Міністерство освіти і науки України
Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"
Фізико-технічний інститут

КРИПТОГРАФІЯ
КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2
Криптоаналіз шифру Віженера

Виконали студенти групи ФБ-32:
Красноок Юлія та Водяник Дмитро

Київ - 2025

Мета роботи: Засвоєння методів частотного криптоаналізу. Здобуття навичок роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.

Порядок виконання роботи

0. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.
1. Самостійно підібрати текст для шифрування (2-3 кб) та ключі довжини r = 2, 3, 4, 5, а також довжини 10-20 знаків. Зашифрувати обраний відкритий текст шифром Віженера з цими ключами.
2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.
3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).

Хід роботи:

1. Самостійно підібрати текст для шифрування (2-3 кб) та ключі довжини r = 2, 3, 4, 5, а також довжини 10-20 знаків. Зашифрувати обраний відкритий текст шифром Віженера з цими ключами.

Ключ довжиною r = 2: да
Ключ довжиною r = 3: дом
Ключ довжиною r = 4: река
Ключ довжиною r = 5: слово
Ключ довжиною 19 знаків (в межах 10-20): преступлениеинаказание

Текст:

```
в начале июля. в чрезвычайно жаркое время. под вечер. один
молодой человек вышел из своей каморки. которую нанимал от
жильцов в см переулке. на улицу и медленно. как бы в
нерешимости. отправился к кну мосту. он благополучно избегнул
встречи с своею хозяйкой на лестнице. каморка его приходилась
под самою кровлей высокого пятиэтажного дома и походила более
на шкаф. чем на квартиру. квартирная же хозяйка его. у которой
он нанимал эту каморку с обедом и прислугой. помещалась одною
лестницей ниже. в отдельной квартире. и каждый раз. при выходе
на улицу. ему непременно надо было проходить мимо хозяйкиной
кухни. почти всегда настежь отворенной на лестницу. и каждый
раз молодой человек. проходя мимо. чувствовал какое-то
болезненное и трусливое ощущение. которого стыдился и от
которого морщился. он был должен кругом хозяйке и боялся с нею
встретиться. не то чтоб он был так труслив и забит. совсем
```

даже напротив. но с некоторого времени он был в каком-то раздражительном и напряженном состоянии. похожем на ипохондрию. он до того углубился в себя и уединился от всех. что боялся даже всякой встречи. не только встречи с хозяйкой. он был задавлен бедностью. но и бедность даже перестала в последнее время тяготить его. насущными делами своими он совсем перестал и не хотел заниматься. никакой хозяйки. в сущности. он не боялся. что бы та ни замышляла против него. но останавливаться на лестнице. выслушивать всякий вздор про всю эту обыденную дребедень. до которой ему не было никакого дела. все эти приставания о платеже. угрозы. жалобы. и при этом самому изворачиваться. извиняться. лгать. нет. уж лучше проскользнуть как-нибудь кошкой по лестнице и уйти незамеченным.

Отриманий результат:

```
--- Аналіз тексту з файлу 'text-lab2.txt' ---
Довжина очищеного тексту (n): 1360 символів

--- Загальний Індекс Відповідності (IC) ---
IC Відкритого тексту (r=1): 0.055496

--- Шифрування та Аналіз ---

Ключ: 'да' (довжина r = 2)
 -> Зашифрований текст збережено: ciphertext_да.txt
Загальний IC Шифртексту: 0.045896

Ключ: 'дом' (довжина r = 3)
 -> Зашифрований текст збережено: ciphertext_дом.txt
Загальний IC Шифртексту: 0.037138

Ключ: 'река' (довжина r = 4)
 -> Зашифрований текст збережено: ciphertext_река.txt
Загальний IC Шифртексту: 0.033984

Ключ: 'слово' (довжина r = 5)
 -> Зашифрований текст збережено: ciphertext_слово.txt
Загальний IC Шифртексту: 0.039045

Ключ: 'преступлениеинаказание' (довжина r = 22)
 -> Зашифрований текст збережено: ciphertext_преступлениеинаказание.txt
Загальний IC Шифртексту: 0.033648
```

(Зашифровані тексти додамо окремими файлами)

Метод реалізації:

Шифрування виконується у функції vigenere_encrypt(plaintext, key).Спочатку текст і ключ очищуються від зайвих символів (preprocess_text()), залишаючи лише літери з заданого алфавіту. Далі для кожного символу відкритого тексту береться його числовий код (позиція в алфавіті) і додається код відповідної букви ключа за модулем довжини алфавіту M = 33:

cipher_int = (text_int + key_int) % M

Отримане число перетворюється назад у букву — це і є зашифрований символ. Ключ повторюється по колу, щоб його довжина відповідала довжині тексту.

