Магістерська кваліфікаційна робота

на тему:

«Інформаційна технологія гешування цифрових даних на основі лічильника»

Виконав: магістрант групи 1КН-17м
Смішко Віталій

Керівник: к.т.н., доц.
Крилик Л. В.

МЕТА ТА ЗАВДАННЯ ДОСЛІДЖЕННЯ

Актуальність

Історично криптоалгоритми розроблялися для імплементації в інформаційних системах, побудованих на високопродуктивних мікропроцесорах загального призначення. Як результат, існуючі криптоалгоритми доволі погано пристосовані до застосування у вбудованих системах, переважна більшість з яких ґрунтується на 8/16/32-бітових процесорах з малими обчислювальними ресурсами. Операції шифрування і гешування за традиційної програмної реалізації на МК загального призначення є доволі повільними і потребують значних витрат постійної і оперативної пам'яті. Відповідно пошук нових алгоритмів та способів реалізації, які б добре працювали на цих платформах, є важливим і актуальним завданням, з яким пов'язаний такий напрямок, як малоресурсна криптографія .

Метою дослідження магістерської кваліфікаційної роботи є підвищення швидкодії та зменшення використання ресурсів комп'ютера програмними засобами гешування цифрових даних за рахунок використання нових математичних моделей геш-функцій.

Для досягнення поставленої мети необхідно розв'язати такі завдання:

- провести аналіз проблеми розв'язання задачі гешування цифрових даних;
- розглянути існуючі методи вирішення задачі гешування цифрових даних та обрати й обґрунтувати вибір методу, який задовольняє мету даної магістерської кваліфікаційної роботи;
- розробити метод та математичну модель гешування цифрових даних;
- сформулювати стадії інформаційної технології, розробити структуру та алгоритм роботи програмного засобу;
- виконати програмну реалізацію запропонованої інформаційної технології гешування цифрових даних;
- провести тестування програмного продукту та виконати аналіз отриманих результатів.

ОБ’ЄКТ, ПРЕДМЕТ ТА МЕТОДИ ДОСЛІДЖЕННЯ

Об’єкт дослідження – процес гешування цифрових даних на основі використання лічильника.

Предмет дослідження – інформаційна технологія та програмні засоби гешування цифрових даних на основі використання лічильника та швидкодія гешування цифрових даних.

Методи дослідження

У роботі використані наступні методи наукових досліджень:

-- системного аналізу,
-- теорії інформації та кодування,
-- теорії захисту інформації,
-- криптографії,
-- теорії побудови цифрових схем,
-- теорії ймовірності та математичної статистики,
-- об’єктно-орієнтованого програмування.

НАУКОВА НОВИЗНА ОДЕРЖАНИХ РЕЗУЛЬТАТІВ

полягає в наступному:

1. Набула подальшого розвитку інформаційна технологія гешування цифрових даних, яка відрізняється визначенням геш-функції за методом на основі лічильника, що дозволило підвищити швидкодію процесу гешування.
2. Удосконалено метод та математичну модель визначення геш-функції, яка відрізняється використанням простих операцій та лічильника, що забезпечило пришвидшення процесу гешування та зменшення апаратних ресурсів на релізацію спеціалізованого процесора гешування..

ПРАКТИЧНЕ ЗНАЧЕННЯ ОДЕРЖАНИХ РЕЗУЛЬТАТІВ

- розроблено вимоги до геш-функцій;
- розроблено алгоритм програмної реалізації інформаційної технології гешування;
- розроблено програмні засоби для гешування цифрових даних на основі лічильника;

Аналіз предметної області гешування цифрових даних

Гешування – перетворення вхідного масиву даних довільної довжини в вихідну бітову послідовність фіксованої довжини, яку можна використати для порівняння даних

