УДК 681.12

О. В. Боголюбський[1]
І.Р. Арсенюк[1]

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ШИФРУВАННЯ ФАЙЛІВ НА ОСНОВІ АДАПТИВНОГО ГАМУВАННЯ

[1] Вінницький національний технічний університет;

Анотація

Запропоновано метод та інформаційну технологію шифрування файлів на основі адаптивного гамування, яке для формування гами використовує прив'зку до параметрів комп'ютера, що дозволило підвищити загальну якість захисту файлів, оскільки має вищу секретність та більшу швидкість шифрування.

Ключові слова: шифрування, інформаційна технологія, гамування, захист інформації.

Abstract

The method and information technology of encryption of files on the basis of adaptive gamma, which for gamma formation uses the access to computer parameters, which has allowed to improve the overall quality of file protection, because it has the highest level of secrecy and higher encryption speed, is proposed.

Keywords: encryption, information technology, gamming, information protection.

Вступ

В даний час у зв'язку з складним характером взаємостосунків на ринку програмних продуктів проблема захисту від несанкціонованого копіювання (НСК) є однією з найгостріших у області розробки програмних засобів (ПЗ). Вона обумовлена «самою суттю людської психології і існуватиме до тих пір, поки програмний продукт є товаром». А це означає, що несанкціоноване копіювання здійснюється тоді, коли у користувача існує потреба в експлуатації якогось програмного продукту, а витрати на копіювання істотно менше витрат на придбання легальної копії.

Проблема захисту програмних продуктів від несанкціонованого використання [1], а зокрема, розробка і реалізація системи захисту від несанкціонованого копіювання, і є предметом даної роботи.

Метою роботи є розроблення інформаційної технології та методу шифрування файлів на основі адаптивного гамування, які мають підвищену якість захисту інформації.

Результати дослідження

Пропонується реалізовувати шифрування на основі гамування. У якості гами слугуватиме повідомлення, отримане з параметрів комп'ютера. Але, якби гама накладалась однаково на все захищуване повідомлення, зламати такий захист не склало би ніяких труднощів. Тому прийнято рішення здійснювати побайтове накладання гами, причому порядок виконання операцій буде залежати від значення пароля.

Шифрування повідомлення відбувається таким чином.

Для шифрування необхідні: F – файл, що підлягатиме захисту; G – гама – послідовність символів (байтів), отриманих в результаті вибору параметрів комп'ютерної системи; psw – пароль користувача.

Файл у програмі буде зчитуватись по байтах (рис. 1).

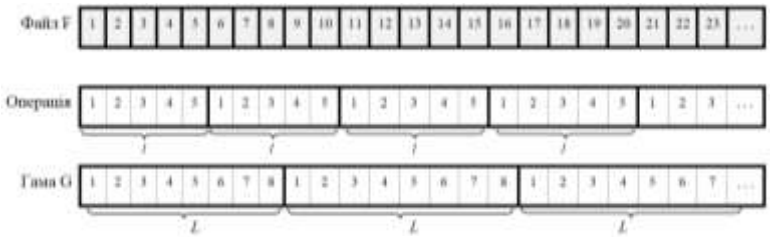

Рисунок 1 – Схема накладання гами

Структура інформаційної технології шифрування файлів на основі адаптивного гамування показана на рис.2.

Рисунок 2 – Структура інформаційної технології шифрування файлів на основі адаптивного гамування

Було спроектовано програмне забезпечення шифрування файлів на основі адаптивного гамування [2]. Програму написано мовою програмування високого рівня C++ під операційну систему Windows. Розроблене програмне забезпечення має більшу секретність, тому що у відомих засобах 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. Тестування показало, що розроблена програма в середньому на 20 відсотків швидше за програму-аналог Folder Lock шифрує і розшифровує файли.

Висновки

Встановлено, що запропонована інформаційна технологія шифрування файлів на основі адаптивного гамування та її програмна реалізація дозволяє підвищити секретність шифрування та збільшити швидкодію шифрування (у середньому на 20%) за рахунок прив'язки процесу формування гами до параметрів комп'ютера.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Каплун В.А., Дмитришин О.В., Баришев Ю.В. Захист програмного забезпечення, частина 2 – Вінниця, ВНТУ, 2014 – 105 с.2.
2. Каплун В. А., Боголюбський О. В. Комп'ютерна програма «Порозрядне шифрування». Свідоцтво про реєстрацію авторського права на твір № 69368 від 22.12.2016.

Боголюбський Олександр Валентинович — студент групи 1КН-17м, факультет інформаційних технологій та компютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: aleksandr.bogolyubskiy@gmail.com

Науковий керівник: ***Арсенюк Ігор Ростиславович*** — к.т.н., доцент кафедри комп'ютерних наук, Вінницький національний технічний університет, м. Вінниця

Bogoliubskyi Olexandr V. — Department of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email : aleksandr.bogolyubskiy@gmail.com

Supervisor: ***Arseniuk Igor R.*** — PhD (Eng.), docent, Chair of Computer Sciences, Vinnytsia National Technical University, Vinnytsia