2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.

```
--- Порівняння загальних IC (Завдання 2) ---
IC Відкритого тексту (r=1): 0.055496
IC Шифртексту (r=2, ключ='да'): 0.045896
IC Шифртексту (r=3, ключ='дом'): 0.037138
IC Шифртексту (r=4, ключ='река'): 0.033984
IC Шифртексту (r=5, ключ='слово'): 0.039045
IC Шифртексту (r=22, ключ='преступлениеинаказание'): 0.033648

Теоретичний IC (m=33): 0.030303
```

Методи реалізації:

Ми дивились, як часто в тексті повторюються однакові букви.Якщо текст — звичайний (відкритий), то деякі букви трапляються частіше (наприклад, «о», «е»), тому IC буде більший. Якщо текст зашифрований шифром Віженера, то букви розподілені майже випадково, тому IC менший і ближчий до 1/33 ≈ 0.0303.

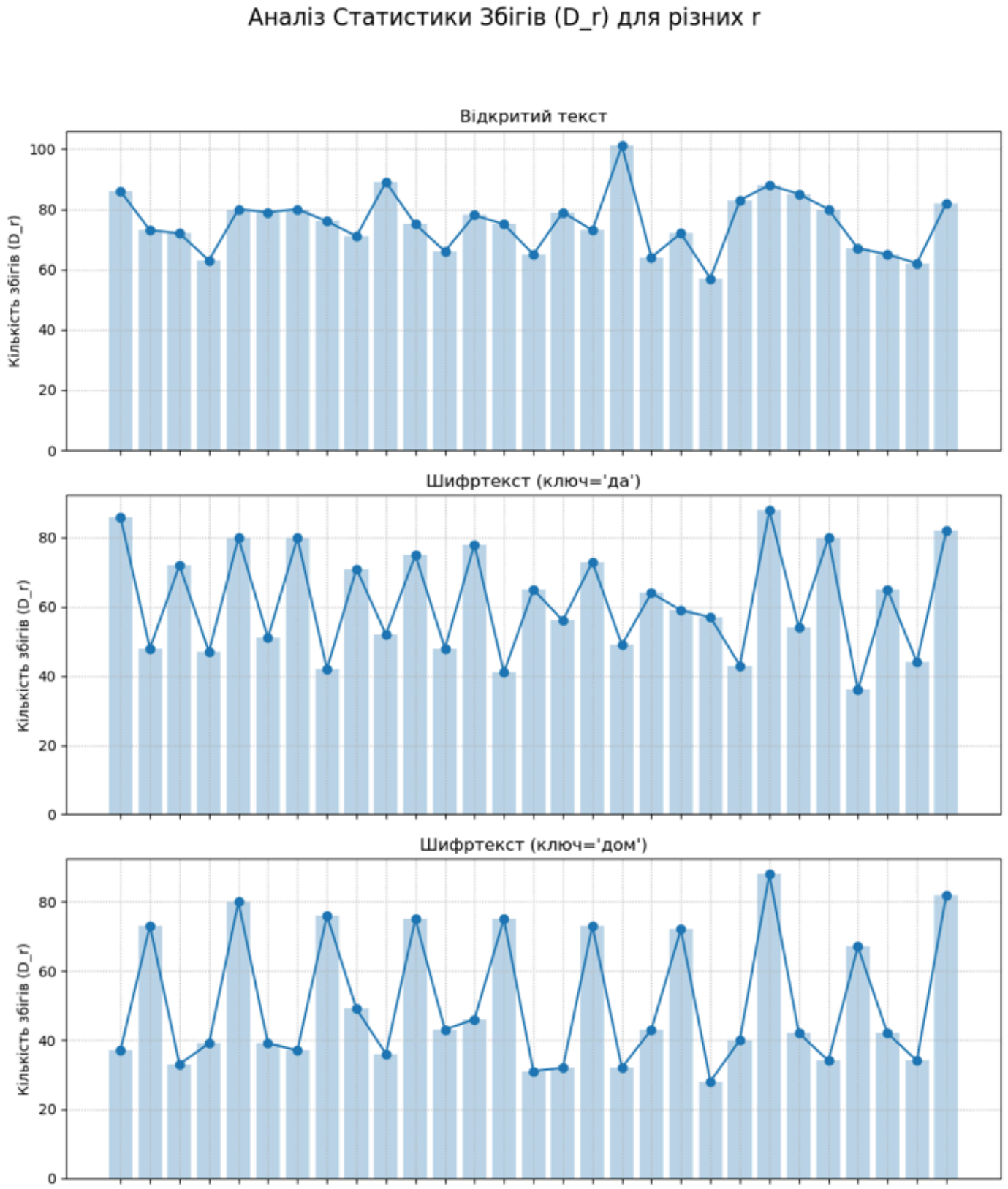
Показник D(r) : У функції calculate_dr_statistics() програма проходить текст і порівнює символи через r позицій:if text[i] == text[i + r]: dr_count += 1