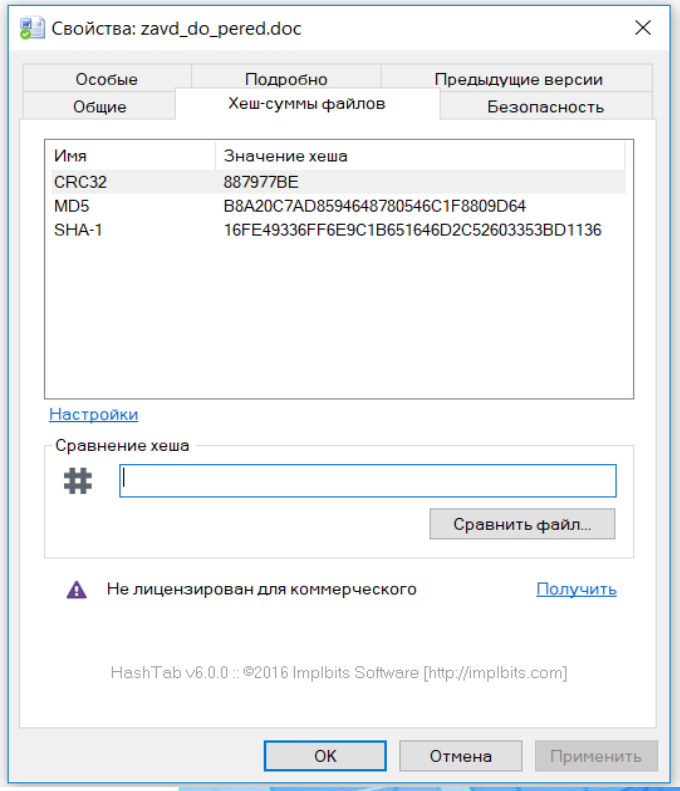
Стандартні підходи до вирішення проблеми створення ефективних методів і засобів малоресурсної криптографії :
1) використання класичних криптографічних алгоритмів;
2) модифікація класичних алгоритмів з адаптацією до апаратних особливостей і обмеженням систем з низькою вартістю;
3) розробка нових спеціалізованих рішень в методологічному, алгоритмічному і програмно-апаратному плані .

Було обрано 3)

У малоресурсній криптографії в основному використовуються алгоритми:
1) блочні, 2) потокові

Вибір і обґрунтування аналогу

Аналог - програма HashTab



Відомі геш-функції

- Skein.
- Алгоритм MD5
- Grøstl
- Keccak

Вимоги до геш-функцій

При практичному використанні геш-функцій мають виконуватися такі вимоги :

- Алгоритм повинен володіти високою швидкістю обробки інформації;
- Геш-функція повинна бути стійкою проти атаки методом «грубої сили»;
- Програмна реалізація геш-функції повинна бути оптимізована під використання на сучасній апаратно-програмній базі.

Властивості криптографічних геш-функцій

- ✓ Функція повинна бути застосовною до блоку даних будь-якої довжини.
- ✓ Функція повинна давати на виході значення фіксованої довжини.
- ✓ Значення H(x) повинне обчислюватися відносно легко для будь-якого заданого x.
- ✓ Для будь-якого даного коду h повинно бути практично неможливо обчислити x, для якого H(x) = h. Таку властивість іноді називають односторонністю.
- ✓ Для будь-якого даного блоку x повинно бути практично неможливо обчислити y, для якого H(x) = H(y). Таку властивість іноді називають слабкою опірністю колізіям.
- ✓ Повинно бути практично неможливо обчислити будь-яку пару різних значень x і y, для яких H(x) = H(y). Таку властивість іноді називають сильною опірністю колізіям

Математична модель геш–функції

- Вхідне повідомлення M розглядається як послідовність байтів $M=\{ m_1, m_2, \ldots, m_L\}$.
- Геш-значення формується з ASCII–кодів байтів з урахуванням номерів позицій.

Номер позиції q байта у повідомленні розглядається як двійковий код:

