МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА НА ТЕМУ:

«Інформаційна технологія шифрування файлів на основі адаптивного гамування»

Виконав: магістрант групи 1КН-17м
Боголюбський О.В.
Керівник: к.т.н., доц. Арсенюк І.Р.

МЕТА ТА ЗАВДАННЯ ДОСЛІДЖЕННЯ

Актуальність Необхідність створення нових способів захисту інформації від несанкціонованого доступу, копіювання, дослідження

Метою дослідження магістерської кваліфікаційної роботи є підвищення якості захисту програмних засобів шифрування комп`ютерної інформації.

Для досягнення поставленої мети необхідно розв’язати такі завдання:

- провести аналіз проблеми розв’язання задачі шифрування комп`ютерної інформації;
- розглянути існуючі методи вирішення задачі шифрування комп`ютерної інформації та обрати й обґрунтувати вибір методу, який задовольняє мету даної магістерської кваліфікаційної роботи;
- розробити метод шифрування комп`ютерної інформації;
- сформулювати стадії інформаційної технології, розробити структуру та алгоритм роботи програмного засобу;
- виконати програмну реалізацію запропонованої інформаційної технології;
- провести тестування програмного продукту та виконати аналіз отриманих результатів.

ОБ’ЄКТ, ПРЕДМЕТ ТА МЕТОДИ ДОСЛІДЖЕННЯ

Об’єкт дослідження – процес шифрування файлів для захисту комп`ютерної інформації від несанкціонованого доступу.

Предмет дослідження – методи та програмні засоби шифрування файлів для захисту комп`ютерної інформації від несанкціонованого доступу та якість захисту.

Методи дослідження

У роботі використані наступні методи наукових досліджень:

-- системного аналізу,
-- теорії інформації та кодування,
-- теорії захисту інформації,
-- криптографії,
-- методи математичної статистики для обрахунків результатів експериментів із програмним засобом,
-- об’єктно-орієнтованого програмування.

НАУКОВА НОВИЗНА ОДЕРЖАНИХ РЕЗУЛЬТАТІВ

полягає в наступному:

1. Набула подальшого розвитку інформаційна технологія шифрування комп`ютерної інформації, яка відрізняється використанням гами, що формується на основі параметрів комп'ютера, що дозволило підвищити секретність програмних засобів шифрування комп`ютерної інформації.

2. Удосконалено метод шифрування файлів на основі гамування, який відрізняється побайтовим накладанням гами у порядку виконання операцій що залежить від значення пароля, що дозволило підвищити швидкість шифрування.

ПРАКТИЧНЕ ЗНАЧЕННЯ ОДЕРЖАНИХ РЕЗУЛЬТАТІВ

- розроблено алгоритм роботи програмної реалізації інформаційної технології шифрування файлів на основі адаптивного гамування;
- розроблено структуру програмного засобу,
- розроблено алгоритм роботи функції формування коду операції,
- розроблено алгоритм роботи модулю зашифровування,
- розроблено алгоритм запуску захищеного файлу на виконання;
- розроблено програмні засоби для шифрування файлів на основі адаптивного гамування;

АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ШИФРУВАННЯ ФАЙЛІВ

Класифікація систем захисту програмного забезпечення

Види перетворень в симетричних криптосистемах

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

ВИБІР І ОБҐРУНТУВАННЯ АНАЛОГУ

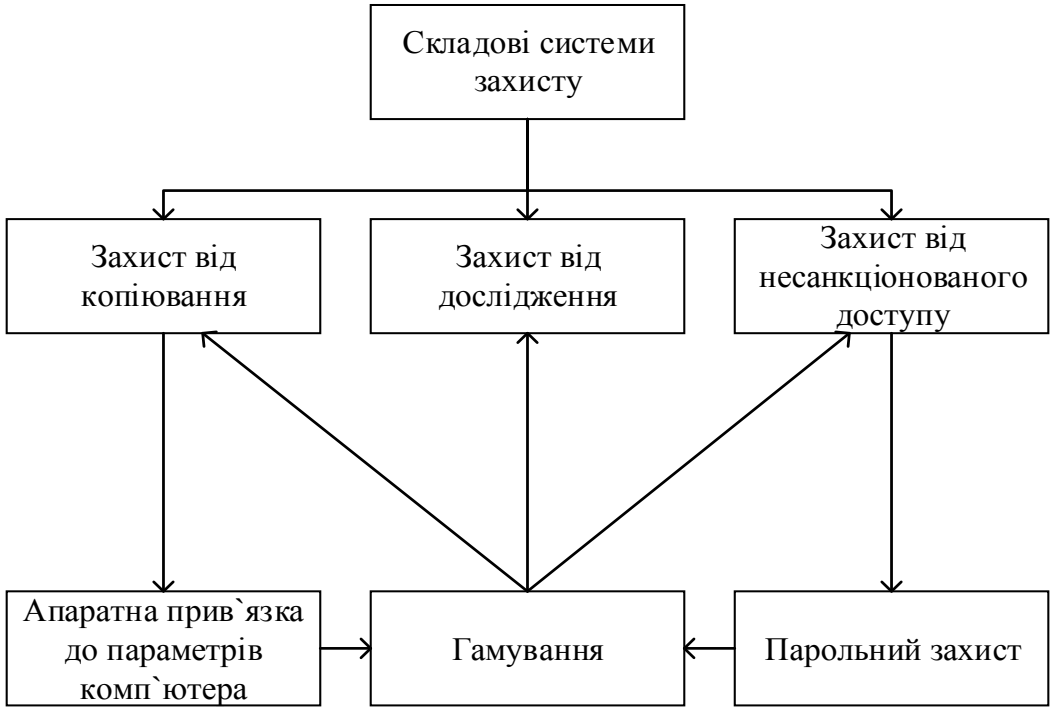
Таблиця 1.1 – Параметри деяких програм шифрування файлів

	Продукт	Ціна $	Оцінка	Продуктивність	Секретність	Швидкість	Зручність використання	Генератор паролів	Криптоалгоритм
1	Folder Lock	39.95	4.2	4.9	5	1	1	-	256-bit key AES
2	Secure IT File Encryption	29.95	5	5	3.4	0,85	1	-	256-bit key AES
3	Consealer	24.95	5	4.7	4	0,77	0,9	+	256-bit key AES
4	Renee File Protector	39.95	4.2	4.5	5	0,9	0,9	-	256-bit key AES

Аналог - програма Folder Lock

Розробка методу шифрування файлів на основі адаптивного гамування

Відповідно до структури системи захисту програмного продукту, захист від копіювання включає в себе реалізацію апаратної прив’язки, захист від несанкціонованого доступу включає в себе парольний захист та захист від дослідження включає в себе гамування відповідно.

