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

# Авторська довідка

*(кваліфікаційної роботи бакалавра)*

**Назва кваліфікаційної роботи бакалавра** *Дослідження моделей і методів контролю цілісності й автентичності даних у телекомунікаційних мережах та їх колізійних властивостей*
*назви записувати нижнім регістром (як у реченні)*

**Назва (англ.):** *Study of Models and Methods of Control of Data Authenticity and Completeness in Telecommunication Networks and their Collision Characteristics*
*переклад англійською*

**Освітній ступінь :** бакалавр

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

**Екзаменаційна комісія**: Екзаменаційна комісія № 46
*напр.: Екзаменаційна комісія №1*

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

**Дата захисту:** 23 червня 2022 року **Місто:** Тернопіль

**Сторінки:**
Кількість сторінок роботи: 82

**УДК:** 004.056

**Автор роботи**
Прізвище, ім'я, по батькові (укр.): Гродський Богдан Павлович
розкривати ініціали

Прізвище, ім'я (англ.): Hrodskyi Bohdan
*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.): Максимчук Олександр Олександрович
повністю

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

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

Вчене звання, науковий ступінь, посада: асистент кафедри КБ

**Рецензент**
Прізвище, ім'я, по батькові (укр.): Матійчук Любомир Павлович
повністю

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

Місце праці (установа, підрозділ, місто, країна): ТНТУ ім. І. Пулюя, Факультет комп'ютерно-інформаційних систем і програмної інженерії, Кафедра комп'ютерних наук, м.Тернопіль, Україна
Вчене звання, науковий ступінь, посада: доктор філософії, к.е.н., доцент кафедри КН

**Ключові слова**
українською: захист інформації, протоколи мережної безпеки, геш-функція, UMAC, MASH-1, MASH-2, гешування, цілісність, автентичність, NESSIE
*до 10 слів*

англійською: INFORMATION security protocols, network security, hash functions, UMAC, MASH-1, MASH-2, hashing, integrity, authenticity, NESSIE
*до 10 слів*

**Анотація**

українською:

Мета роботи полягає у в аналізі механізмів забезпечення автентичності і цілісності інформації у телекомунікаційних мережах, оцінці їх основних ймовірно-часових характеристик, програмної реалізації нових методів формування МАС-кодів на основі використання модулярних перетворень. В результаті виконання роботи отримані наступні результати:

- проведено аналіз стану та обґрунтування шляхів удосконалювання моделей і методів контролю цілісності та автентичності даних, алгоритмів ключового й безключового гешування для формування кодів виявлення маніпуляцій (MDC) і кодів автентифікації повідомлень (MAC);
- реалізовано математичний апарат і здійснено дослідження колізійних властивостей кодів контролювання цілісностей та аутентичності даних, обґрунтовано пропозиції з їх удосконалювання;
- реалізовано модель і метод формування кодів контролю цілісності та автентичності даних на основі доведено стійкого ключового гешування;
- досліджено ефективність запропонованих моделей і методів контролю цілісності та автентичності даних, обґрунтовано практичні рекомендації з їх використання в протоколах безпеки комунікаційних мереж.

англійською:

Purpose is to analyze the mechanisms to ensure the authenticity and integrity of information in telecommunication networks, assessing their likely-time major characteristics of program implementation of new methods of generating the MAC code through the use of modular transformations.

As a result of the implementation of the following results:

- conducted analysis and study ways to improve models and methods for monitoring the integrity and authenticity of data, algorithms and key keyless hash codes to identify the formation of manipulation (MDC) authentication messages and codes (MAC);
- implemented mathematical tools and the research of conflicting properties codes control the integrity and authenticity of data substantiated proposals for their improvement;
- implemented model and method of forming the control codes of integrity and authenticity of data based on proven resistant hash key;
- investigated the effectiveness of the proposed models and methods of monitoring the integrity and authenticity of data, practical recommendations on their use in security protocol telecommunication networks.

Бібліографічний опис:

Гродський Б. П. Дослідження моделей і методів контролю цілісності й автентичності даних у телекомунікаційних мережах та їх колізійних властивостей: кваліфікаційна робота бакалавра за спеціальністю 125 — Кібербезпека / Гродський Богдан Павлович. – Тернопіль : ТНТУ, 2022. – 82 с.

Hrodskyi B. Study of Models and Methods of Control of Data Authenticity and Completeness in Telecommunication Networks and their Collision Characteristics: Bachelor thesis 125 — Cybersecurity / Hrodskyi Bohdan - Ternopil, TNTU, 2022 – 82 p.