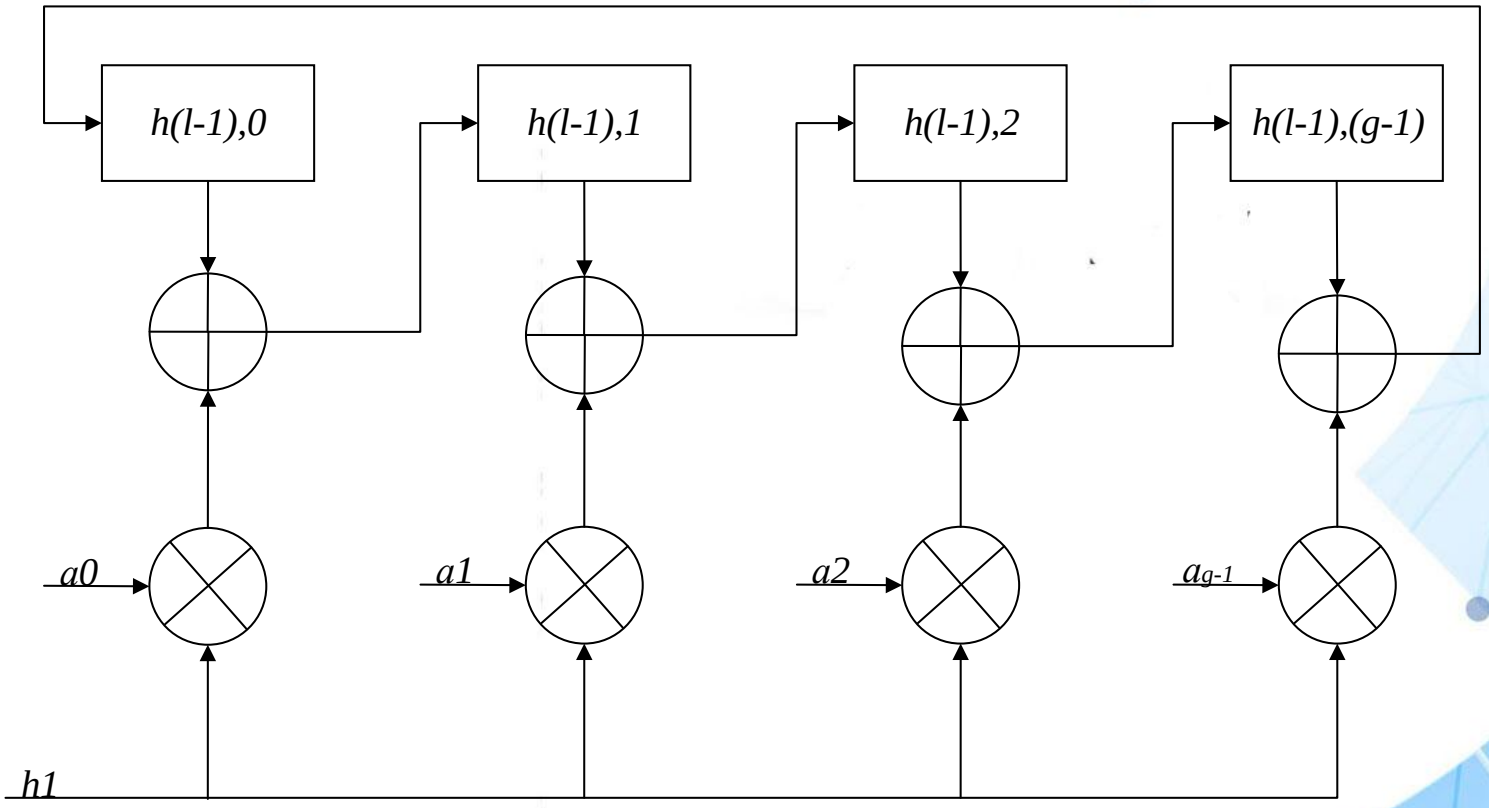
$$q = \sum_{i=0}^{g-1} a_i \cdot 2^i$$

Проміжні хеш-значення $h_l = \{h_{l,0}, h_{l,1}, \ldots, h_{l,(g-1)}\}$ обчислюється на основі попереднього хеш-значення, двійкового представлення номера позиції q та ASCII–кода байта :