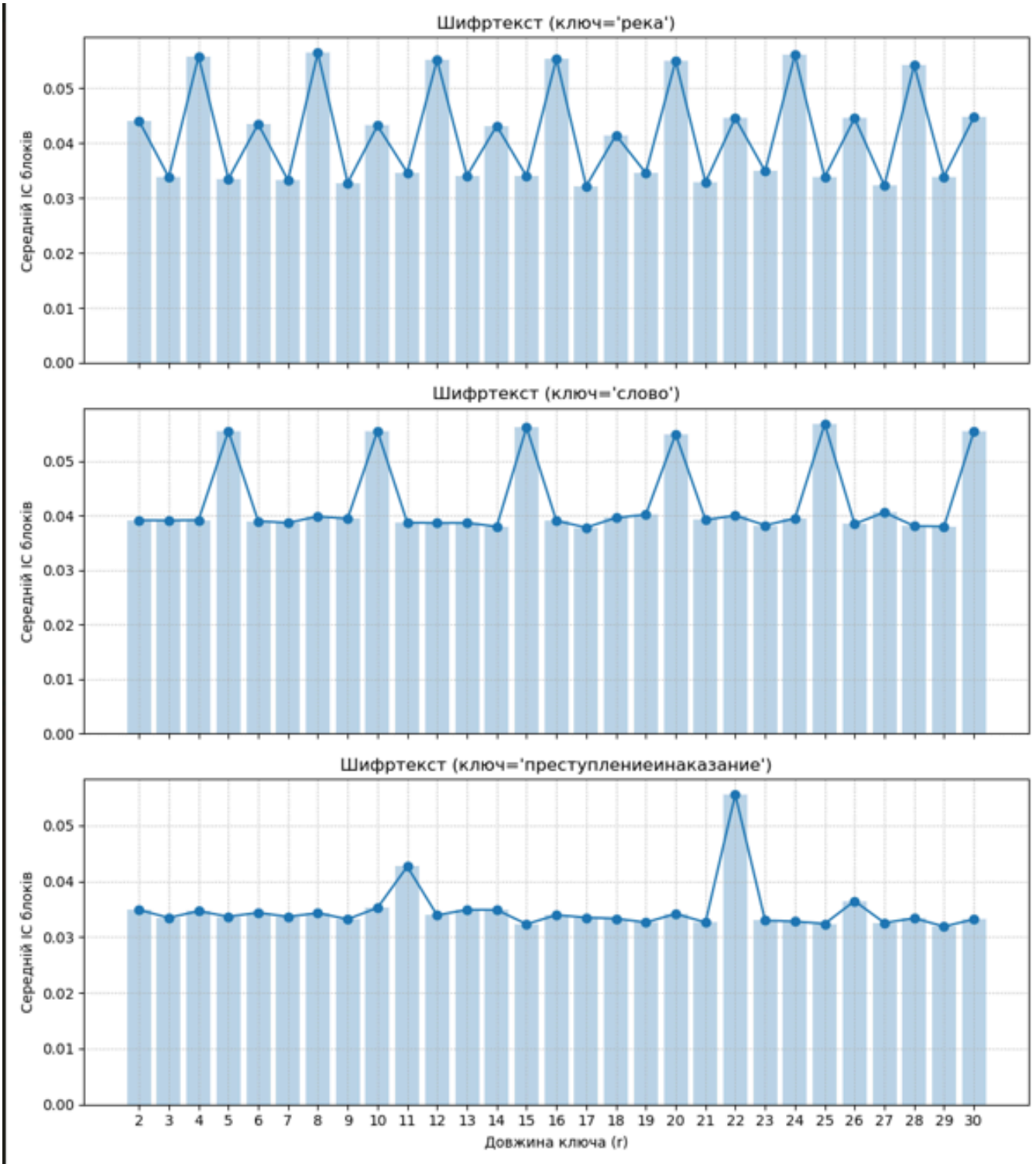
Для кожного зміщення r (від 2 до max_r) рахується кількість збігів dr_count,
тобто скільки букв у тексті збігаються із символами, що стоять через r.Якщо при певному r кількість збігів зростає, це може вказувати на довжину ключа шифру Віженера.

