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

Авторська довідка

(реферату дипломної роботи магістра)

Назва дипломної роботи магістра: Дослідження методів безпечного гешування для забезпечення цілісності та автентичності інформації у автоматизованих банківських системах
назви записувати нижнім регістром (як у реченні)

Назва (англ.): Research of secure hashing methods to ensure the integrity and authenticity of information in automated banking systems
переклад англійською

Освітній ступінь : ***магістр***

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 національно технічний університет імені І. Пулюя**

напр.: Тернопільський національний технічний університет імені Івана Пулюя

Дата захисту: 23.12.2020 **Місто:** Тернопіль

Сторінки:
Кількість сторінок дипломної роботи: 82 Кількість сторінок реферату: 1

УДК: 004.021

Автор дипломної роботи
Прізвище, ім'я, по батькові (укр.): Очеретний Владислав Олегович
розкривати ініціали

Прізвище, ім'я (англ.): Ocheretnyi Vladyslav Olegovich
використовувати паспортну транслітерацію (КМУ 2010)

Місце навчання (установа, факультет, місто, країна): Тернопільський національний технічний університет ім. І.Пулюя., Факультет комп'ютерно-інформаційних систем та програмної інженерії, м. Тернопіль, Україна

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

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

Місце праці (установа, підрозділ, місто, країна): Тернопільський національний технічний університет ім. І. Пулюя, м. Тернопіль, Україна

Вчене звання, науковий ступінь, посада: доктор технічних наук, професор

Рецензент
Прізвище, ім'я, по батькові (укр.): Приймак Микола Володимирович
повністю

Прізвище, ім'я (англ.): Priymak Mykola Volodymyrovych
використовувати паспортну транслітерацію (КМУ 2010)

Місце праці (установа, підрозділ, місто, країна): Тернопільський національний технічний університет

ім. І. Пулюя, м. Тернопіль, Україна

Вчене звання, науковий ступінь, посада: доктор наук, професор

Ключові слова

українською: цілісність інформації, автентифікація повідомлення, електронний цифровий підпис, геш-функція, національна платіжна система

до 10 слів

англійською: information integrity, message authentication, electronic digital signature, hash function, national payment system

до 10 слів

Анотація

українською: Дана магістерська кваліфікаційна робота присвячена дослідженню механізмів забезпечення автентичності за допомогою геш-функцій на основі MAC та MDC-кодів. Об’єктом дослідження є процес забезпечення автентичності та цілісності банківської інформації.
Предметом дослідження є методи ключового гешування забезпечення автентичності та цілісності банківської інформації.
Метою роботи є моделювання ключового гешування забезпечення автентичності та цілісності банківської інформації.
При розробленні програмного продукту було використано програмне середовище NetBeans IDE 6.9.1 та мова програмування – Java.
Методами розробки обрано:
При аналізі побудови MAC- (MDC-) кодів використані методи теорії захисту інформації. При оцінці технічних характеристик MAC- (MDC-) кодів використані методи теорії ймовірності та математичної статистики.
У результаті роботи проведений аналіз механізмів забезпечення автентичності на основі MAC та MDC-кодів, обґрунтовані рекомендації щодо їх використання в організаціях банківського сектора.

200-300 слів

англійською: This master's thesis is devoted to the study of mechanisms for ensuring authenticity using hash functions based on MAC and MDC codes. The object of the research is the process of ensuring the authenticity and integrity of banking information. The subject of the research is the methods of key hashing to ensure the authenticity and integrity of banking information.
The aim of the work is to simulate key hashing to ensure the authenticity and integrity of banking information.
During the development of the software product, the NetBeans IDE 6.9.1 software environment and the programming language Java used.
The development methods selected:
When analyzing the construction of MAC- (MDC-) codes, the methods of information security theory used.
When evaluating the technical characteristics of MAC- (MDC-) codes, the methods of probability theory and mathematical statistics used. As a result of the work, an analysis of mechanisms for ensuring authenticity based on MAC and MDC codes was carried out, recommendations for their use in organizations of the banking sector were substantiated.

200-300 слів