$$h_{l,j} = h_{(l-1),(j-1)} \oplus (n_l \cdot a_{j-1}),$$

$$h_{l,0} = h_{l,(g-1)} \oplus (n_l \cdot a_{g-1}),$$

Схема обчислень геш–значень

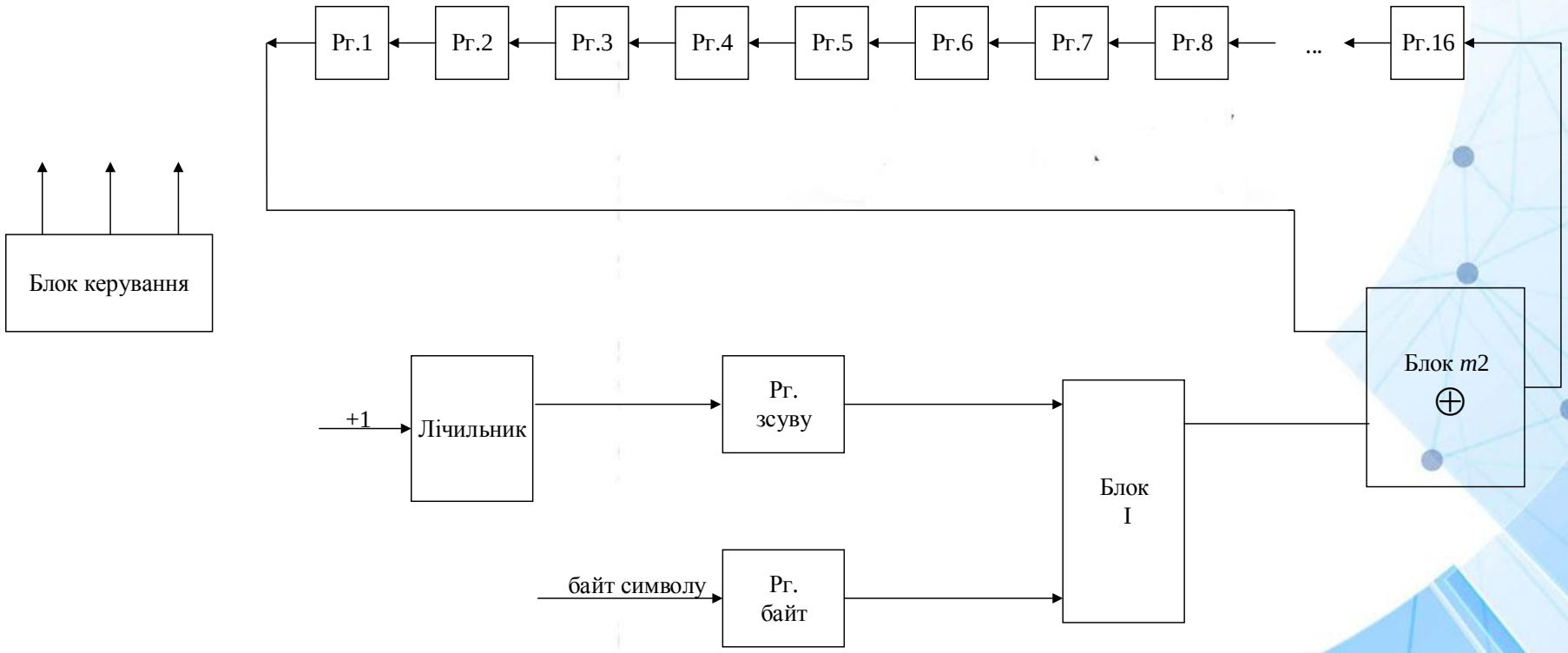


Структура інформаційної технології гешування цифрових даних на основі лічильника

Алгоритм гешування

L- вхідне повідомлення;
h1 – проміжне геш-значення;
l, *g* – лічильник;
q – номер байта

Структура спеціалізованого процесора для гешування



Оцінка складності процесора

Складність реалізації різних логічних елементів для технології 0.18нм

Елемент	GE
І	1,33
Додавання за модулем 2	4,67
Тригер	5,33

В одному регістрі 8 тригерів, значить складність усіх 16 регістрів становить: $8 \cdot 16 \cdot 5{,}33 \approx 682\,GE$

В пристрої вісім суматорів за модулем 2, складність яких дорівнює: $8 \cdot 4{,}67 \approx 37\,GE$

Блок І теж восьмирозрядний, тому його складність: $8 \cdot 1{,}33 \approx 11\,GE$

