Магістерська кваліфікаційна робота на тему:

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ЗАХИСТУ АУДІОІНФОРМАЦІЇ

Студент гр. 1КН-16 м ***І.В.Колодій***

Керівник к.т.н., доц. ***О.К. Колесницький***

МЕТА ТА ЗАВДАННЯ ДОСЛІДЖЕННЯ

Метою дослідження є підвищення швидкості шифрування аудіоінформації, поданої як у вигляді WAV-файлів, так і звуку з мікрофона, під'єднаного до комп'ютера.

Для досягнення поставленої мети необхідно розв'язати такі завдання:

- здійснити аналіз методів і алгоритмів захисту аудіоінформації;
- здійснити розробку методу розв'язання задачі захисту аудіоінформаці;
- здійснити розробку інформаційної технології шифрування аудіоінформації;
- здійснити розробку нейромережевого методу генерування масиву випадкових чисел;
- здійснити проектування програмних засобів захисту аудіоінформації;
- обґрунтувати вибір програмного інструментарію для реалізації інформаційної технології захисту аудіоінформації;
- здійснити програмну реалізацію та тестування програмних засобів захисту аудіоінформації.

ОБ’ЄКТ, ПРЕДМЕТ ТА МЕТОДИ ДОСЛІДЖЕННЯ

Об’єкт дослідження – процес захисту аудіоінформації у комп`ютерних системах.

Предмет дослідження – методи та програмні засоби захисту аудіоінформації, швидкість шифрування аудіоінформації у WAV-форматі та аудіосигналів безпосередньо з мікрофону.

Методи дослідження

У роботі використані наступні методи наукових досліджень:
-- системного аналізу,
-- криптографії для реалізації інформаційної технології захисту аудіоінформації ,
-- теорії штучних нейронних мереж,
-- методи математичної статистики для розробки процесу захисту та обрахунків результатів експериментів із програмним засобом,
-- об’єктно-орієнтованого програмування.

НАУКОВА НОВИЗНА ОДЕРЖАНИХ РЕЗУЛЬТАТІВ

полягає в наступному:

1. Удосконалено цифровий криптографічний метод захисту інформації, а саме - метод однократного гамування, який відрізняється від відомих правилом формування гами із файлу великого змінного розміру, що забезпечило підвищення швидкості шифрування аудіоінформації.
2. Удосконалено метод генерації псевдовипадкових чисел, який відрізняється від відомих застосуванням нейронної мережі, що забезпечило підвищення ступеня випадковості.

.

ПРАКТИЧНЕ ЗНАЧЕННЯ ОДЕРЖАНИХ РЕЗУЛЬТАТІВ

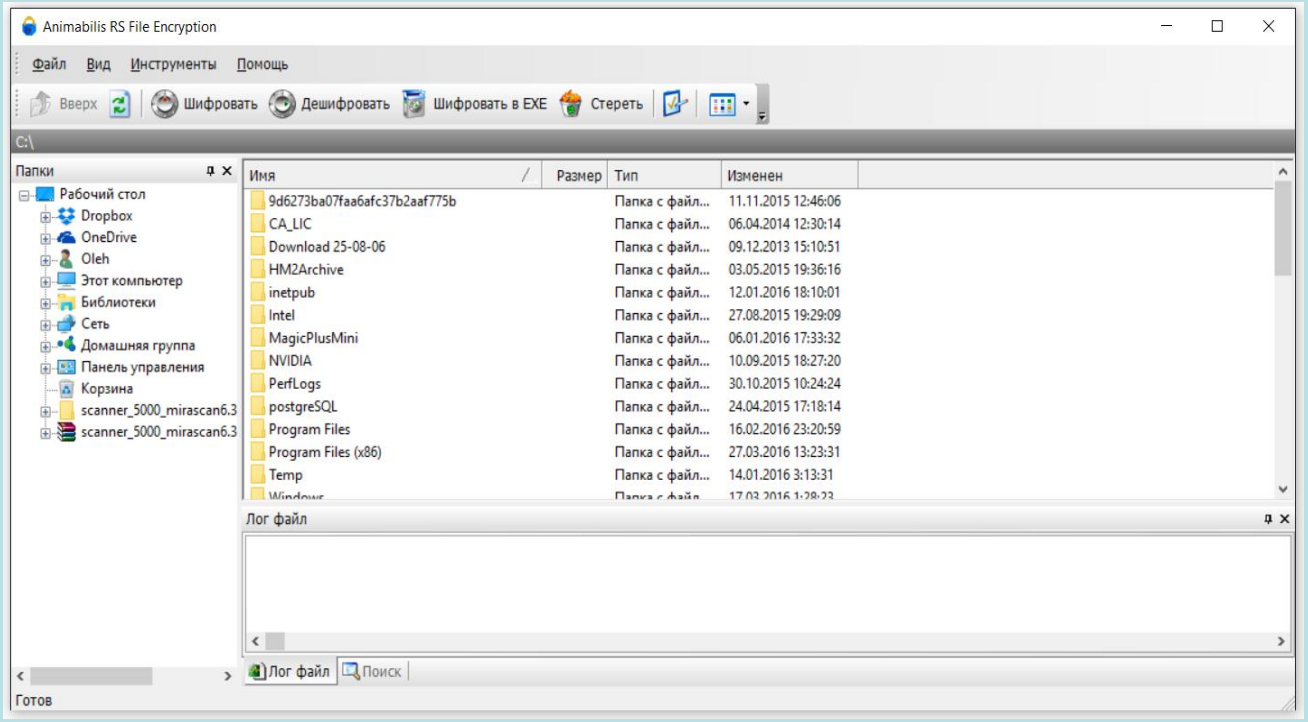
- розроблено алгоритм генерування масиву випадкових чисел на основі штучної нейронної мережі;
- розроблено алгоритм роботи програмного забезпечення захисту аудіоінформації;
- розроблено програмні засоби для захисту аудіоінформації на основі штучної нейронної мережі;

;

