МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

ФІЗИКА, ЕЛЕКТРОНІКА, ЕЛЕКТРОТЕХНІКА

ФЕЕ :: 2018

МАТЕРІАЛИ
та програма

НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

(Суми, 05–09 лютого 2018 року)

Суми
Сумський державний університет
2018

Застосування адаптивного шифрування в автоматизованих системах

Бережна О.В., *доцент*; Качан Ю.Ю., *студентка*;
Шевченко М.С., *студент*; Гермес М.О., *студент*;
Сумський державний університет, м. Суми

Однією з актуальних задач при побудові інформаційних каналів в розподілених автоматизованих системах є забезпечення з мінімальними витратами достатнього рівня захисту інформації від несанкціонованого доступу при різних рівнях криптографічних загроз в тракті передачі інформації.

Аналіз показав, що забезпечення достатнього рівня захисту при мінімальних ресурсних витратах пов'язано із застосуванням адаптивної зміни параметрів алгоритмів шифрування, коли кожному набору адаптивних параметрів шифрування можна спрогнозувати криптостійкість запропонованого криптографічного перетворення.

В результаті досліджень виявилось доцільним при шифруванні застосовувати алгоритми подвійної перестановки, обрав в якості варіативних параметрів для адаптивного шифрування розмір шифрувальних таблиць, кількість рядків і стовпців в них, різні способи заповнення таблиць, такі, наприклад, як заповнення зигзагом, змійкою, по спіралі або іншим способом.

Для оцінки ефективності різних параметрів шифрування здійснювались початкова та поточна оцінки їх криптостійкості по відношенню до відомих видів таких криптографічних атак, як атаки методами «грубої сили» та лінійного методу криптоаналізу. При цьому стійким вважався алгоритм, який вимагав від противника для досягнення успіху значних ресурсів, значного обсягу перехоплених відкритих і зашифрованих повідомлень та значного часу розкриття, по завершенню якого захищена інформація втратить свою актуальність.

Застосування раціональних для програмної та апаратної реалізації алгоритмів шифрування методом подвійної перестановки та отриманих способів оцінки прогнозованої криптостійкості для кожного з варіантів при адаптивному шифруванні дозволяє забезпечити з мінімальними витратами достатній рівень захисту інформації від несанкціонованого доступу при різних рівнях криптографічних загроз в інформаційних каналах розподілених автоматизованих систем.