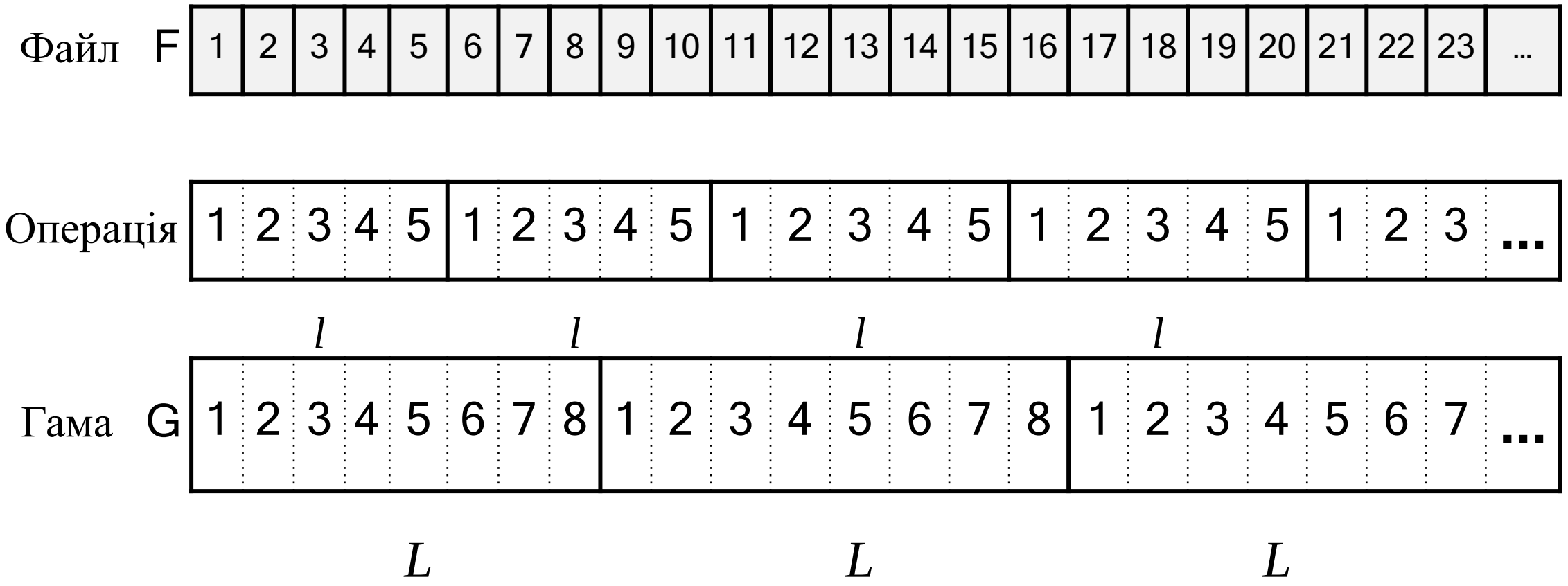


Метод шифрування файлів :

1. Отримання бітових рядків із обраних користувачем . параметрів комп’ютерної системи.
2. Отримання гами (послідовність символів), яка формується конкатенацією бітових рядків, сформованих із обраних користувачем параметрів комп’ютерної системи.
3. Визначення виду порозрядної операції (одна з чотирьох: XOR, HI, циклічний зсув ліворуч, циклічний зсув праворуч) для кожних двох біт файлу на основі паролю користувача.
4. Всі отримані зашифровані байти записуються у вихідний зашифрований файл.