Актуальність

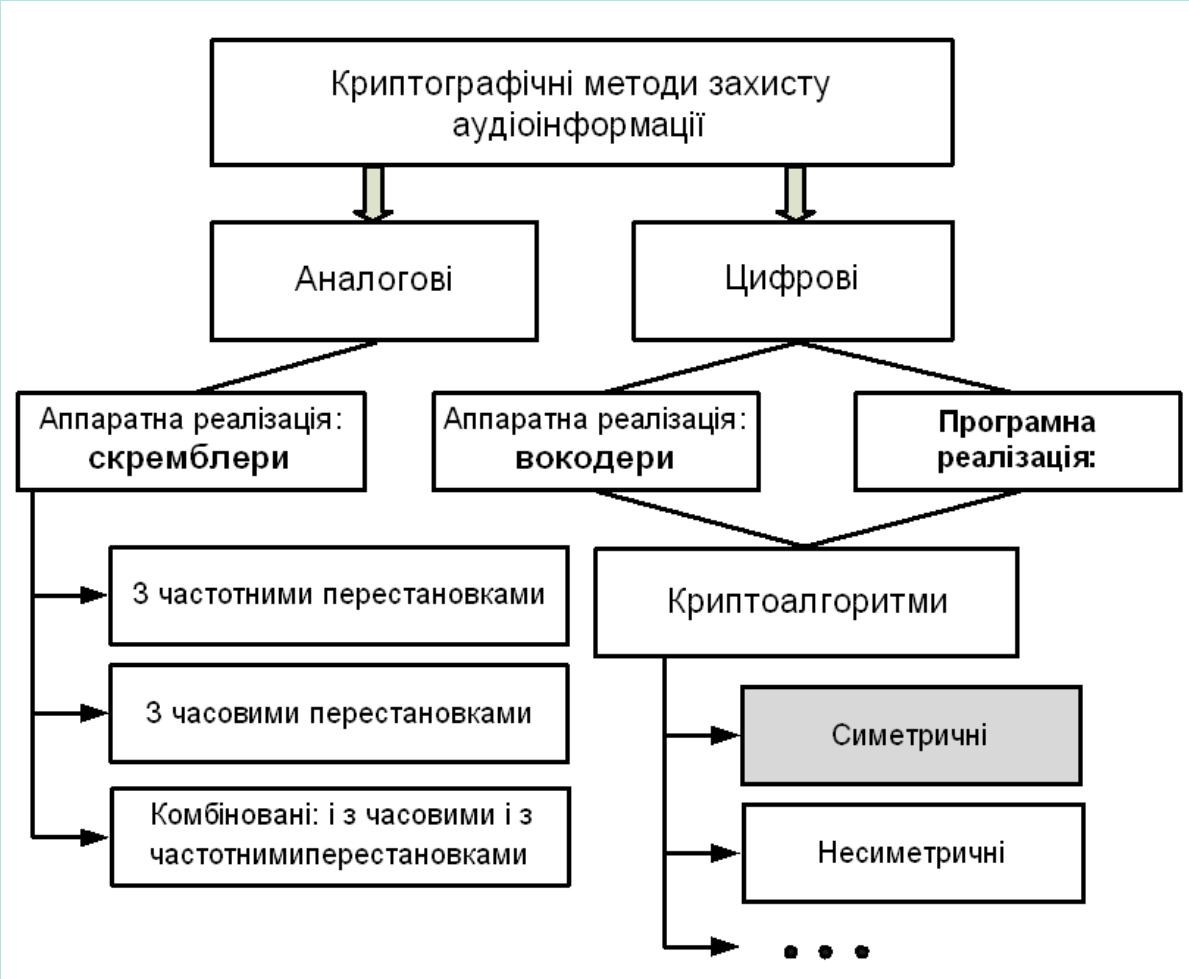
У сучасному суспільстві головним ресурсом стає інформація. Інформаційна безпека займає особливе місце у зв'язку зі зростаючим впливом інформації на економіку та життя суспільства.

Тема роботи є актуальною в зв’язку з необхідністю впровадження нових інформаційних технологій захисту інформації.



Як **АНАЛОГ** було обрано програму “Animabilis RS File Encryption 1.3”, яка забезпечують шифрування файлів, що зберігаються на змінних носіях чи підлягають передачі через інтернет.

АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ



Було проаналізовано можливі методи та засоби захисту аудіоінформації та виявлено, що найбільш ефективним є використання криптографічних методів шифрування, причому найбільші переваги мають цифрові методи

Види перетворень в симетричних криптосистемах

Було проаналізовано відомі види перетворень в симетричних криптосистемах і обрано для реалізації метод однократного гамування, який був дещо модифікований з метою підвищення криптостійкості

Порівняння алгоритмів захисту інформації

Алгоритми шифрування інформації	Характеристики	
	Ключ	Використання масиву випадкових чисел
DES	56 біт	-
AES	128,192,256 біт	-
ГОСТ 28147-89	256 біт	-
TEA	128 біт	-
Запропонований варіант	128 біт	+

