РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ОТРИМАННЯ ТА ВИКОРИСТАННЯ ХЕШ-ФУНКЦІЇ ДЖЕНКІНСА

канд. техн. наук, проф. О.М. Рисований, студ. Р.Д. Сухой, студ. М.А. Чекун, Національний технічний університет "Харківський політехнічний інститут", м. Харків

Хешування інформації є важливим заходом для забезпечення безпеки та конфіденційності в цифровому середовищі [1 – 3]. Хешування залишається актуальним завдяки широкому спектру застосувань у безпеці, зберіганні даних, пошукових алгоритмах та блокчейн-технологіях. З розвитком кіберзагроз та збільшенням обсягів даних значимість ефективних хеш-функцій лише зростає.

Розрізняють два великі класи отримання хеш-функцій:

- хеш-функції, засновані на розподілі;
- хеш-функції, засновані на доборі значень.

Алгоритм отримання хеш-функції Дженкинса складається з послідовних операцій зсуву в різні сторони на різне число розрядів та виконання операцій суми та суми за модулем 2. Ці операції отримані в результаті багаторазової зміни даних та аналізу отриманих результатів щодо швидкості виконання і лавинного процесу.

Практична цінність отриманих в роботі результатів полягає в тому, що в рамках роботи розроблена програма хешування за алгоритмом Дженкінса, яка виконана на низькорівневій мові, що сприяє швидкості обробки даних.

Список літератури: **1**. Рисований О.М., Ігнатьєв К.І., Рибалка Р.В., Рудаковський Д.Р. Механізм шифрування повідомлень з максимальною довжиною // Інформатика, управління та штучний інтелект. Тези одинадцятої міжнародної науково-технічної конференції. – Харків: НТУ "ХПІ", 2024. – 176 с. – С.127. **2.** Рисований О.М., Ігнатьєв К.І., Рибалка Р.В., Рудаковський Д.Р. Вибір багаточленів з максимальним періодом генерації станів // Інформаційні технології: наука, техніка, технологія, освіта, здоров'я: тези доповідей XXXII міжнародної науково-практичної конференції MicroCAD-2024, 22-25 травня 2024 р. / за ред. проф. Сокола Є.І. – Харків: НТУ "ХПІ". – С. 1421. **3.** Рисований О.М. Криптостійкий генератор псевдовипадкової наслідності з використанням майстер-ключа // Проблеми інформатики та моделювання (ПІМ-2024). Тези двадцять четвертої міжнародної науково-технічної конференції. – Харків: НТУ "ХПІ", 2024. – С.120.