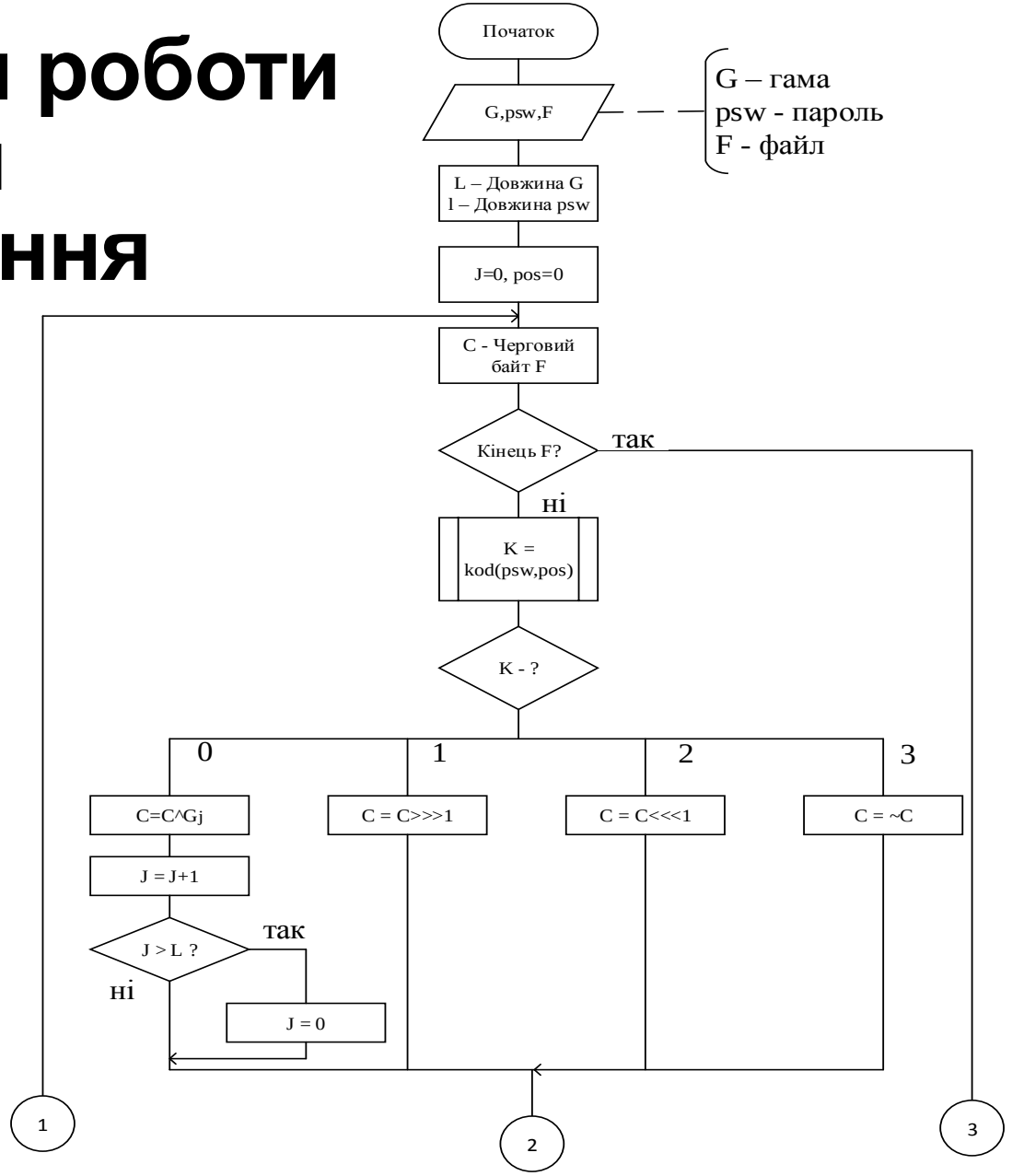
Детально – на схемі шифрування

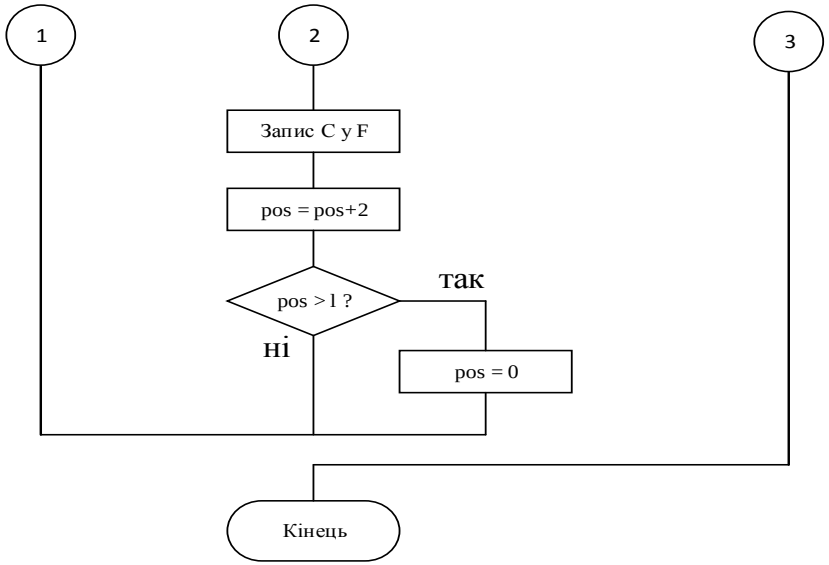
Схема шифрування (накладання гами)



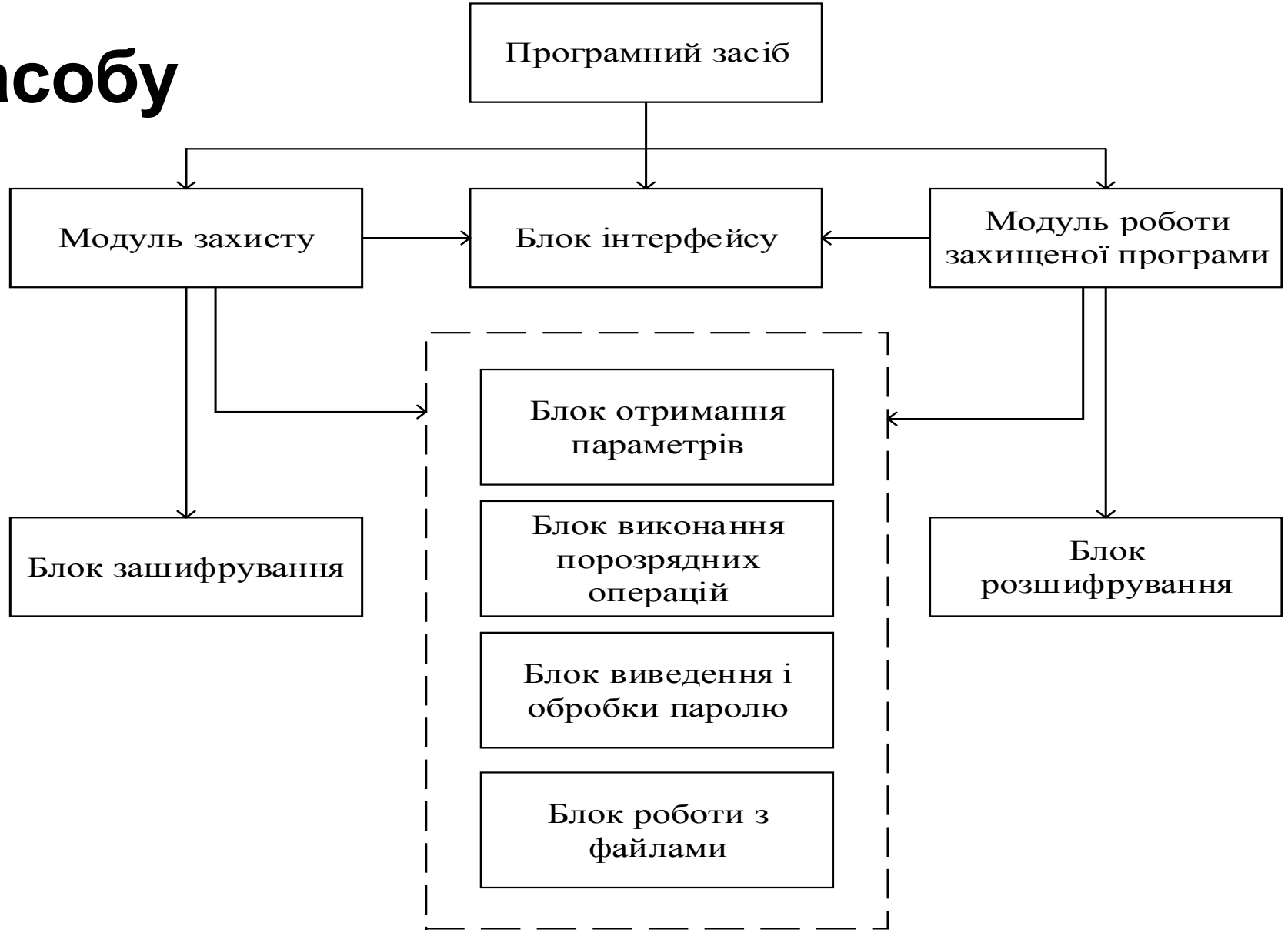
Структура інформаційної технології шифрування файлів на основі адаптивного гамування