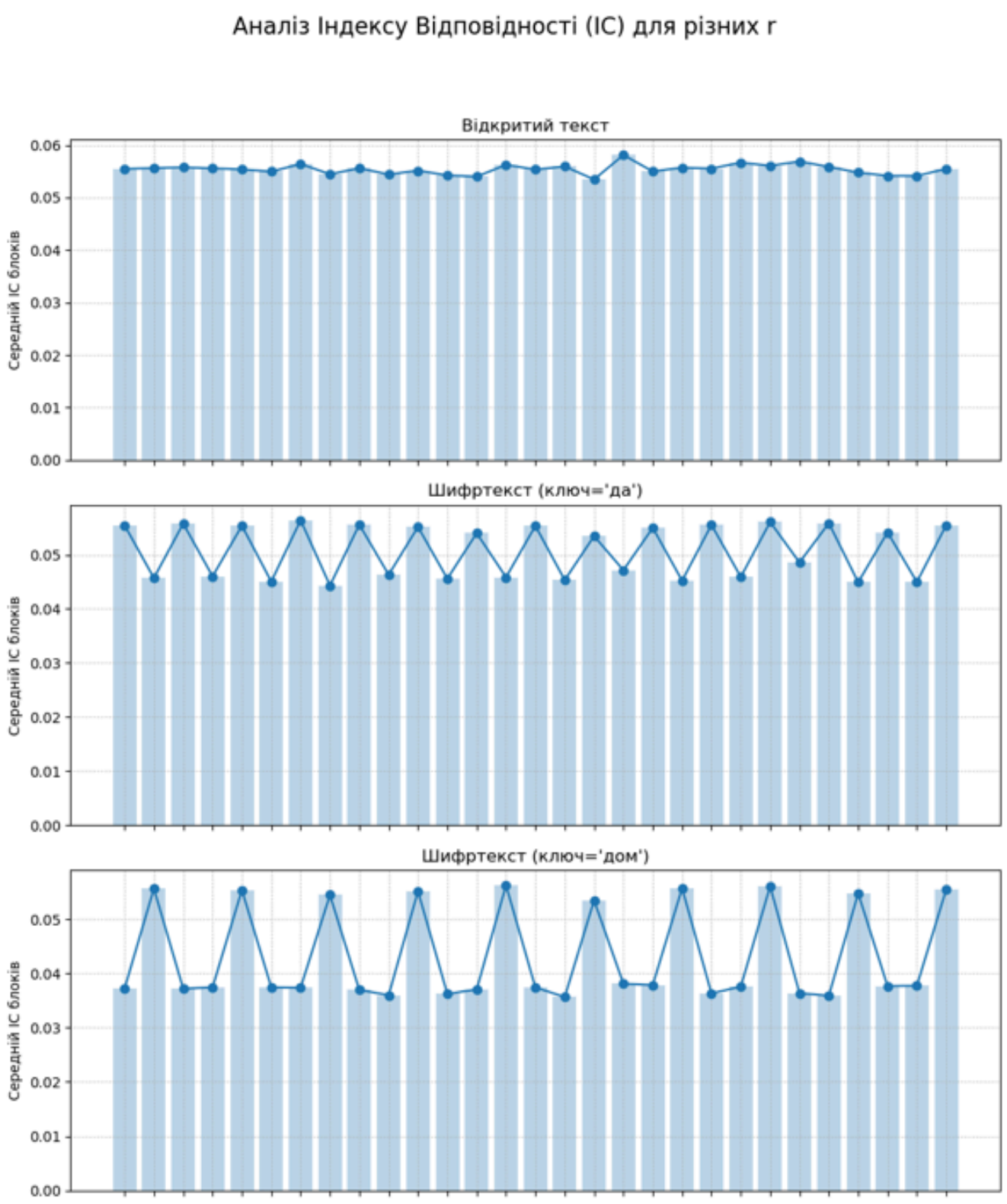
(Додано до протокола таблиці)

