

ВИКОРИСТАННЯ ОБЕРНЕНИХ СИСТЕМ УПРАВЛІННЯ ДЛЯ ПЕРЕТВОРЕННЯ І ПЕРЕДАВАННЯ ДАНИХ

Постановка проблеми. Проблема конфіденційності передачі інформації та більш широка проблема захисту інформації стає все більш актуальною на ринку цивільних застосувань сфери комунікаційних технологій [1]. Прикладами можуть служити захист комерційної інформації в комп'ютерах та інформаційних мережах, безпека електронних платежів, захист від копіювання музичної, відео та іншої інформації, поширюваної по інформаційних мережах, інтернет-телефонія та ін. Типовою вимогою для схем шифрування стає можливість масового застосування та низька собівартість на одиницю "інформаційної" продукції. При вирішенні таких проблем захисту інформації можуть успішно застосовуватися засоби, які засновані на детермінованому хаосі, що породжується нелінійними динамічними системами.

Постановка задачі. Дослідити ефективність використання зворотних систем управління для перетворення і передачі інформації в порівнянні з відомими методами шифрування.

Розв'язання задачі. У даній роботі розглядається застосування хаотичних алгоритмів при передачі повідомлень по телекомунікаційних лініях, заснованих на динамічних системах [2] з використанням полів кінцевої потужності. Для цього використовувалися поля класів вичетов по модулю p . Встановлено, що з зростанням p робота алгоритму стає більш ефективнішою.

Для порівняння були реалізовані алгоритм А5, який використовує для отримання псевдовипадкової послідовності три лінійних регістра зсуву зі зворотним зв'язком, і алгоритм RC4, розроблений спеціально для потокових шифрів. А також були застосовані графічні та оціночні тести, які виявили статистичні властивості та деякі числові характеристики алгоритма шифрування.

В результаті експериментів було встановлено, що шифри, які використовують зворотні системи управління для перетворення і передачі інформації не поступаються за ефективністю відомим алгоритмам і мають високі швидкісні показники. Таким чином запропонований алгоритм має високий ступінь захисту і може бути використаний для безпечної передачі текстових графічних або звукових повідомлень через телекомунікаційні лінії або іншими способами.

Список літератури

1. Kyrychenko V.V., Lesina Ye.V. Application of dynamic systems for encoding data in telecommunication channels // Electronics & Control Systems. – 3 (53), 2017. – P. 11-16.
2. Кириченко В.В., Лесина Е.В. Об особенностях применения динамических систем в алгоритмах защиты данных // Проблемы автоматизации та управління. – 3 (59), 2017. – С. 26-32.