Алгоритм роботи програми шифрування



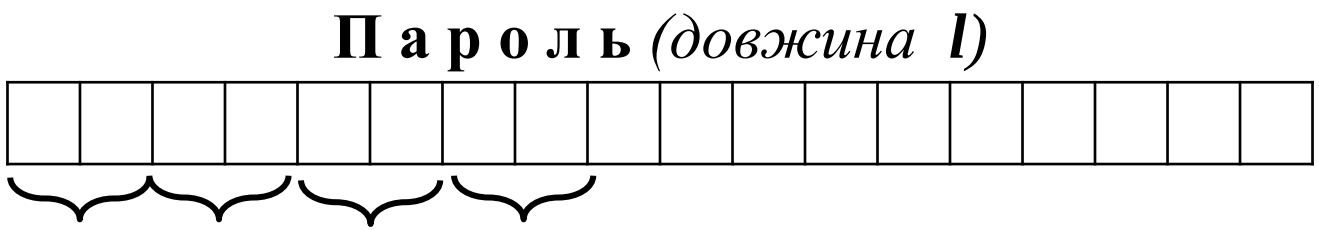


Структура програмного засобу

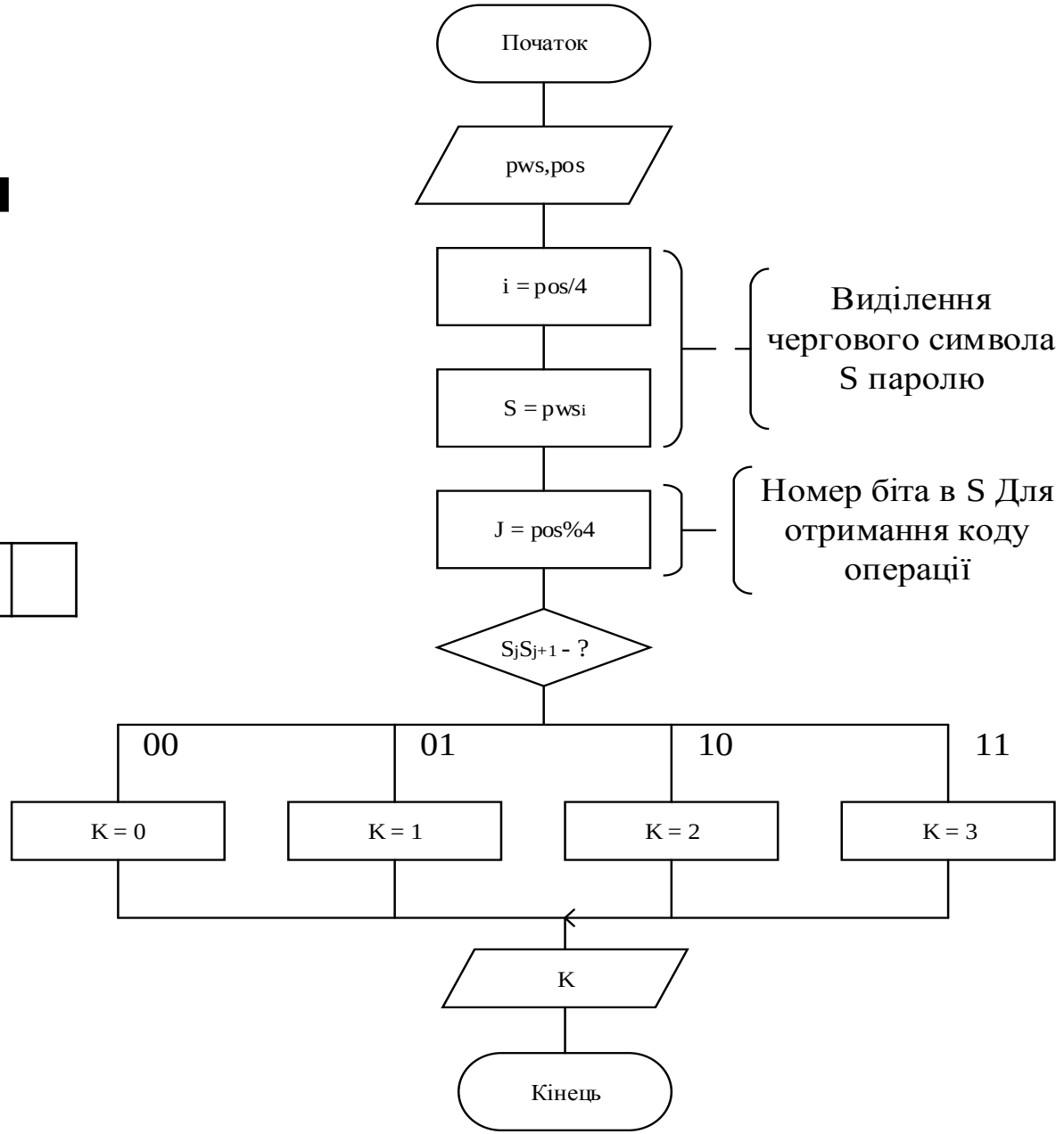


Блок обробки паролю

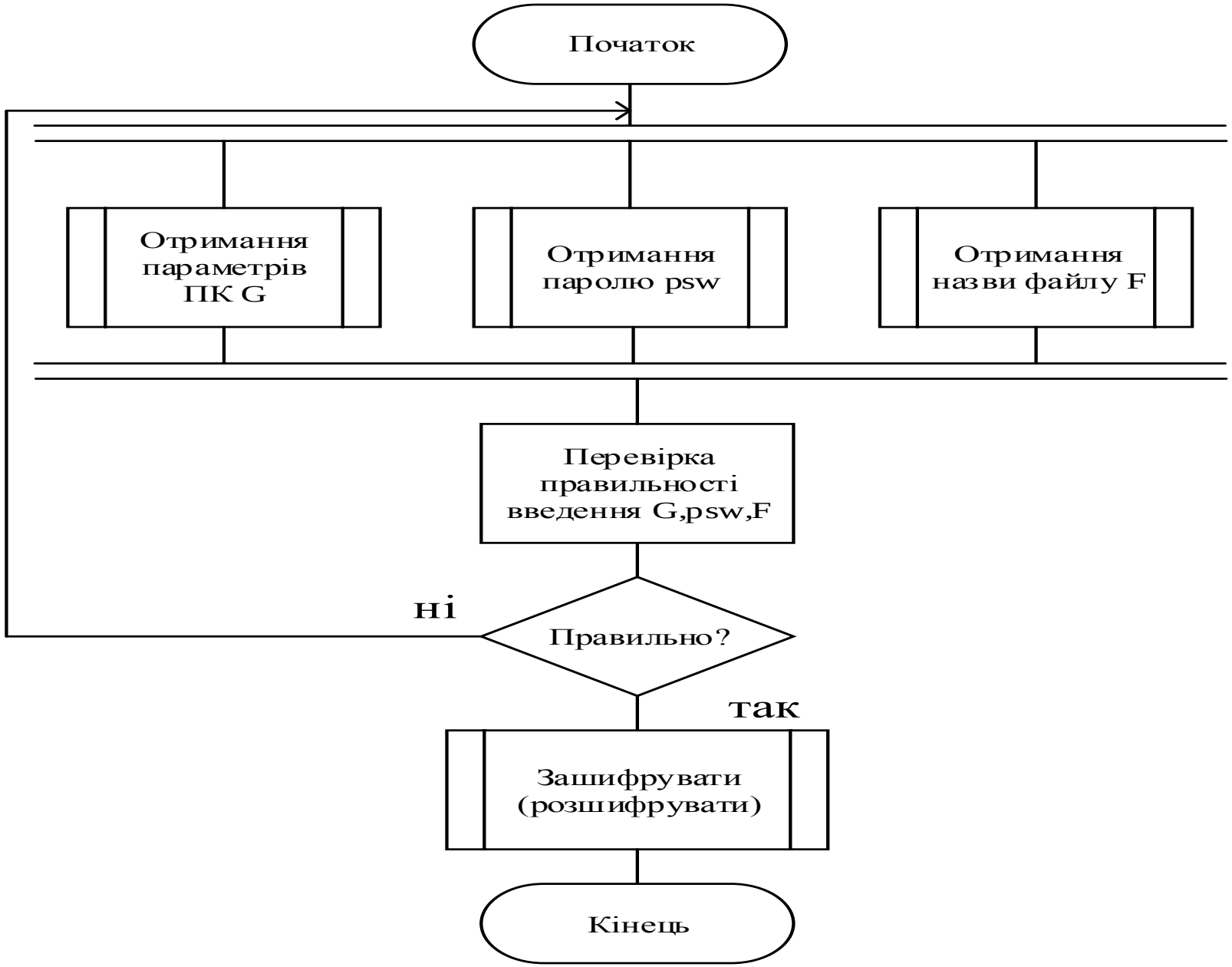
