**Додаток 1**

Форма відомостей про авторів матеріалу та описова інформація для видань ТНТУ

**Авторська довідка**

*(кваліфікаційної роботи бакалавра)*

**Назва кваліфікаційної роботи бакалавра:** аналіз та оцінка ефективності сучасних асиметричних криптографічних алгоритмів

*назви записувати нижнім регістром (як у реченні)*

Назва (англ.): analysis and evaluation of the effectiveness of modern asymmetric cryptographic algorithms

*переклад англійською*

**Освітній ступінь : *бакалавр***

**Шифр та назва спеціальності:** 125 Кібербезпека

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

**Екзаменаційна комісія:** Екзаменаційна комісія №1

*напр.: Екзаменаційна комісія №1*

**Установа захисту:** Тернопільський національний технічний університетімені Івана Пулюя

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

**Дата захисту:** 25.06.2024  **Місто:** Тернопіль

**Сторінки:**

Кількість сторінок роботи: 73

**УДК:**  004.56

**Автор роботи**

Прізвище, ім’я, по батькові (укр.): Вихованець Дмитро Володимирович

*розкривати ініціали*

Прізвище, ім’я (англ.): Vykhovanets Dmytro

*використовувати паспортну транслітерацію (КМУ 2010)*

Місце навчання (установа, факультет, місто, країна): Тернопільський національний технічний університет імені Івана Пулюя, факультет комп’ютерно-інформаційних систем і програмної інженерії, Тернопіль, Україна

**Керівник**

Прізвище, ім’я, по батькові (укр.): Кульчицький Тарас Русланович

*повністю*

Прізвище, ім’я (англ.): Kulchytskyi Taras

*використовувати паспортну транслітерацію (КМУ 2010)*

Місце праці (установа, підрозділ, місто, країна): Тернопільський національний технічний університет імені Івана Пулюя, кафедра кібербезпеки, Тернопіль, Україна

Вчене звання, науковий ступінь, посада: кандидат технічних наук, доцент, зав.кафедри

**Рецензент**

Прізвище, ім’я, по батькові (укр.): Цебрій Олексій Романович

*повністю*

Прізвище, ім’я (англ.): Tsebriy Oleksiy

*використовувати паспортну транслітерацію (КМУ 2010)*

Місце праці (установа, підрозділ, місто, країна): Тернопільський національний технічний університет імені Івана Пулюя, кафедра програмної інженерії, Тернопіль, Україна

Вчене звання, науковий ступінь, посада: кандидат фізико-математичних наук, доцент кафедри ПІ

**Ключові слова**

Криптографія, цифровий підпис, вразливості, асиметричне шифрування, аутентифікація, цілісність інформації, захист інформації.

Сryptography, digital signature, vulnerabilities, asymmetric encryption, authentication, information integrity, information protection

**Анотація**

Дослідження присвячено аналізу та оцінці ефективності сучасних асиметричних криптографічних алгоритмів. Вибір надійного криптографічного алгоритму є критично важливим для забезпечення безпеки інформаційних систем, оскільки він безпосередньо впливає на захист конфіденційних даних.

У роботі розглянуто три популярні алгоритми для цифрових підписів: RSA, DSA та ECDSA. Теоретичний аналіз включав дослідження архітектури алгоритмів та їх ключових параметрів. Проведені експериментальні дослідження дозволили оцінити продуктивність алгоритмів з точки зору часу виконання, використання пам’яті та навантаження на процесор.

Отримані результати та розроблений підхід можуть бути корисними для системних адміністраторів та розробників з метою підвищення рівня захисту даних в інформаційних системах.

Висновки та рекомендації, представлені у роботі, сприятимуть підвищенню рівня безпеки інформаційних систем завдяки вибору найбільш ефективного асиметричного криптографічного алгоритму відповідно до специфічних вимог та обмежень.

The research is dedicated to the analysis and evaluation of the effectiveness of modern asymmetric cryptographic algorithms. The choice of a reliable cryptographic algorithm is critically important for ensuring the security of information systems, as it directly impacts the protection of confidential data.

The work examines three popular digital signature algorithms: RSA, DSA, and ECDSA. The theoretical analysis included studying the architecture of the algorithms and their key parameters. Experimental studies were conducted to evaluate the performance of the algorithms in terms of execution time, memory usage, and CPU load.

The obtained results and the developed approach can be useful for system administrators and developers to enhance the level of data protection in information systems.

The conclusions and recommendations presented in the work will contribute to improving the security of information systems by selecting the most effective asymmetric cryptographic algorithm according to specific requirements and constraints.