Інформаційна технологія захисту аудіоінформації

- Зчитування чергового відліку звукового файлу з мікрофона зі стандартного звукового файлу у WAV-форматі. Відлік являє собою двійкову цифру (код) довжиною в 1 байт (8 бітів).
- Над цим відліком і псевдовипадковим двійковим числом довжиною 8 бітів, яке вибране із масиву псевдовипадкових чисел, виконується операція XOR. Правило вибору псевдовипадкових чисел з масиву задається паролем. Для визначеності будемо вважати, що пароль має довжину 16 символів (=16 байтів =128 бітів). Структуру паролю показано в табл. 2.2. Перше псевдовипадкове число має в масиві позицію, яке визначається другим полем пароля, воно дорівнює 20 біт. Друге псевдовипадкове число має в масиві позицію, яке визначається третім полем пароля, воно дорівнює 20 бітів. Третє псевдовипадкове число має в масиві позицію, яке визначається четвертим полем пароля, воно дорівнює 20 біт. Четверте псевдовипадкове число має в масиві позицію, яке визначається п'ятим полем пароля, воно дорівнює 20 біт. П'яте псевдовипадкове число має в масиві позицію, яке визначається шостим полем пароля, воно дорівнює 20 біт. Шосте псевдовипадкове число має в масиві позицію, яке визначається сьомим полем пароля, воно дорівнює 20 біт. Наступне псевдовипадкове число береться з кроком, яке визначається першим полем пароля, воно дорівнює 8 біт (табл. 2.2).
- Отримане число (8-бітне двійкове) записується у файл.
- На приймальній стороні (або при дешифруванні файлу) знову виконується операція XOR над цим числом і псевдовипадковим числом, яке точно співпадає з тим, що брали при шифруванні звукового відліку, оскільки на приймальній стороні є такий самий масив псевдовипадкових чисел і кореспондент знає секретний пароль.
- Оскільки операція XOR є взаємо-зворотною, то ми отримуємо двійковий код, який і є відліком декодованого звуку, який подається для відтворення на динамік чи записується у декодований файл.

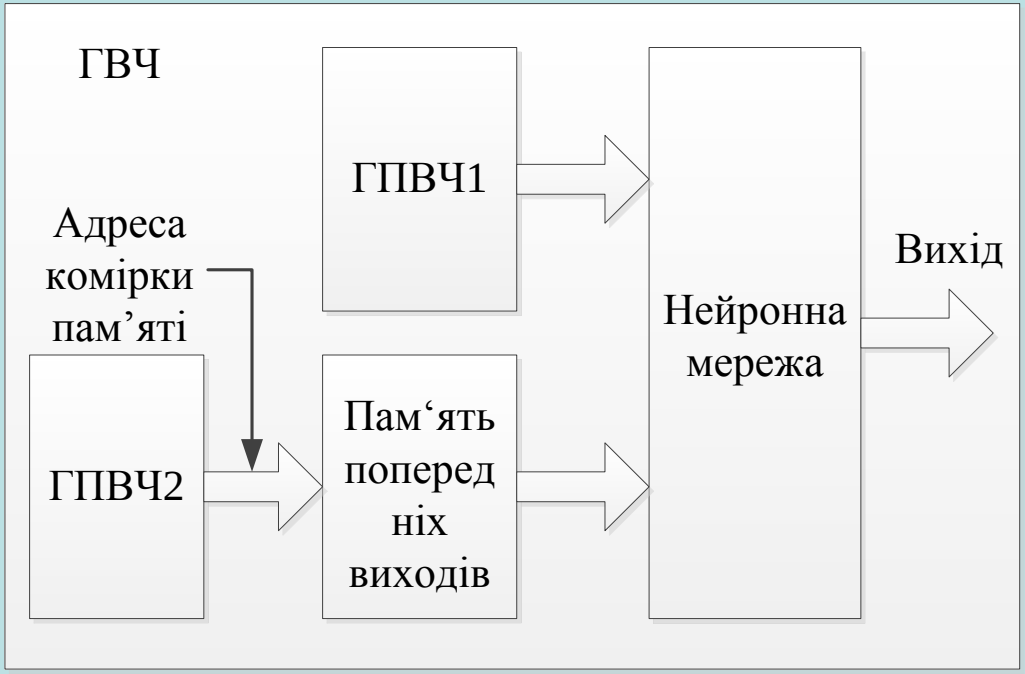
Масив псевдовипадкових чисел має бути сформований перед початком використання програми за допомогою генератора псевдовипадкових чисел.

Пароль, який вводиться користувачем, є фіксованим, його довжина складає 16 символів. Це зроблено для зменшення ступеня ризику при кодуванні/декодуванні звукового файлу, та для безвідмовної роботи програми.

Таблиця 2.2 - Структура паролю

8 біт	20 біт	20 біт	20 біт	20 біт	20 біт	20 біт
1 поле	2 поле	3 поле	4 поле	5 поле	6 поле	7 поле

Структура генератора випадкових чисел на основі нейронної мережі

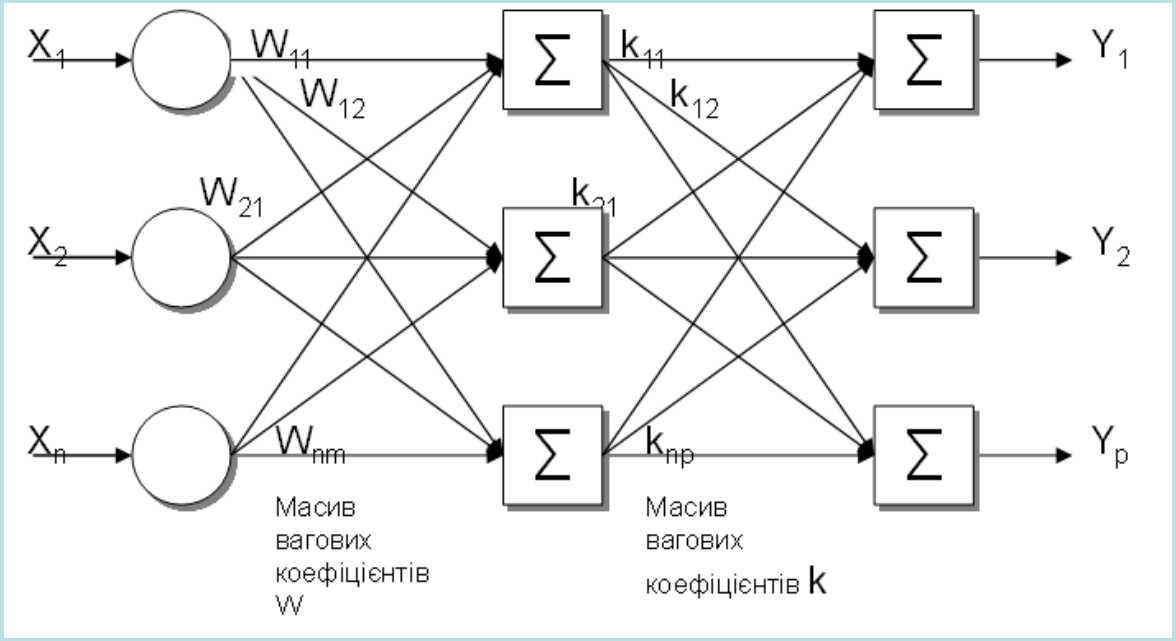


Ніякий детермінований алгоритм не може генерувати повністю випадкові числа, він може тільки апроксимувати деякі їх властивості.