(формування кодів операцій для шифрування)



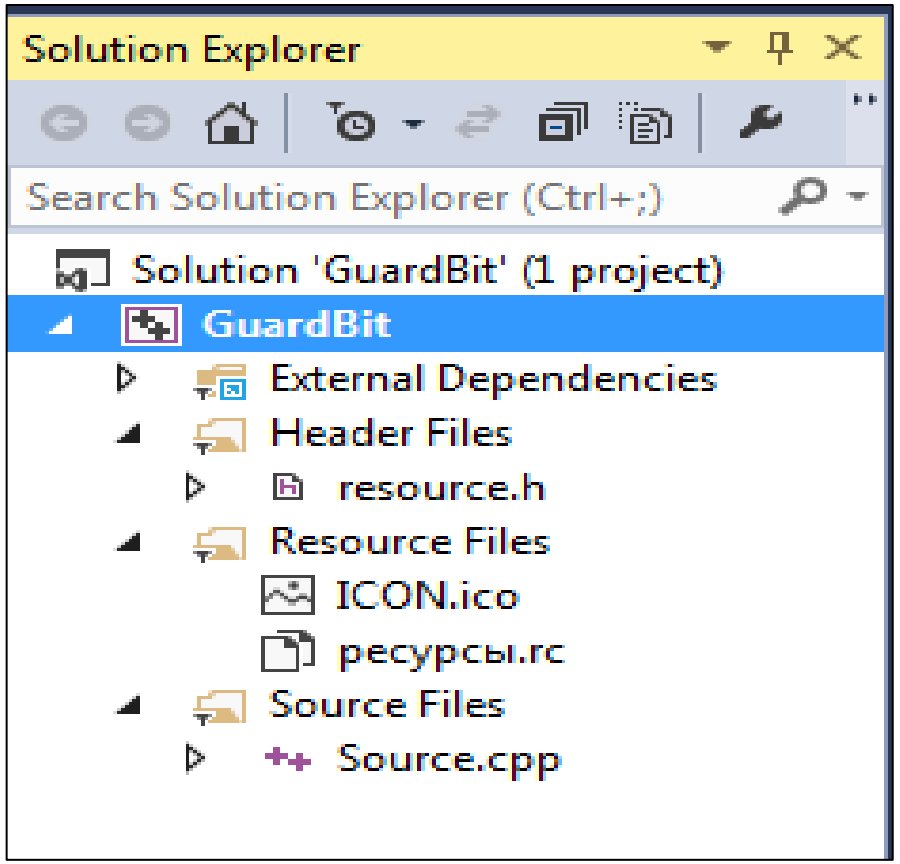
00 (0) – операція XOR (^);
01 (1) – операція зсуву вправо (>>>);
10 (2) – операція зсуву вліво (<<<);
11 (3) – операція бітової інверсії (~);