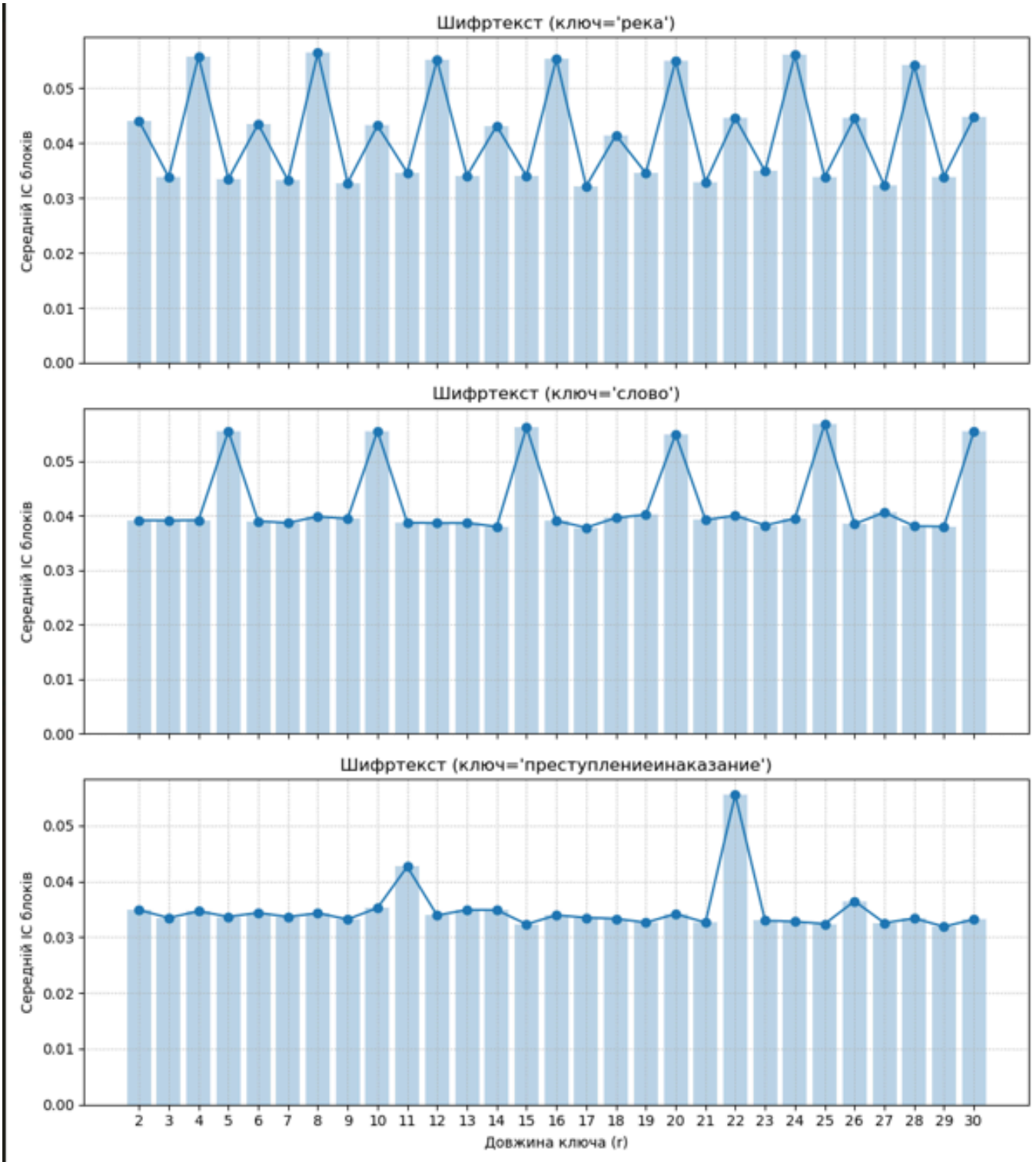
Діаграми:

:

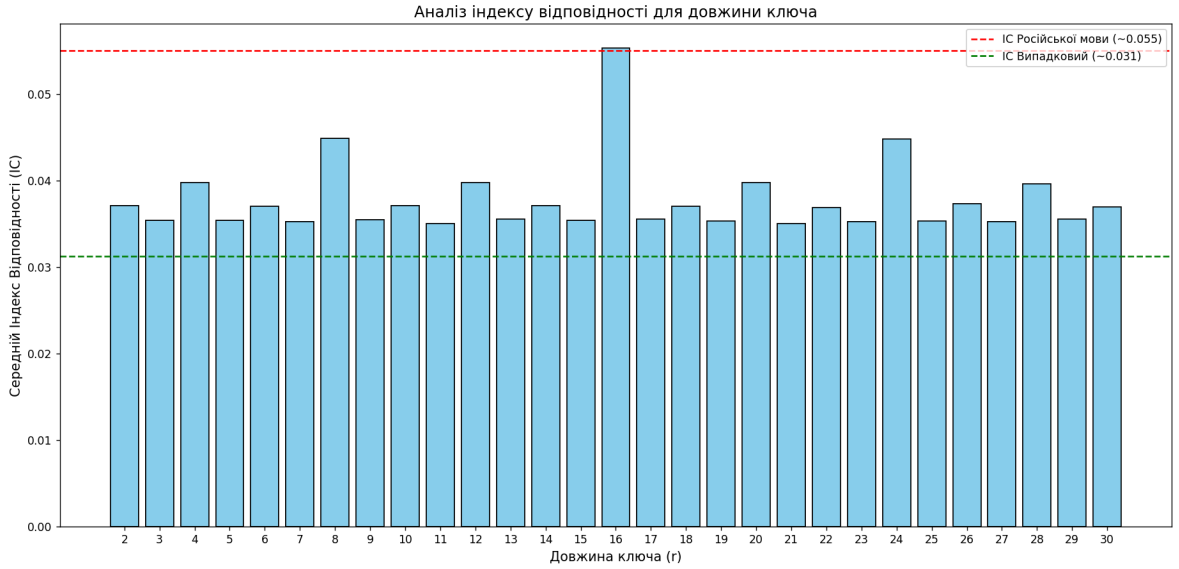

Аналіз Статистики Збігів (D_r) для різних r
Відкритий текст
Шифртекст (ключ='да')
Шифртекст (ключ='дом')
Кількість збігів (D_r)
0
20
40
60
80
100


Шифртекст (ключ='река')
Середній ІС блоків
0.00
0.01
0.02
0.03
0.04
0.05
Шифртекст (ключ='слово')
Середній ІС блоків
0.00
0.01
0.02
0.03
0.04
0.05
Шифртекст (ключ='преступлениеинаказание')
Середній ІС блоків
0.00
0.01
0.02
0.03
0.04
0.05
2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30
Довжина ключа (r)


Аналіз Індексу Відповідності (IC) для різних r
Відкритий текст
Шифртекст (ключ='да')
Шифртекст (ключ='дом')
Середній IC блоків
0.00
0.01
0.02
0.03
0.04
0.05
0.06


Шифртекст (ключ='река')
Середній ІС блоків
0.00
0.01
0.02
0.03
0.04
0.05
Шифртекст (ключ='слово')
Середній ІС блоків
0.00
0.01
0.02
0.03
0.04
0.05
Шифртекст (ключ='преступлениеинаказание')
Середній ІС блоків
0.00
0.01
0.02
0.03
0.04
0.05
2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30
Довжина ключа (r)