Перед початком використання ГВЧ нейронну мережу навчають видавати послідовність випадкових чисел на основі словника випадкових чисел («одноразового блокноту»). Періоди зациклювання ГПВЧ1 та ГПВЧ2 мають бути неоднакові і відрізнятись на невелике значення

ГПВЧ1 генерує псевдовипадкове число, яке разом з числом із комірки пам'яті попередніх значень НМ викликає появу вихідного випадкового числа. Останнє записується в пам'ять попередніх значень НМ, витісняючи з нього значення, адреса якого задається ГПВЧ2. На наступному кроці вихідне випадкове число формується нейронною мережею на основі нового значення ГПВЧ1 та числа із пам'яті попередніх значень НМ за адресою наступного значення ГПВЧ2.

Структура та математична модель багатошарового персептрона



$$NET_{jl} = \sum_i w_{ijl} x_{ijl}$$

$$OUT_{jl} = F\left(NET_{jl} - \theta_{jl}\right)$$

$$x_{ij(l+1)} = OUT_{il}$$

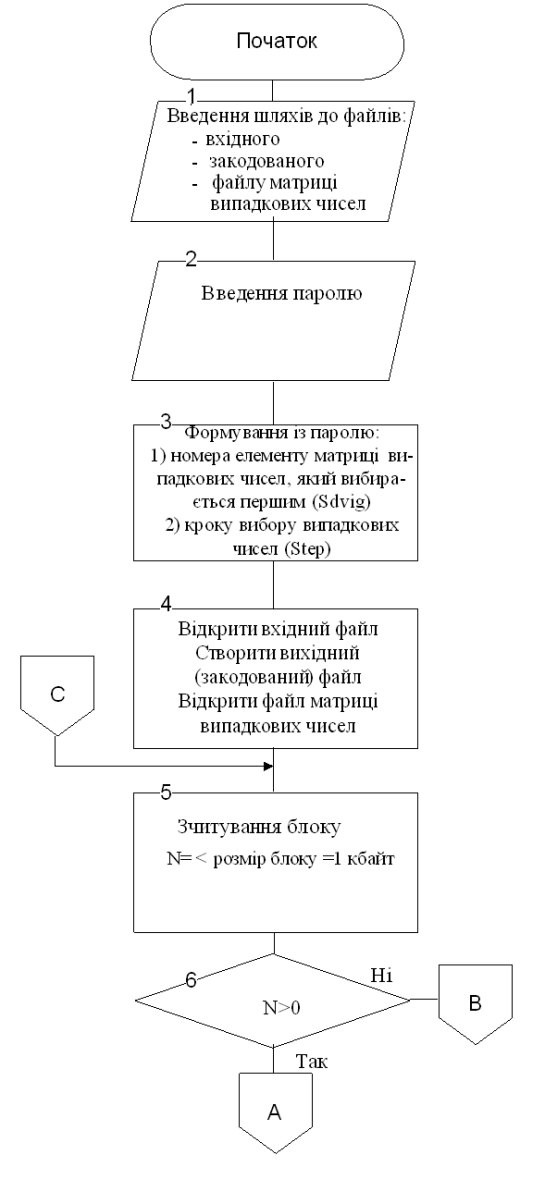
$$OUT = \begin{cases} 0, & NET \le \theta \\ \dfrac{(NET - \theta)}{\Delta}, & \theta \le NET < \theta + \Delta \\ 1, & NET \ge \theta + \Delta \end{cases}$$

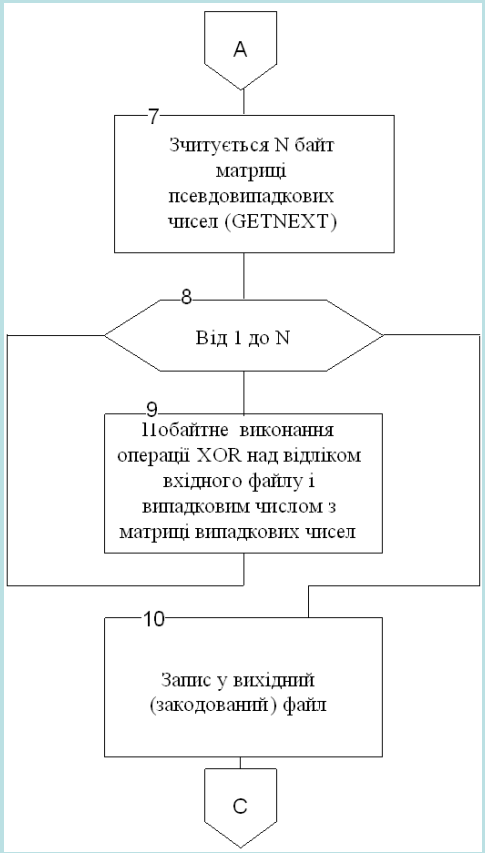
$$f(x) = F\left(\underbrace{\sum_{i_N} w_{i_N j_N N} \cdots \underbrace{\sum_{i_2} w_{i_2 j_2 2} \underbrace{F\left(\underbrace{\sum_{i_1} w_{i_1 j_1 1} x_{i_1 j_1 1} - \theta_{j_1 1}}_{\text{слой } 1}\right)}_{\text{слой } 2} - \theta_{j_2 2} \cdots - \theta_{j_N N}}_{\text{слой } N}\right)$$

$$E = \frac{1}{2} \sum_j \sum_s \left(y_j^s - d_j^s\right)^2$$

$$\begin{cases} \Delta w_{ij} = \varepsilon \left(d_j^s - y_j^s\right) x_{ij} \\ \Delta \theta_j = -\varepsilon \left(d_j^s - y_j^s\right) \end{cases}$$