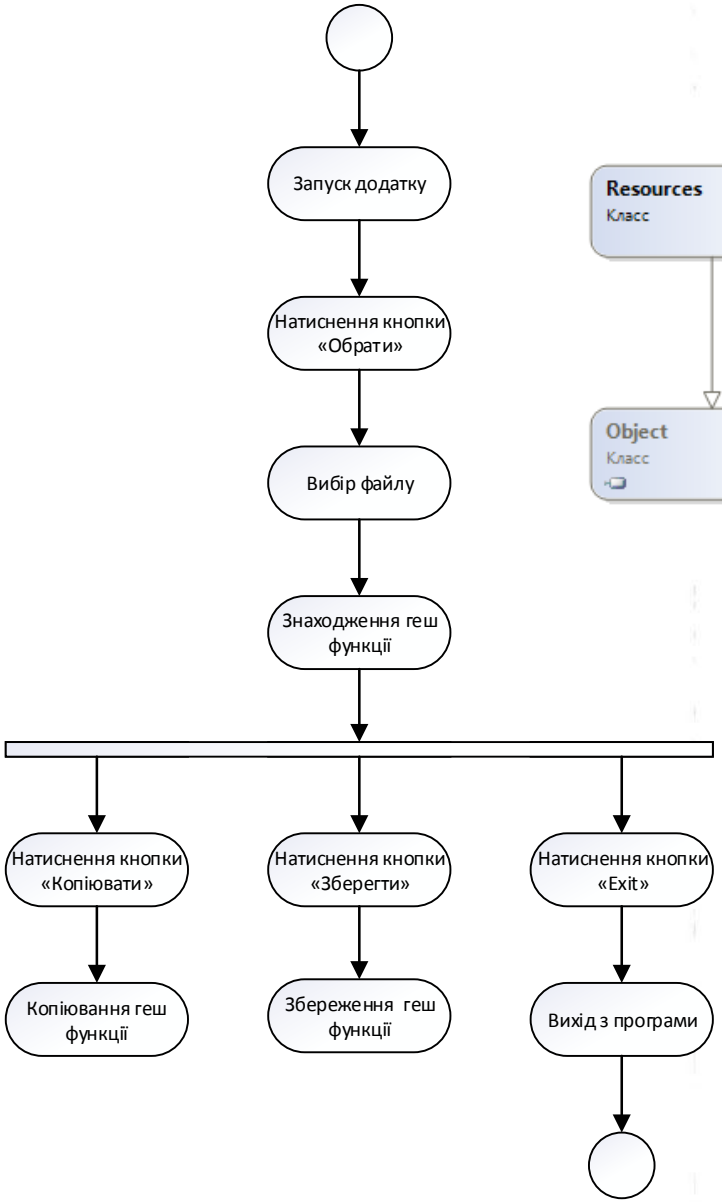
Шістнадцятирозрядний регістр зсуву має складність: $16 \cdot 5{,}33 \approx 85\,GE$

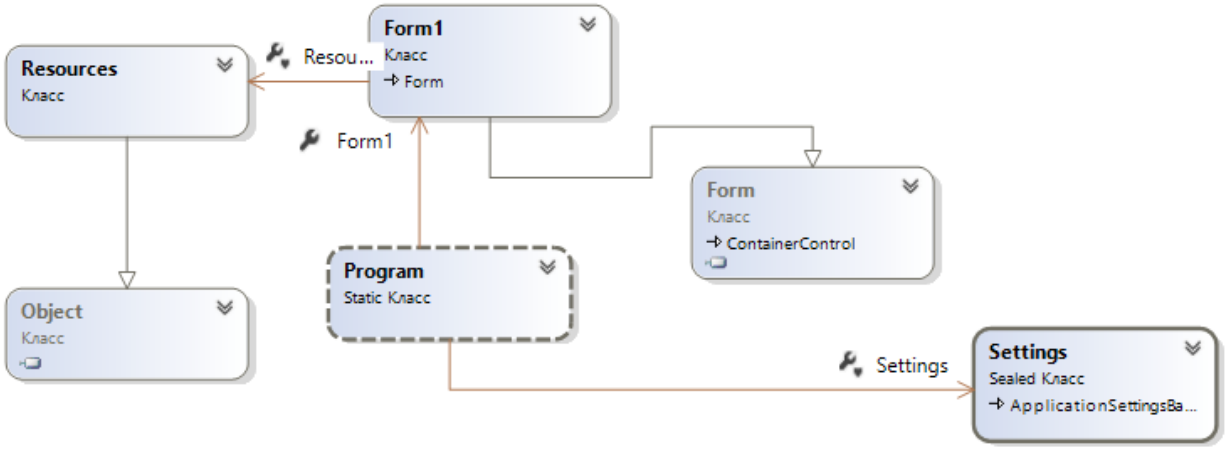
Складність восьмирозрядного регістру зсуву дорівнює: $8 \cdot 5{,}33 \approx 43\,GE$

