки для парного числа змінних *n,* і її відмінність від усіх лінійних функцій максимальна. Однак однією з ключових властивостей бент-функцій є: бент-функції не можуть бути збалансованими. Бент-функції мають значення 1 і 0 в неоднаковій кількості. Наприклад, для *n=2*, є лише одна бент-функція (з 4 можливих входів), яка приймає 1 лише один раз і 0 — тричі (або навпаки). Отже, бент-функція завжди незбалансована і тому не може використовуватись у криптографії як єдина основа, наприклад, для S-box, без додаткової обробки — бо збалансованість є бажаною властивістю для захисту від атак. Бент-функції — це відмінний вибір для використання в контекстах, де важлива максимальна нелінійність, але вони не підходять для систем, де важлива висока кореляційна імунність і пропагативна здатність. Вони є корисними для побудови деяких криптографічних конструкцій, але не завжди підходять для всіх випадків.

**Приклад 2. Функція, що забезпечує стійкість**

Розглянемо просту булеву функцію $f(x_1,x_2,x_3)=x_1 \oplus x_2 \oplus x_3$, де $\oplus$ позначає операцію XOR. Це базова функція, що широко використовується в криптографічних системах для побудови генераторів псевдовипадкових чисел та в потокових шифрах.

1) нелінійність цієї функції дорівнює 1, оскільки вона є лінійною (це просто XOR трьох змінних);
2) функція збалансована, оскільки вона має рівну кількість одиниць та нулів для всіх можливих комбінацій змінних;
3) оскільки ця функція має низьку нелінійність, її стійкість до атак типу диференціальний аналіз буде обмеженою;
4) ця функція має високу кореляційну імунність для більшості малих підмножин змінних, однак через лінійність вона може бути уразливою для лінійного криптоаналізу.

Таким чином, ця функція добре підходить для простих застосувань, де важливі збалансованість та стійкість, але її лінійність обмежує її використання у криптографічних системах, що потребують високої нелінійності. Вона може бути застосована в простих генераторах псевдовипадкових чисел або для певних етапів у побудові шифрів.

**Приклад 3. Функція Фаулера**

Функція Фаулера є класичною функцією, яка використовується в криптографії для побудови генераторів псевдовипадкових чисел. Вона є прикладом функції, що має добрі характеристики нелінійності та стійкості.

Нехай $f(x_1,x_2,x_3,x_4)=x_1 \oplus (x_2 \cdot x_3) \oplus x_4$ де $\cdot$ позначає операцію AND. Це нелінійна функція з чотирьох змінних.

1) нелінійність цієї функції вища за просту лінійну функцію, але не максимальна. Вона забезпечує високу стійкість проти лінійного криптоаналізу;
2) функція не є збалансованою, оскільки її значення виводяться залежно від множення змінних. Це може призвести до статистичних асиметрій у результатах;
3) функція має високий рівень стійкості завдяки своїй нелінійності. Вона є стійкою до атак на основі фіксації деяких змінних;
4) функція має хорошу кореляційну імунність для низьких порядків, оскільки змінні функції не лінійно залежать одна від одної.

Як бачимо, функція Фаулера добре підходить для застосувань, де важлива нелінійність та стійкість. Вона має добрі криптографічні властивості, хоча її не збалансованість обмежує її використання в деяких контекстах, таких як генератори випадкових чисел, де збалансованість є критичною. У таблиці 1 наведено порівняння трьох функцій з різними властивостями.

Таблиця 2

**Порівняння трьох функцій з різними властивостями**

| Функція | Нелінійність | Збалансованість | Стійкість | Кореляційна імунність |
|---|---|---|---|---|
| Бент-функція | Максимальна | Ні | Висока | Висока |
| XOR функція | Низька | Так | Низька | Висока |
| Функція Фаулера | Середня | Ні | Висока | Середня |

Таким чином, бент-функція є оптимальним вибором для застосувань, де важлива максимальна нелінійність та стійкість до лінійного криптоаналізу, але через свою відсутність збалансованості вона не підходить для генерації випадкових чисел; функція XOR підходить для простих застосувань, але її лінійність обмежує її використання в більш складних криптографічних системах; функція Фаулера, незважаючи на її низьку збалансованість, є чудовим компромісом для генераторів псевдовипадкових чисел і криптографічних схем, де важлива нелінійність та стійкість.

**Досвід навчання студентів при вивченні криптографічних властивостей булевих функцій**

Під час викладання теми «Булеві функції та їх криптографічні властивості» студентам спеціальностей 121 «Інженерія програмного забезпечення» та 122 «Комп'ютерні науки» було виявлено, що найскладнішими для засвоєння є питання, пов'язані з розумінням взаємозв'язку між теоретичними властивостями функцій та їх практичною роллю в захисті інформації. Зокрема, студенти часто потребують додаткових прикладів, які демонструють компроміс між високою нелінійністю та збалансованістю, а також вплив низької кореляційної імунності на вразливість криптографічної системи.