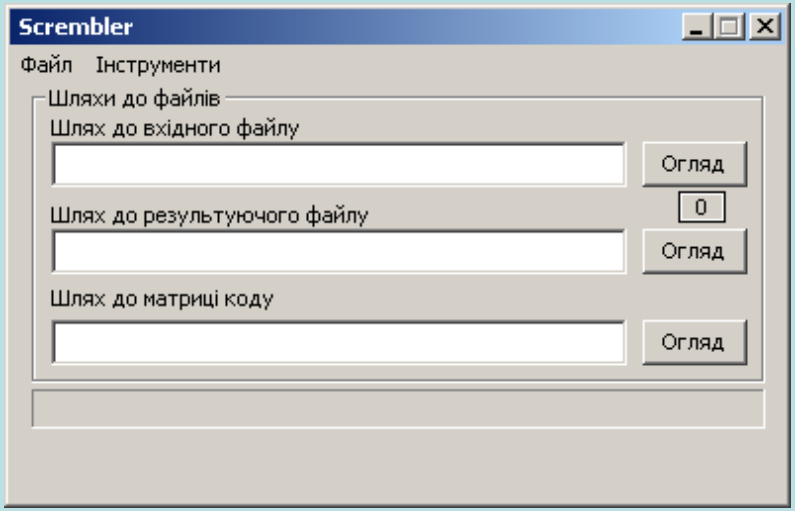
СХЕМА АЛГОРИТМУ РОБОТИ ПРОГРАМИ ЗАХИСТУ АУДІОІНФОРМАЦІЇ



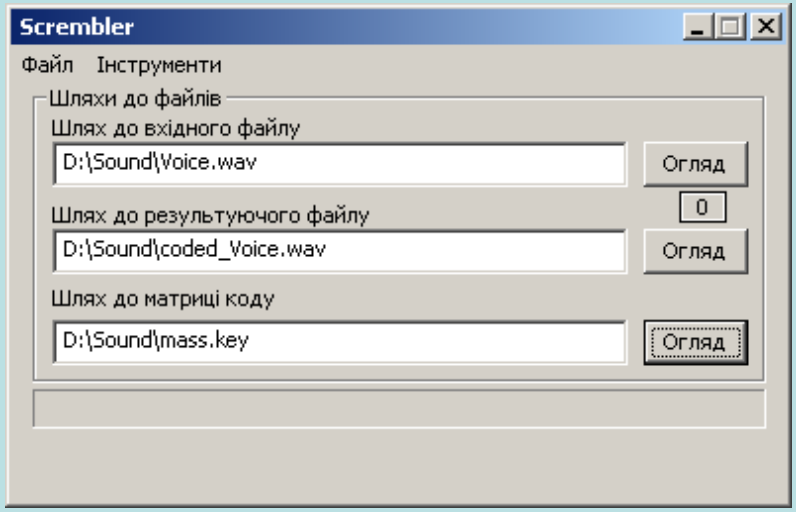


Для написання програми використовувалася мова програмування Visual C++.