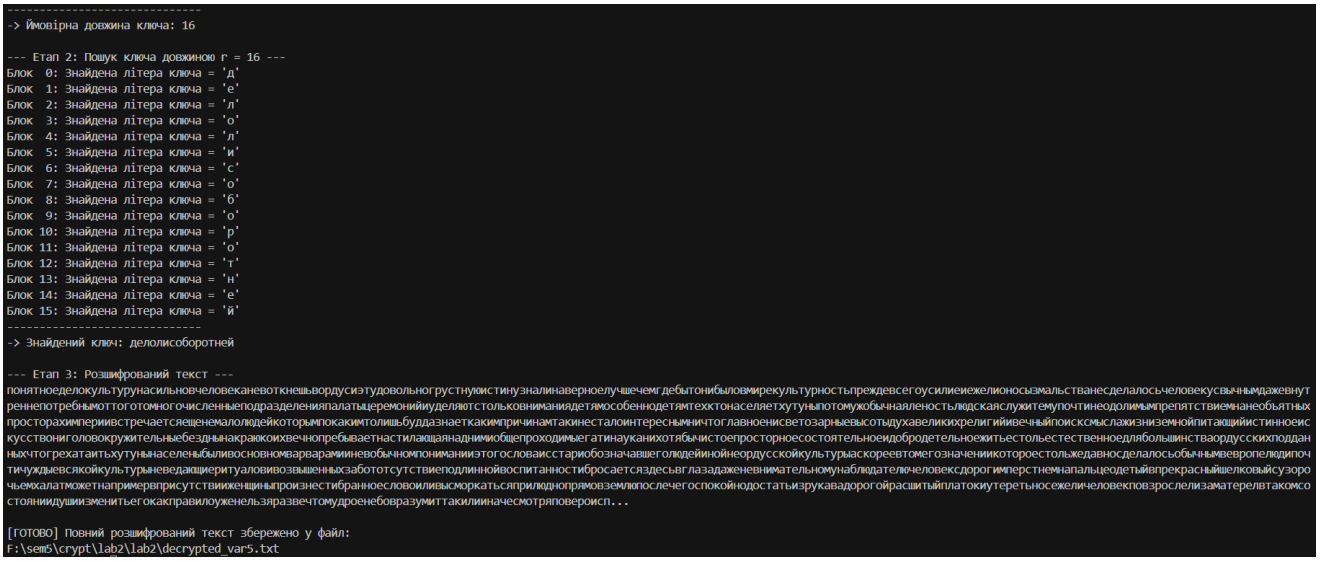
3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).



Отриманий результат:

```
PS C:\Users\PC> & C:/Users/PC/AppData/Local/Programs/Python/Python311/python.exe f:/sem5/crypt/lab2/lab2/lab2.3.py
Довжина очищеного шифртексту: 5621 символів

--- Етап 1: Пошук довжини ключа (r) ---
r =  2: 0.037072
r =  3: 0.035351
r =  4: 0.039749
r =  5: 0.035422
r =  6: 0.037037
r =  7: 0.035212
r =  8: 0.044851
r =  9: 0.035461
r = 10: 0.037072
r = 11: 0.035048
r = 12: 0.039756
r = 13: 0.035504
r = 14: 0.037067
r = 15: 0.035385
r = 16: 0.055325
r = 17: 0.035503
r = 18: 0.037042
r = 19: 0.035310
r = 20: 0.039748
r = 21: 0.035039
r = 22: 0.036850
r = 23: 0.035243
r = 24: 0.044813
r = 25: 0.035303
r = 26: 0.037297
r = 27: 0.035249
r = 28: 0.039642
r = 29: 0.035570
r = 30: 0.036919
```



Ми отримали ключ - оротнейделолисоб, якщо трохи зсунути текст, то отримаємо:
Дело лис-оборотней

Висновок:

Під час виконання роботи було засвоєно методи частотного криптоаналізу та здобуто навички аналізу шифру Віженера. Було досліджено два основні методи визначення періоду ключа: метод, що ґрунтується на індексі відповідності, та метод статистики співпадінь. Після знаходження періоду, задача дешифрування зводилася до розв'язання окремих шифрів Цезаря шляхом частотного аналізу кожного блоку. На практиці ці методики були успішно застосовані для знаходження ключа та повного розшифрування наданого шифртексту.