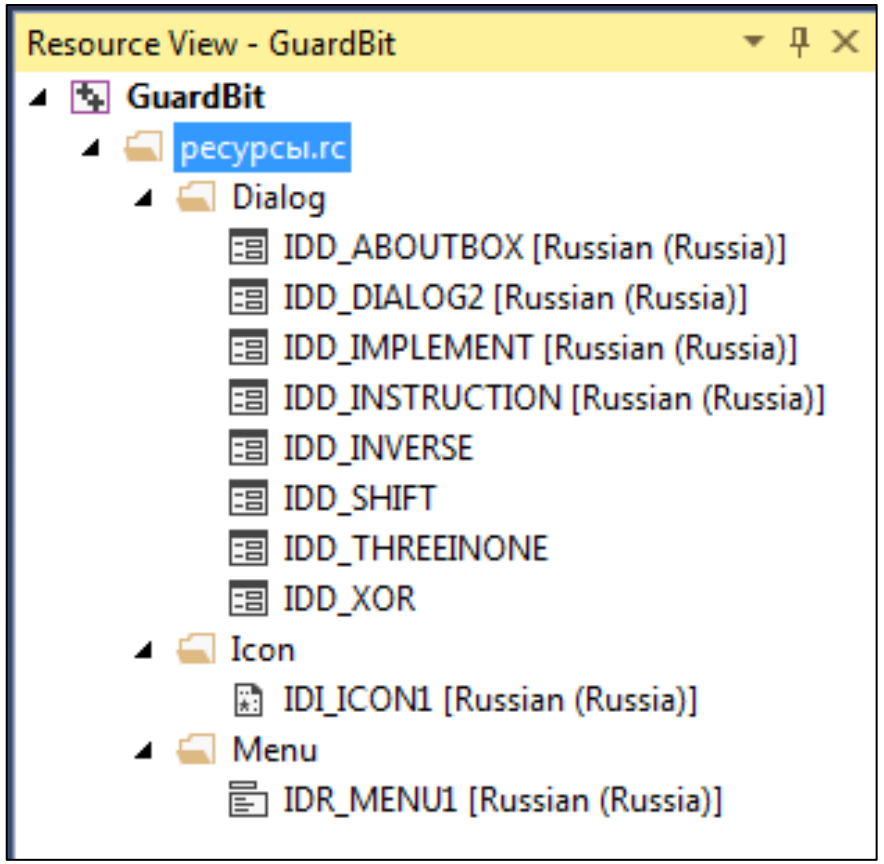


Алгоритм роботи модуля зашифрування та розшифрування



СТРУКТУРА ПРОЕКТУ

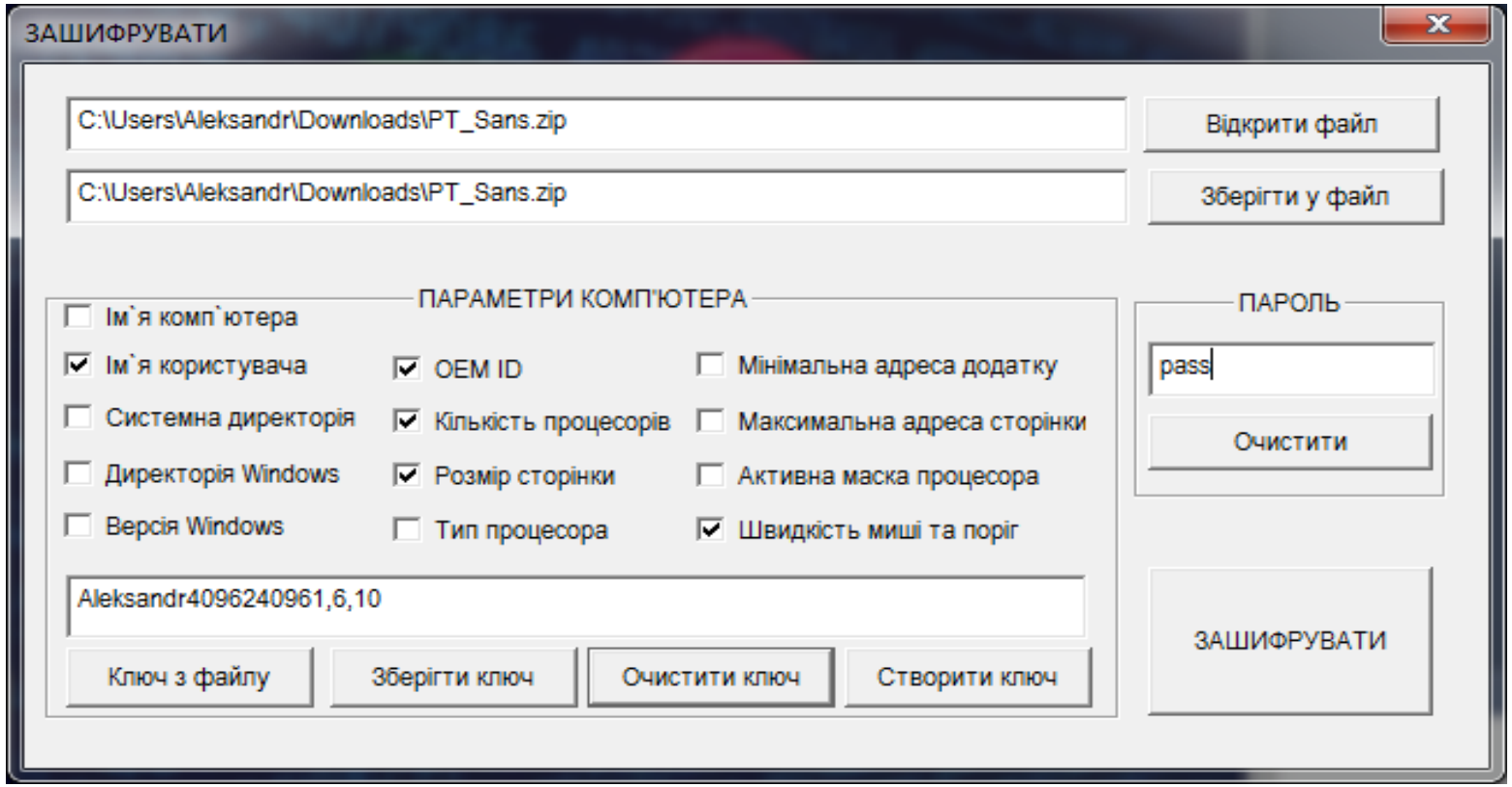




Програмна реалізація інформаційної технології шифрування файлів на основі адаптивного гамування виконана на мові C++ у середовищі Microsoft Visual Studio 2015