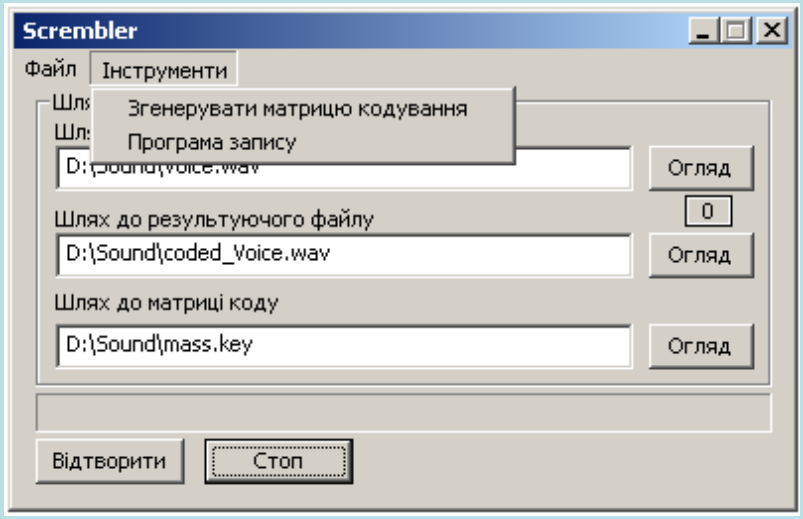
ВИД ІНТЕРФЕЙСУ ПРОГРАМИ ПІСЛЯ ЗАПУСКУ



Вікно програми після запуску



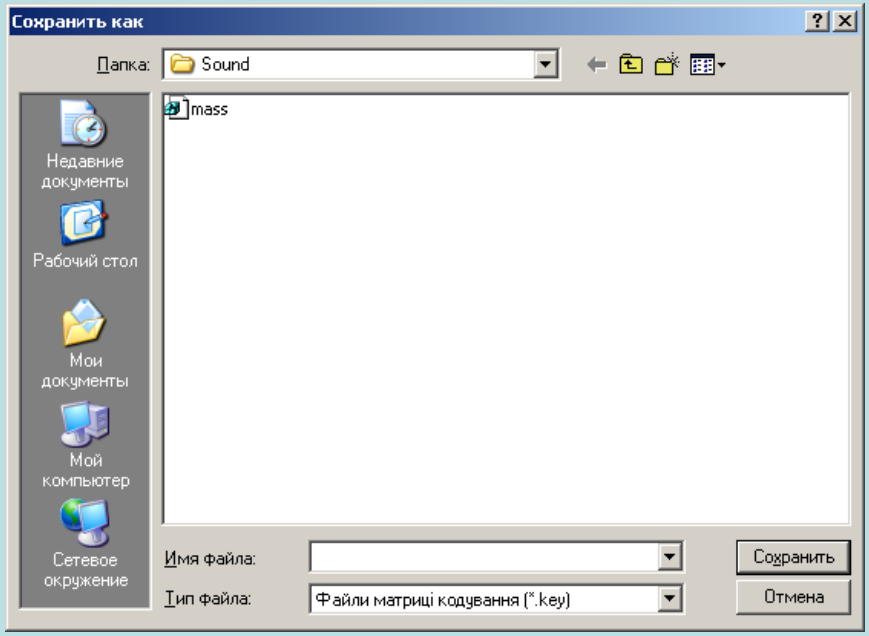
Вказання шляхів до файлів



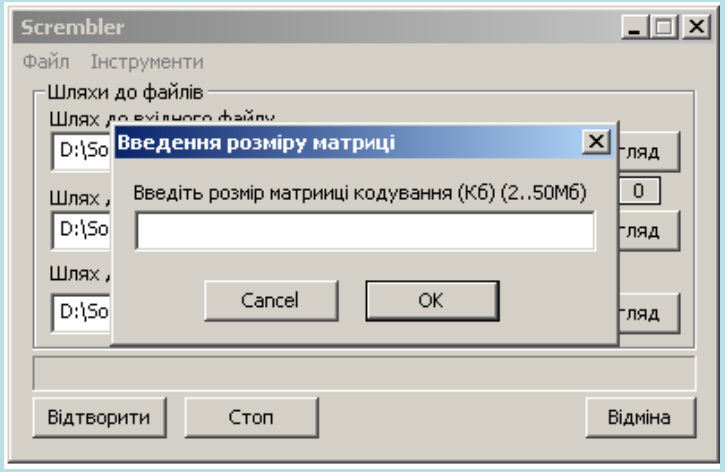
Вибір опції «Згенерувати матрицю кодування» пункту меню «Інструменти»

Розроблена програма дозволяє шифрувати звук як безпосередньо з мікрофона, так і зі звукових файлів WAV-формату і передбачає використання секретного масиву випадкових чисел великого розміру та короткого паролю (напр., 16 символів), який треба пам‘ятати і не розголошувати

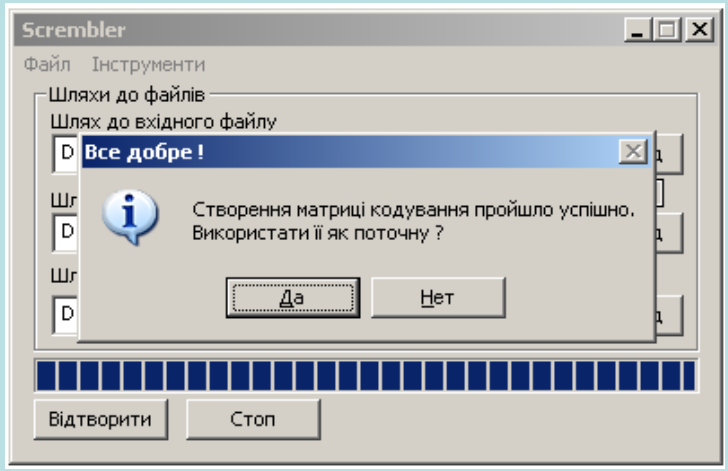
ВИД ІНТЕРФЕЙСУ ПРОГРАМИ ПРИ СТВОРЕННІ МАСИВУ ВИПАДКОВИХ ЧИСЕЛ



Створення файлу з масивом випадкових чисел

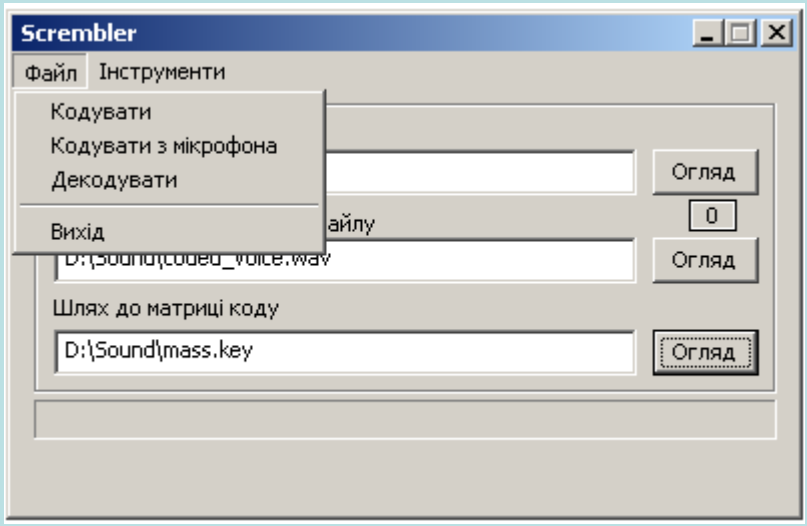


Задання розміру масиву випадкових чисел

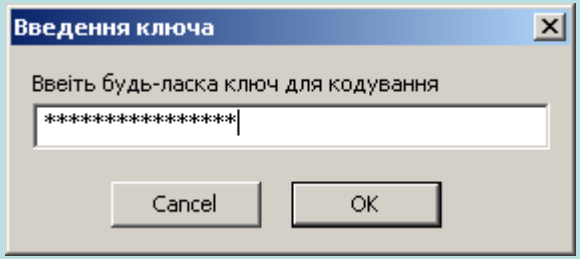


Вид вікна програми при успішному виконанні процесу генерування матриці випадкових чисел