Шістнадцятирозрядний лічильник має складність: $16 \cdot 5{,}33 \approx 85\,GE$

Отже, складність пристрою в цілому дорівнює: $682+37+11+85+43+85=943\,GE$

Діаграма діяльності програми гешування цифрових даних



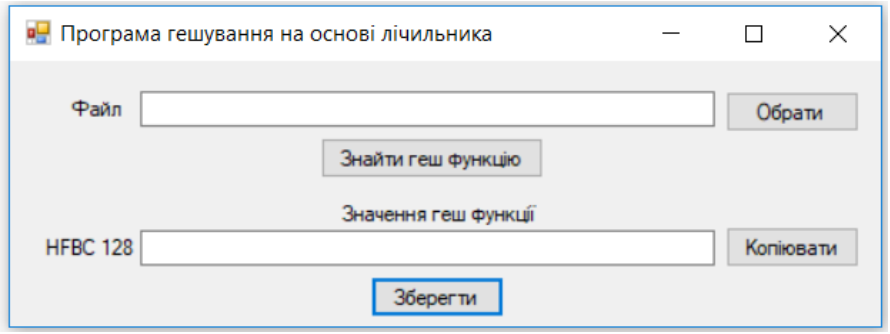


Діаграма класів програми гешування цифрових даних

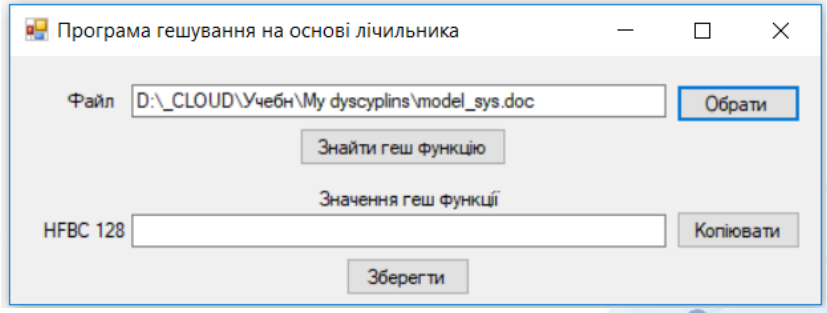
Програму написано мовою програмування C# під операційну систему Windows

Робочі вікна програми гешування

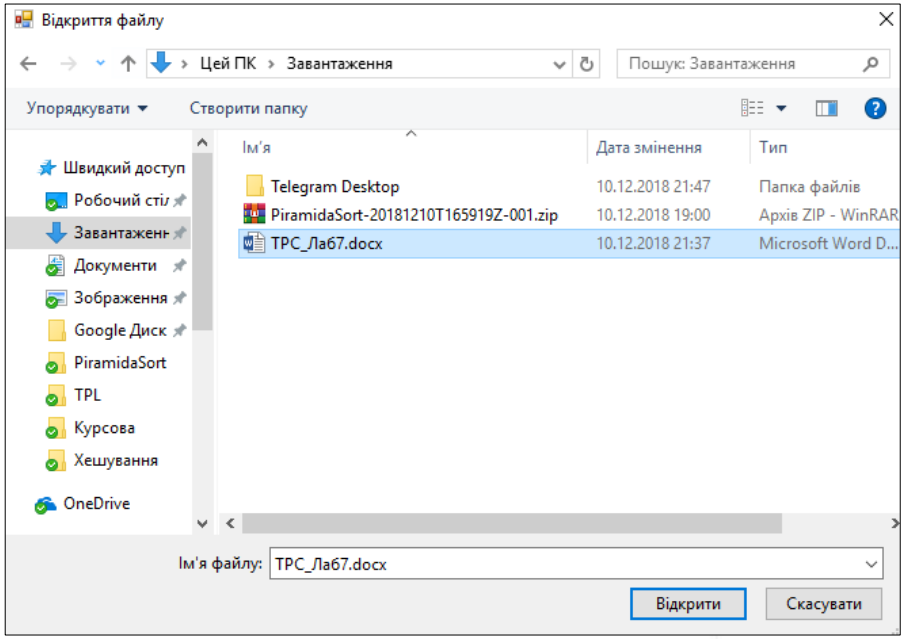
Стартове вікно програми гешування цифрових даних



