УДК 004.56.5

МЕТОД КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ В КС

Вузій С.В
Науковий керівник – к. т. н., ст. викл. Дмитришин О.В.

За оцінками Business Software Alliance фінансові збитки через порушення авторських прав станом 2008 рік становить $53 млрд. Основною причиною порушення авторських прав в тому, що програмні засоби є абсолютно беззахисні. Саме тому для захисту програмного забезпечення потрібно використовувати надійні методи захисту.

Метою даної роботи є дослідження існуючих методів захисту на основі блокового шифру та внесення пропозицій для покращеного методу з ціллю подальшого дослідження запропонованого методу.

Розглянуто наступні методи блокового шифрування. Перший з них полягає у генеруванні секретного ключа з відповідною інформацією двійкового коду під час виконання. У даному методі всі функції дешифрування або шифрування інших функцій, використовують їх власний код в якості ключового матеріалу, що забезпечує цілісність. Даний метод має недолік, коли функція, що шифрується, викликається декількома іншими функціями.

Наступний метод дуже схожий на попередній. Даний метод шифрує N-й блок за допомогою ключа, який був отриманий на основі (N-1)-го блоку. Якщо блок викликається більш ніж з двох попередніх блоків, то блок що викликається дублюється. Щоб вирішити цю проблему надлишковості запропонуємо нову схему на основі індексної таблиці. У нашій схемі блоки B і C може розшифрувати блок D без дублювання блоку D, так як блок B і C можуть отримати ключ B з індексної таблиці, як показано на рис. 2.

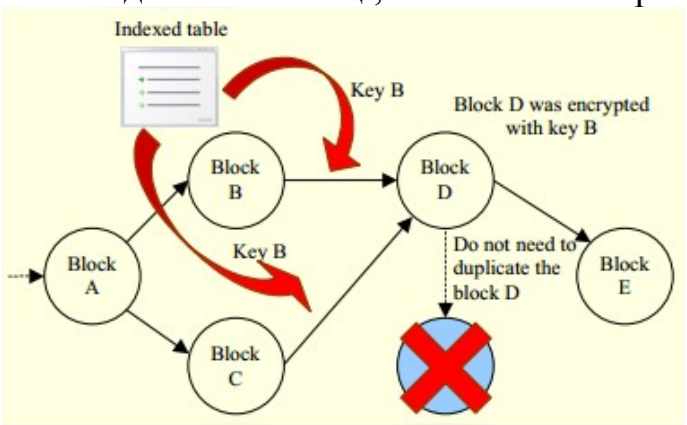

Рисунок 2 – Шифрування на основі індексної таблиці

Висновок в дані роботі було досліджено існуючі методи блокового шифрування та запропонований вдосконалений метод, який враховує недоліки попередніх. В подальшому планується дослідження ефективності запропонованого методу та його реалізація.