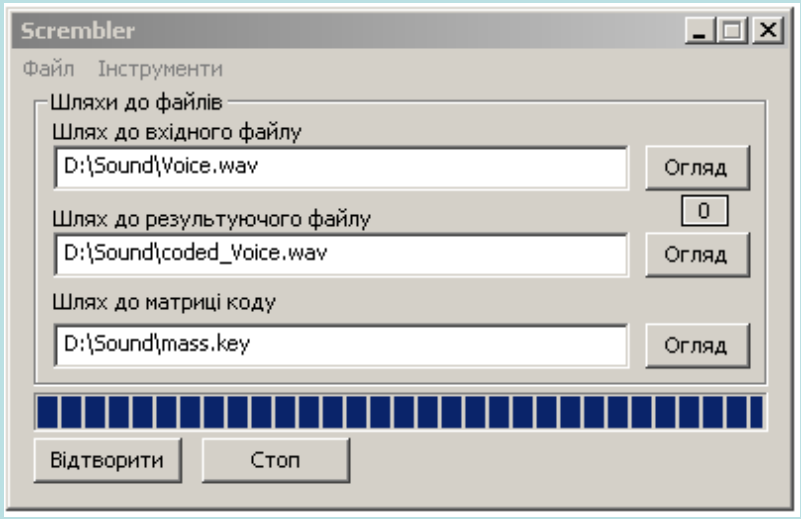
ВИД ІНТЕРФЕЙСУ ПРОГРАМИ ПРИ ВИБОРІ РЕЖИМУ ШИФРУВАННЯ



Запуск процесу шифрування

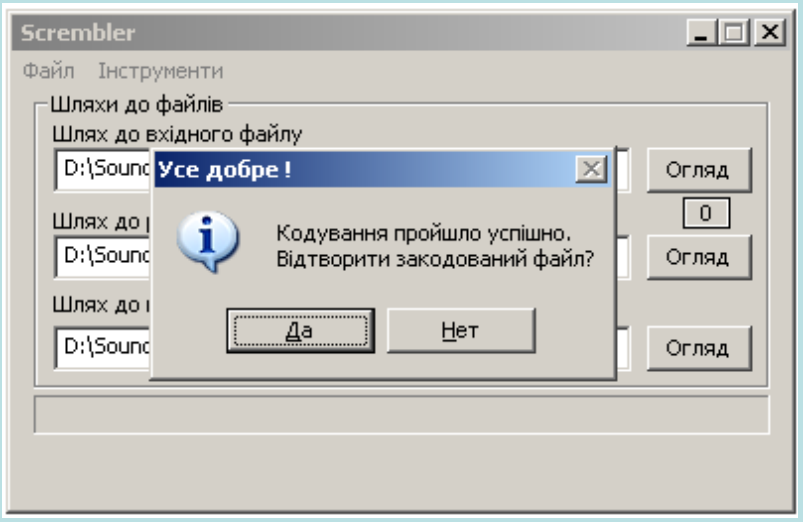


Введення паролю

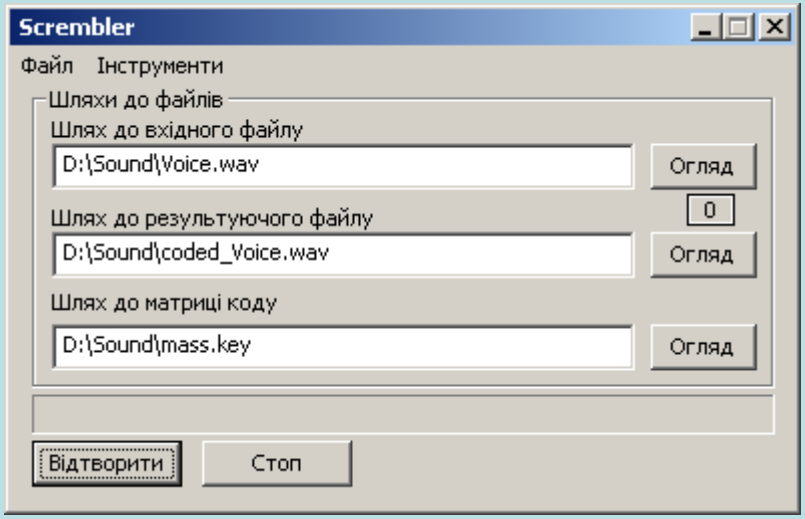


Виконання процесу шифрування

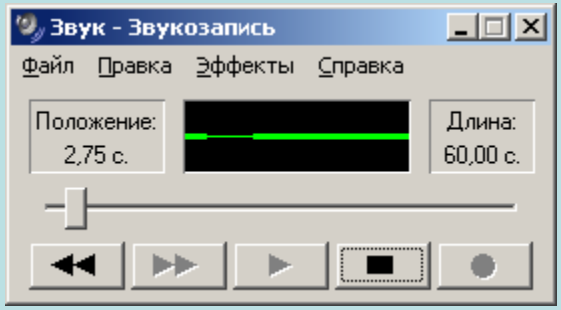
ВИД ІНТЕРФЕЙСУ ПРОГРАМИ ПРИ ВИБОРІ РЕЖИМУ ВІДТВОРЕННЯ ЗАШИФРОВАНОГО ФАЙЛУ



Вид вікна програми при успішному виконанні процесу кодування



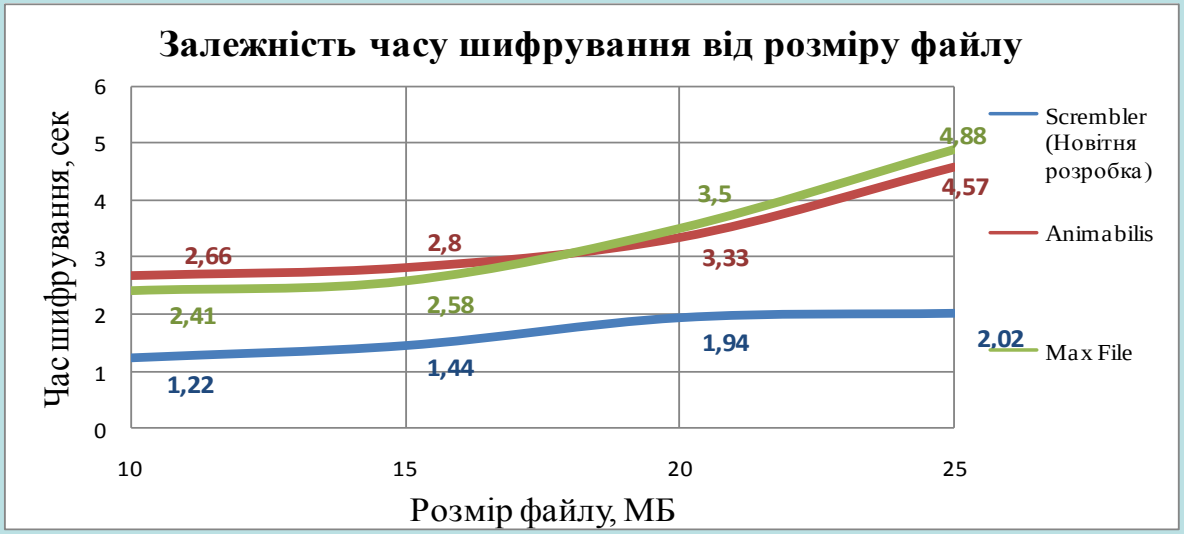
Виконання процесу відтворення закодованого файлу

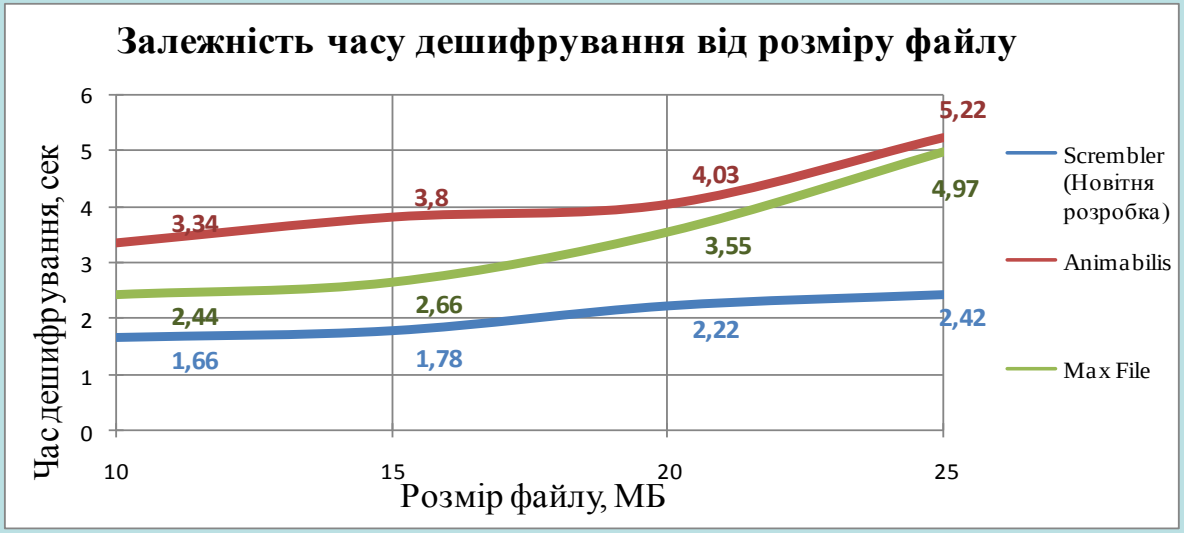


Використання стандартної програми «Звукозапис» при кодуванні звуку з мікрофона

Для написання програми використовувалася мова програмування Visual C++

Порівняльна характеристика роботи розробленої програми і аналогів





Як видно з діаграм, час шифрування за допомогою розробленої програми в середньому на 1,1 секунду менше, ніж за допомогою програм аналогів. Час дешифрування в середньому склав приблизно 1,6-2,1 секунди, що на 1,3-2,6 секунди менше, ніж у програм-аналогів, при чому довжина ключа у програм-аналогів на 32 біти менше, ніж у розробленої програми

ЕКОНОМІЧНА ЧАСТИНА

Було здійснено економічне обґрунтування доцільності розробки інформаційної технології захисту аудіо інформації. Зазначена розробка має вищий рівень якості, ніж продукт конкурентів, обраний за аналог (RS File Encryption), оскільки коефіцієнт відносної якості дорівнює 2,075; також розробка є більш