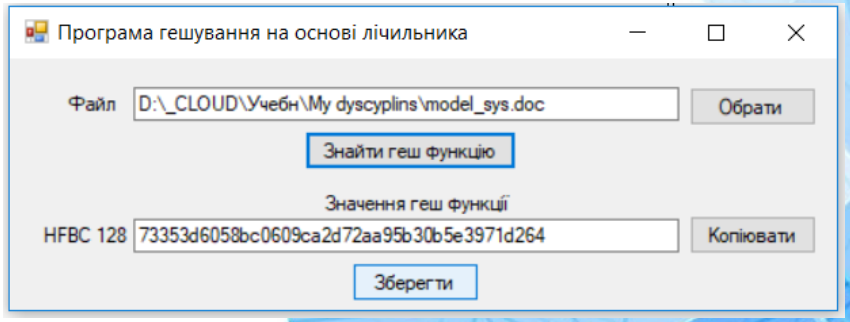
Вид вікна після вибору файлу для гешування



Вікно вибору файлу для гешування



Знайдене значення геш-функції



Результати гешування файлів розробленою програмою та програмою-аналогом

Розмір файла	Час отримання хеш-коду файла		Коефіцієнт збільшення швидкодії
	Програма-аналог HashTab	Розроблена програма	
3.31 Гбайт	33.3 сек	27,3 сек	1,22
350,6 Мбайт	3,52 сек	2,84 сек	1,24
1,015 Мбайт	95 мсек	72 мсек	1,32
Середнє значення			1,26

Із табл. видно, що розроблене програмне забезпечення має більшу швидкодію (у середньому в 1,26 раз, тобто на 26%), ніж аналогічна програма HashTab, а значить мета роботи досягнута.

ЕКОНОМІЧНА ЧАСТИНА

Було проведено економічне обґрунтування доцільності розробки програмного засобу гешування цифрових даних на основі лічильника. Комерційний потенціал розробки за результатами експертного оцінювання - вище середнього. Відносний рівень якості інноваційної розробки на 9% краще базового товару-конкурента. Прогнозована загальна сума витрат на виконання розробки - 17386,27 грн. Прогнозовані загальні витрати на виконання та впровадження результатів наукової роботи - 25568,05 грн. Абсолютна ефективність вкладених інвестицій становить 289901,39 грн, і це свідчить про те, що вкладання коштів на виконання та впровадження результатів НДДКР є доцільним. Відносна (щорічна) ефективність вкладених в наукову розробку інвестицій – 131 %, отже інвестор буде зацікавлений у фінансуванні даної наукової розробки. Термін окупності складає 0,76 року, тобто фінансування розробки програмного засобу гешування цифрових даних на основі лічильника є економічно доцільним проектом.

АПРОБАЦІЯ РЕЗУЛЬТАТІВ РОБОТИ ТА ПУБЛІКАЦІЇ

Апробація результатів роботи.

Результати досліджень апробовані на конференції «Молодь в науці: дослідження, проблеми, перспективи-2019», Вінниця, 2019 https://conferences.vntu.edu.ua/index.php/mn/index/pages/view/zbirn2019

Публікації.

За результатами магістерської кваліфікаційної роботи опубліковано 1 тези доповідей на конференції та свідоцтво про реєстрацію авторського права на твір (Комп'ютерну програму).

ВИСНОВОК

В результаті виконання роботи було розроблено інформаційну технологію гешування цифрових даних на основі лічильника. Програмну реалізацію технології здійснено об’єктно-орієнтованою мовою програмування C# під операційну систему Windows. Розроблене програмне забезпечення має більшу швидкодію (у середньому в 1,26 раз, тобто на 26%), ніж аналогічна програма HashTab, а значить мета роботи досягнута.

ДЯКУЮ ЗА УВАГУ!