# Авторська довідка

*(кваліфікаційної роботи бакалавра)*

**Назва кваліфікаційної роботи бакалавра** *Криптоаналіз історичних шифрів заміни*
*назви записувати нижнім регістром (як у реченні)*

**Назва (англ.):** *Cryptanalysis of historical substitution ciphers*
*переклад англійською*

**Освітній ступінь :** бакалавр

**Шифр та назва спеціальності:** 125 «Кібербезпека»
напр.:151 Автоматизація та комп'ютерно-інтегровані технології

**Екзаменаційна комісія**: Екзаменаційна комісія № 37
*напр.: Екзаменаційна комісія №1*

**Установа захисту:** Тернопільський національний технічний університет імені Івана Пулюя
*напр.: Тернопільський національний технічний університет імені Івана Пулюя*

**Дата захисту:** 17 червня 2021 року **Місто:** Тернопіль

**Сторінки:**
Кількість сторінок роботи: 51

**УДК:** 004.056

**Автор роботи**
Прізвище, ім'я, по батькові (укр.): Цубера Василь Васильович
розкривати ініціали

Прізвище, ім'я (англ.): Tsubera Vasyl Vasylovych
*використовувати паспортну транслітерацію (КМУ 2010)*

Місце навчання (установа, факультет, місто, країна): ТНТУ ім. І. Пулюя, Факультет комп'ютерно-інформаційних систем і програмної інженерії, Кафедра кібербезпеки, м.Тернопіль, Україна

**Керівник**
Прізвище, ім'я, по батькові (укр.): Стадник Марія Андріївна
повністю

Прізвище, ім'я (англ.): Stadnyk Mariia Andriivna
*використовувати паспортну транслітерацію (КМУ 2010)*

Місце праці (установа, підрозділ, місто, країна): ТНТУ ім. І. Пулюя, Україна

Вчене звання, науковий ступінь, посада: кандидат технічних наук, старший викладач кафедри кібербезпеки

**Рецензент**
Прізвище, ім'я, по батькові (укр.): Скоренький Юрій Любомирович
повністю

Прізвище, ім'я (англ.): Skorenkyi Yurii Liubomyrovych
*використовувати паспортну транслітерацію (КМУ 2010)*

Місце праці (установа, підрозділ, місто, країна): ТНТУ ім. І. Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра фізики, м.Тернопіль, Україна
Вчене звання, науковий ступінь, посада: доцент, кандидат фізико-математичних наук, зав. кафедри ФЗ

**Ключові слова**
українською криптографія, атака, шифр, криптоаналіз, частотний аналіз, моноалфавітний шифр, поліалфавітний шифр
*до 10 слів*
англійською cryptography, attack, cipher, cryptanalysis, frequency analysis, monoalphabetic cipher, polyalphabetic cipher
*до 10 слів*

**Анотація**

українською:

Кваліфікаційна робота присвячена розробці програмного забезпечення для криптоаналізу історичних шифрів та дослідженню впливу частотного аналізу на них. В роботі обґрунтовано вибір програмного середовища розробки та вибір методів криптоаналізу моно- та поліалфавітних шифрів.. Розроблено програмне забезпечення, в якому реалізовано найпростіші методи криптоаналізу шифрів заміни, яке може бути використане в навчальних цілях для злому шифрованих текстів.

В роботі використано відомі методи криптоаналізу для моноалфавітних, біграмних та поліалфавітних шифрів та проведено оцінку складності злому текстів, зашифрованих різними шифрами. Встановлено, що шифр Віженера є найбільш складним для взлому, особливо якщо період ключа достатньо великий, або текст достатньо короткий. Встановлено також, що всі ці методи використовують частотний аналіз, який можливий лише при достатній довжині шифротексту.

англійською:

The qualification thesis is devoted to the development of software for cryptanalysis of historical ciphers and research of the influence of frequency analysis on them. The paper substantiates the choice of software development environment and the choice of methods of cryptanalysis of mono- and polyalphabetic ciphers.

The known methods of cryptanalysis for monoalphabetic, bigram and polyalphabetic ciphers are used in the thesis and the complexity of hacking of texts encrypted with different ciphers is estimated. It is established that the Vigener cipher is the most difficult to crack, especially if the key period is long enough or the plaintext is short enough. It is also established that all these methods use frequency analysis, which is possible only with a sufficient length of ciphertext.