

РЕАЛІЗАЦІЯ АЛГОРИТМУ СКРЕМБЛЮВАННЯ У МОВІ ПРОГРАМУВАННЯ C++

Інформація є найціннішим ресурсом, тому її захист є пріоритетною задачею. В наш час, коли цінність інформації стає все вищою, а власники інформації хочуть як найбільше знизити ризик її втрати, розглядати цю тему в край необхідно. В країнах Західної Європи питанням захисту інформації приділяють не менше уваги ніж в нашій країні. Тому ця проблема актуальна на сьогодні як для користувачів телефонів та інших засобів передачі інформації, так і для її розробників. Згідно закону, захист інформації в системі - діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі.

Скремблер – програмний або апаратний пристрій (алгоритм), що виконує скремблювання - оборотне перетворення цифрового потоку без зміни швидкості передачі з метою отримання властивостей випадкової послідовності. Після скремблювання поява «1» і «0» у вихідній послідовності різновірогідні. Скремблювання - оборотний процес, тобто вихідне повідомлення можна відновити, застосувавши зворотний алгоритм.

Пропонуємий алгоритм скремблювання полягає в побітному обчисленні результуючого коду на основі бітів вихідного коду та отриманих у попередніх тактах бітів результуючого коду.

Після отримання заскрембленої послідовності бітів приймач передає її дескреблеру, який відновлює вихідну послідовність на підставі співвідношення оберненого до того, яке використовувалось для скремблювання.

На ефективність скремблювання впливає багато факторів а саме: метод скремблювання , довжина фрагментів на які розбивається аудіо інформація, значення частот та їх кількість, відносно яких відбувається інверсія. Запропонований вище алгоритм скремлювання досить легкий у реалізації та може бути використаний для скремблювання аудіо інформації у кожному кадрі окремо. Недоліком даного алгоритму скремблювання є не надто високий рівень захисту аудіоінформації

Науковий керівник – к.т.н., с.н.с., Ю.І. Хлапонін