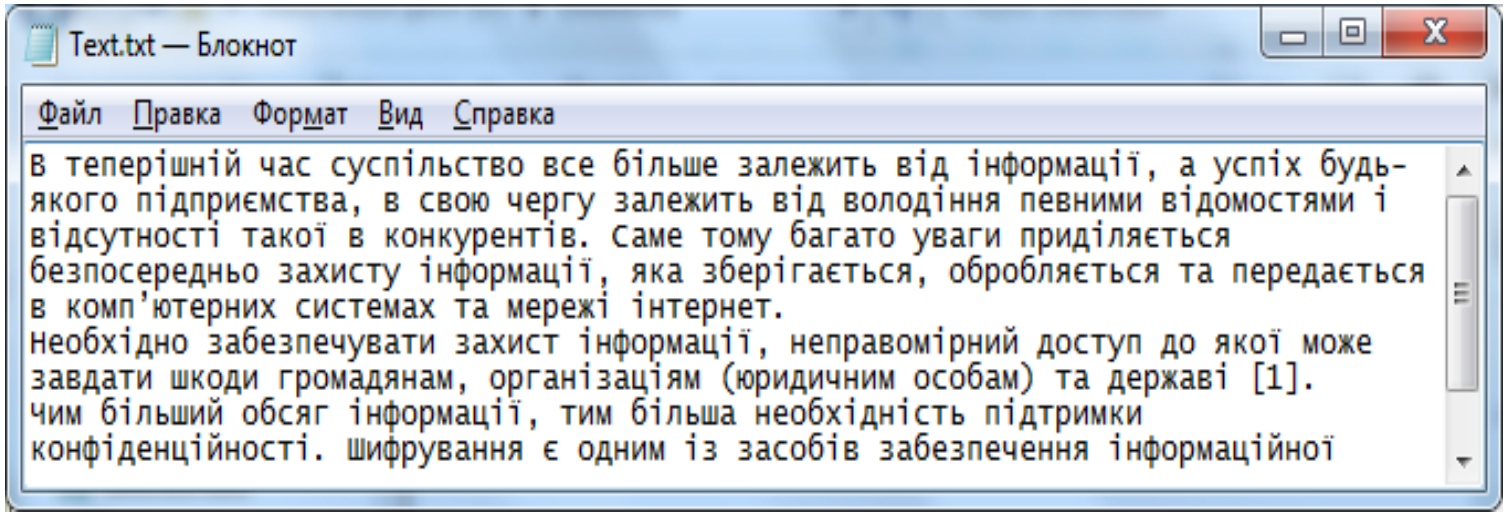
Фрагменти інтерфейсу програмного засобу

Головне вікно програми

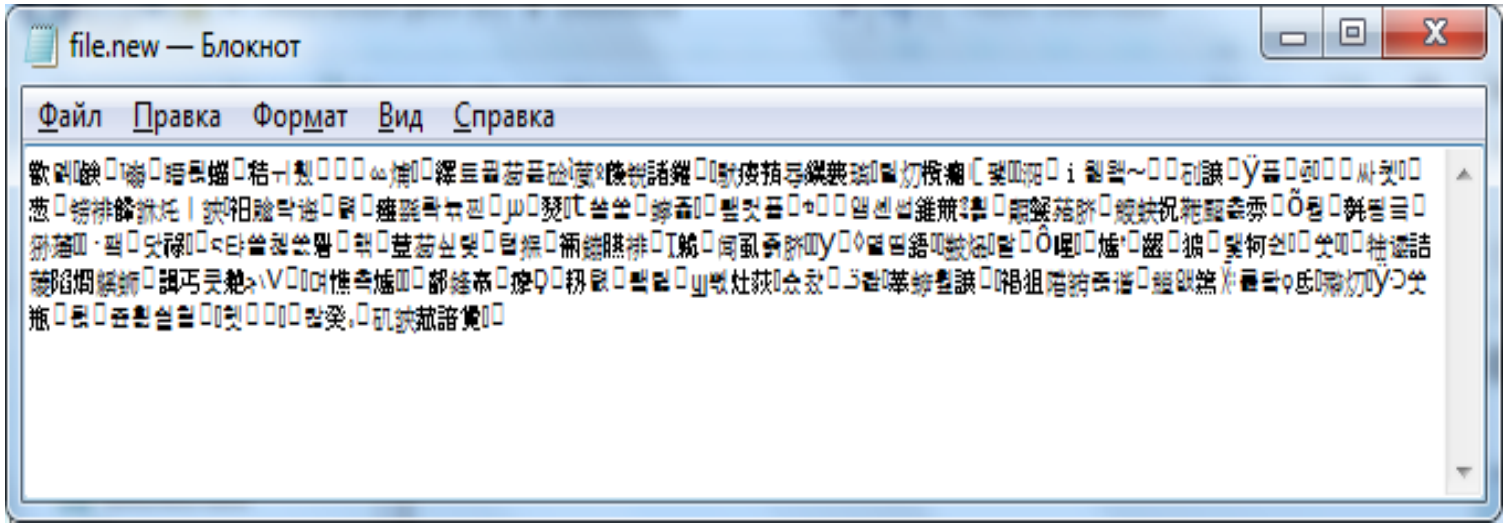


Діалогове вікно для зашифрування інформації

Результати зашифровування текстового файлу

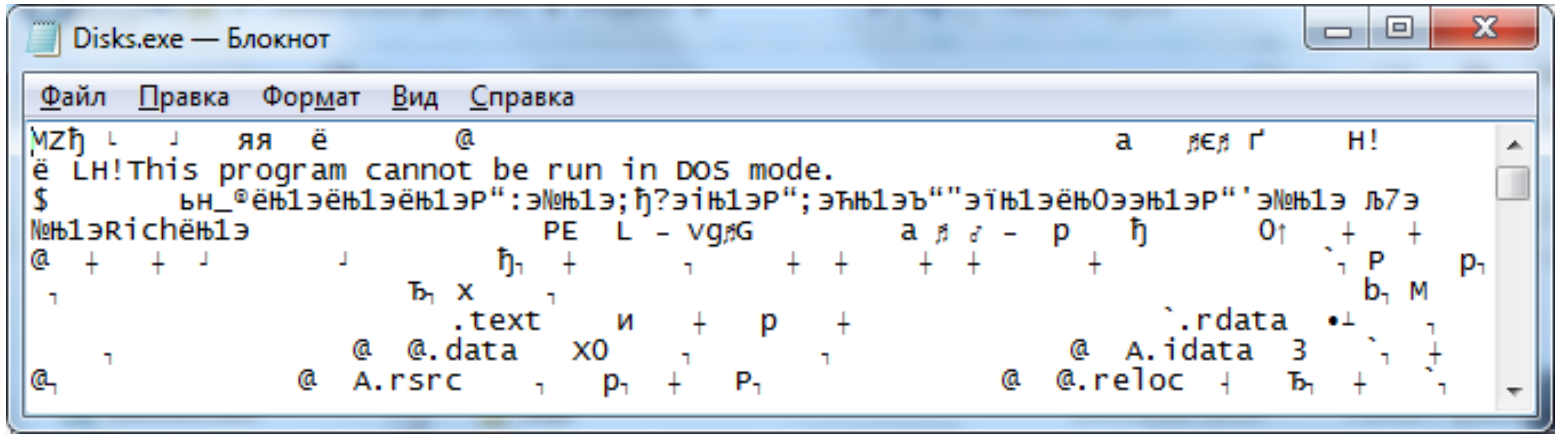


Вигляд файлу до проведення операції зашифрування

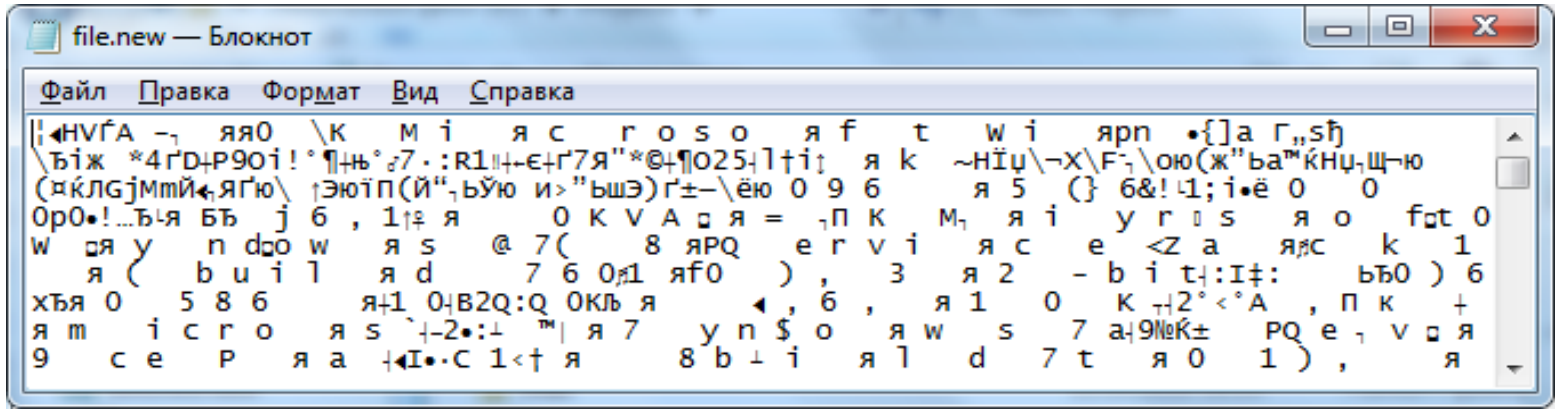


Вигляд файлу після проведення операції зашифрування

Результати захисту виконуваного файлу



Вміст виконуваного файлу у символьному вигляді до зашифрування



Вміст виконуваного файлу у зашифрованому вигляді

Результат запуску зашифрованого файлу на виконання

Аналіз результатів роботи програмного засобу шифрування файлів на основі адаптивного гамування

Таблиця 3.1 – Порівняння параметрів аналога та розробленої програми

	Програма-аналог Folder Lock	Розроблена програма
Секретність (балів)	5	6
Швидкість	1	1,2
Зручність використання (балів)	1	1,1
Криптоалгоритм	256-bit key AES	Запропонований в МКР

У табл. секретність оцінено у балах. Розроблена програма має 6 балів (а аналог 5), тому що в аналозі секретність визначається алгоритмом шифрування та паролем, а в розробленій програмі - алгоритмом шифрування, паролем та обраними параметрами комп'ютера. Тобто у розробленій програмі більше факторов впливають на секретність. Швидкість програми-аналога умовно прийнята за 1, а швидкість розробленої програми – 1,2. Це означає, що розроблена програма в середньому на 20 відсотків швидше за програму-аналог шифрує і розшифровує файли. Із табл. видно, що розроблене ПЗ має вищу секретність, більшу швидкість та зручність користування ніж аналогічна програма, тобто її загальна якість покращилась, а значить мета роботи досягнута.

ЕКОНОМІЧНА ЧАСТИНА

Було проведено економічне обґрунтування доцільності розробки програми для шифрування файлів, яка створена у результаті науково-технічної діяльності. Нова розробка має рівень комерційного потенціалу вище середнього. Загальна сума витрат на виконання робіт склала "35641,12" грн. Загальні витрати на виконання та впровадження результатів наукової роботи – 41930,73 грн. Абсолютна ефективність вкладених інвестицій становить 385264,39 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 – 117 %, отже інвестор буде зацікавлений у фінансуванні даної наукової розробки. Термін окупності складає 0,85 року. В загальному, можна зробити висновок, що фінансування розробки програми для шифрування файлів, яка створена у результаті науково-технічної діяльності є висококункурентоспроможним.

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 шифрування файлів на основі адаптивного гамування. Програмну реалізацію технології здійснено об’єктно-орієнтованою мовою програмування C++ під операційну систему Windows. Розроблене програмне забезпечення має вищу секретність, більшу швидкість (у середньому на 20%) та зручність користування ніж аналогічна програма, тобто її загальна якість покращилась, а значить мета роботи досягнута.

Дякую за увагу!