конкурентоспроможною, оскільки загальний коефіцієнт конкурентоспроможності дорівнює 2,2. В процесі розрахунків було також визначено загальні витрати на проведення науково-дослідної роботи, які скадають 51175,6 грн. Джерелом зазначених коштів можуть бути інвестори, для залучення яких визначено розмір чистих прибутків за три роки реалізації розробленого ПЗ (979200 грн.) та термін окупності інвестицій, який складає 0,65 року. Таким чином, проведені розрахунки підтверджують економічну доцільність розробки інформаційної технології захисту аудіо інформації та її конкурентоспроможність на ринку програмного забезпечення.

АПРОБАЦІЯ РЕЗУЛЬТАТІВ РОБОТИ ТА ПУБЛІКАЦІЇ

Апробація результатів роботи.

Результати досліджень апробовані на IV МІЖНАРОДНІЙ НАУКОВО-ПРАКТИЧНІЙ КОНФЕРЕНЦІЇ «Інформаційні технології та взаємодії» м. Київ, 8-10 листопада 2017 року

Публікації.

За результатами магістерської кваліфікаційної роботи опубліковано 1 тези доповідей на конференції.

ВИСНОВОК

В результаті виконання роботи було розроблено інформаційну технологію захисту аудіоінформації. Програмну реалізацію технології здійснено об’єктно-орієнтованою мовою програмування Visual C++. Створений програмний засіб має підвищений ступінь захисту звукових файлів у WAV-форматі та мовленнєвих сигналів безпосередньо з мікрофону.
Швидкодія розробленої програми порівняно з двома програмами-аналогами в середньому вища на 45% для файлів різного розміру. Отже, мета роботи досягнута.

Дякую

за увагу!