Для підвищення мотивації та практичного розуміння теми ефективними виявилися завдання з аналізу реальних функцій, наприклад, побудова бент-функцій та розрахунок їх характеристик у програмному середовищі Python або SageMath. Це дозволило студентам не лише формально засвоїти теоретичний матеріал, а й на практиці побачити наслідки відсутності чи наявності певної властивості функції. Крім того, інтеграція навчального контенту з сучасними викликами інформаційної безпеки — такими як криптостійкість проти атак диференціального або лінійного типу — стимулювала студентів до міждисциплінарного мислення й застосування знань з інших дисциплін, зокрема математичної логіки, теорії складності, алгоритмів.

**Висновки з даного дослідження**

Булеві функції є важливими елементами сучасних криптографічних систем, оскільки вони забезпечують необхідні властивості, такі як нелінійність, стійкість до атак та кореляційну імунність, які є основою для створення безпечних шифрів і механізмів генерації псевдовипадкових чисел. В результаті проведеного аналізу можна зробити наступні основні висновки: для шифрів, що потребують високого рівня захисту від лінійного криптоаналізу, найкращим вибором є бент-функції, які досягають максимального рівня нелінійності, але їх не збалансованість обмежує використання цих функцій у випадках, де важливе рівномірне розподілення одиничних і нульових значень, для простих криптографічних застосувань. Де важлива збалансованість, але не критична нелінійність, можна використовувати функції на основі операцій XOR. Вони прості у реалізації, проте їх низька нелінійність обмежує захист від більш складних атак. Функції, що використовують комбінацію логічних операцій (як функція Фаулера), можуть забезпечити хороший компроміс між нелінійністю та стійкістю, проте їх незбалансованість потребує додаткової уваги під час розробки криптографічних схем, які потребують рівномірного розподілення вихідних значень.

Важливою проблемою є конфлікти між властивостями: для досягнення високої нелінійності або стійкості можуть викликати труднощі з балансом або кореляційною імунністю. Тому в реальних криптографічних системах часто потрібно знаходити компроміси, залежно від конкретних вимог до безпеки. Проектування криптографічних функцій вимагає ретельного аналізу та вибору оптимальних характеристик. Подальші дослідження повинні зосередитись на розробці нових функцій, які забезпечують баланс між всіма необхідними криптографічними властивостями, а також на вдосконаленні методів їх аналізу та перевірки в умовах реальних загроз.

В умовах навчального процесу, аналіз подібних функцій дозволяє студентам формувати аналітичне мислення та розуміння практичних задач криптографії [7; 8].

**Література**

1. Crama, Y., Hammer, P. L. Boolean Functions: Theory, Algorithms, and Applications. – New York: Springer, 2011. – 770 p.

2. Cusick, T. W., Stanica, P. Cryptographic Boolean Functions and Applications. – 2nd ed. – Amsterdam: Academic Press, 2009. – 248 p.

3. Carlet, C. Boolean Functions for Cryptography and Error Correcting Codes // In: Crama, Y., Hammer, P.L. (Eds.). *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*. – Cambridge: Cambridge University Press, 2010. – P. 257–397.

4. Shparlinski, I. Cryptographic Applications of Analytic Number Theory: Complexity Lower Bounds and Pseudorandomness. – Basel: Birkhäuser, 2003. – 276 p.

5. Stinson, D. R., Paterson, M. Cryptography: Theory and Practice. – 4th ed. – Boca Raton: CRC Press, 2018. – 600 p.

6. Doerr, A., Levasseur, K. Applied Discrete Structures [Електронний ресурс]. – URL: https://discretemath.org (дата звернення: 07.05.2025).

7. Єршов, А. А., Глушков, В. М., Яновська, О. В. Дискретна математика: підручник. – К.: Вища школа, 2007. – 447 с.

8. Васильєв, В. В., Гапон, Ю. В. Основи криптології: теорія та практика: навч. посіб. – Харків: ХНУРЕ, 2015. – 196 с.

**References**

1. Crama, Y., Hammer, P. L. Boolean Functions: Theory, Algorithms, and Applications. – New York: Springer, 2011. – 770 p.

2. Cusick, T. W., Stanica, P. Cryptographic Boolean Functions and Applications. – 2nd ed. – Amsterdam: Academic Press, 2009. – 248 p.

3. Carlet, C. Boolean Functions for Cryptography and Error Correcting Codes // In: Crama, Y., Hammer, P.L. (Eds.). Boolean Models and Methods in Mathematics, Computer Science, and Engineering. – Cambridge: Cambridge University Press, 2010. – P. 257–397.

4. Shparlinski, I. Cryptographic Applications of Analytic Number Theory: Complexity Lower Bounds and Pseudorandomness. – Basel: Birkhäuser, 2003. – 276 p.

5. Stinson, D. R., Paterson, M. Cryptography: Theory and Practice. – 4th ed. – Boca Raton: CRC Press, 2018. – 600 p.

6. Doerr, A., Levasseur, K. Applied Discrete Structures [Electronic resource]. – URL: https://discretemath.org (access date: 07.05.2025).

7. Yershov, A. A., Glushkov, V. M., Yanovska, O. V. Discrete Mathematics: A Textbook. – Kyiv: Higher School, 2007. – 447 p.

8. Vasilyev, V. V., Hapon, Yu. V. Fundamentals of Cryptology: Theory and Practice: Educational Guide. – Kharkiv: KhNURE, 2015. – 196 p.