**Додаток 1**
Форма відомостей про авторів матеріалу та описова інформація для видань ТНТУ

# Авторська довідка

*(реферату дипломної роботи магістра)*

**Назва дипломної роботи магістра:** Оцінка ефективності алгоритмів блоково-симетричного шифрування на основі використання міні-версій
*назви записувати нижнім регістром (як у реченні)*

Назва (англ.): Mini-versions-based assessment of block-symmetric encryption algorithms efficiency
*переклад англійською*

**Освітній ступінь :** ***магістр***

**Шифр та назва спеціальності:** **125** кібербезпека

*напр.:151 Автоматизація та комп'ютерно-інтегровані технології*

**Екзаменаційна комісія:** Екзаменаційна комісія №38
*напр.: Екзаменаційна комісія №1*

**Установа захисту:** Тернопільський національний технічний університет імені Івана

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

**Дата захисту:** 22.12.2020 **Місто:** Тернопіль

**Сторінки:**
Кількість сторінок дипломної роботи: 72 Кількість сторінок реферату:

**УДК:**

**Автор дипломної роботи**
Прізвище, ім'я, по батькові (укр.): Піх Василь Володимирович
*розкривати ініціали*

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

Місце навчання (установа, факультет, місто, країна): ТНТУ імені Івана Пулюя, ФІС кафедра КБ, Тернопіль

**Керівник**
Прізвище, ім'я, по батькові (укр.): Карпінський Микола Петрович
*повністю*

Прізвище, ім'я (англ.): Karpinski Mykola Petrovich
*використовувати паспортну транслітерацію (КМУ 2010)*

Місце праці (установа, підрозділ, місто, країна): ТНТУ імені Івана Пулюя. Кафедра КБ, Тернопіль

Вчене звання, науковий ступінь, посада: д.т.н., проф.

**Рецензент**
Прізвище, ім'я, по батькові (укр.): Никитюк Вячеслав Вячеславович
*повністю*

Прізвище, ім'я (англ.): Vyacheslav Nykytyuk
*використовувати паспортну транслітерацію (КМУ 2010)*

Місце праці (установа, підрозділ, місто, країна): ТНТУ імені Івана Пулюя, кафедра КН

Вчене звання, науковий ступінь, посада: к.т.н. асистент

**Ключові слова**

українською: МІНІ-ВЕРСІЯ, БЛОЧНИЙ СИМЕТРИЧНИЙ ШИФР, КРИПТОАНАЛІЗ, ДИФЕРЕНЦІАЛЬНИЙ КРИПТОАНАЛІЗ, ЛІНІЙНИЙ КРИПТОАНАЛІЗ, АТАКА.

*до 10 слів*

англійською: MINI-VERSION, BLOCK SYMMETRIC CIPHERS, CRYPTANALYSIS, DIFFERENTIAL CRYPTANALYSIS, LINEAR CRYPTANALYSIS, ATTACK

*до 10 слів*

**Анотація**

українською: Дана магістерська кваліфікаційна робота присвячена дослідженню методів підвищення ефективності використання міні-версій БСШ для оцінки криптостійкості повних шифрів.
Об'єктом дослідження є процес забезпечення адекватності використання міні-версій щодо оцінки криптостійкості повних шифрів.
Предметом дослідження є оцінка ефективності алгоритмів блоково-симетричного шифрування на основі використання міні-версій.
Алгоритми реалізовані на основі програмного забезпечення, розробленого в середовищі Microsoft Visual Studio 2013 мовою C# та C++.
При дослідженні алгоритмів конкурсантів використовувалася оцінка трьох показників: стійкості алгоритму до відомих криптоаналітичних атак, продуктивність програмної реалізації алгоритму на сучасних персональних комп'ютерах і "статистична безпека" (формування унікальних псевдовипадкових послідовностей).
У результаті проведений порівняльний аналіз міні-версій блочних симетричних шифрів України, та оцінено адекватність їх використання.
Методами розробки обрано:
При аналізі методів і алгоритмів симетричної криптографії використовуються міні-версії шифрів – конкурсантів на алгоритм симетричного шифрування в Україні. При досліджені рівня їх стійкості використовуються основні положення теорій захисту та криптоаналізу, а саме методи лінійного та диференціального аналізу.
При дослідженні стійкості алгоритму були використані методи теорії ймовірності та математичної статистики.
У результаті роботи проведено дослідження можливості використання міні-версій алгоритмів традиційного шифрування щодо отримання їх властивостей повних шифрів за рахунок оцінки стійкості до методів лінійного та диференційного аналізу.

*200-300 слів*

англійською: This master's thesis is devoted to the study of methods to improve the efficiency of using mini-versions of block symmetric ciphers (BSC) to assess the cryptographic strength of complete ciphers.
The object of the study is the process of ensuring the adequacy of the use of mini-versions in assessing the cryptographic strength of complete ciphers.
The subject of the study is to evaluate the effectiveness of block-symmetric encryption algorithms based on the use of mini-versions.
The algorithms are implemented on the basis of software developed in Microsoft Visual Studio 2013 in C # and C ++.
In the study of the algorithms of the contestants used the assessment of three indicators: the resistance of the algorithm to known cryptanalytic attacks, the performance of software implementation of the algorithm on modern personal computers and "statistical security" (formation of unique pseudo-random sequences).
As a result, a comparative analysis of mini-versions of block symmetric ciphers of Ukraine was conducted, and the adequacy of their use was assessed.
Development methods selected:
In the analysis of methods and algorithms of symmetric cryptography, mini-versions of ciphers are used – a competition for the symmetric encryption algorithm in Ukraine. In studying the level of their stability, the main provisions of the theories of protection and cryptanalysis are used, namely the methods of linear and differential

analysis.
Methods of probability theory and mathematical statistics were used to study the stability of the algorithm.
As a result, the possibility of using mini-versions of traditional encryption algorithms to obtain their properties of complete ciphers by assessing the resistance to the methods of linear and differential analysis.

*200-300 слів*