УДК 681.3.06
Карпінський В.М. - ст. гр. КСМ-22
Тернопільська академія народного господарства

ОГЛЯД СУЧАСНИХ МЕТОДІВ КРИПТОАНАЛІЗУ

Науковий керівник: викл. Коркішко Л.М.

Охорона від неавторизованого доступу є надзвичайно важливою для сучасних елементів комп'ютерних мереж, зокрема як Firewall-и, засоби VPN (Virtual Private Network – віртуальні комп'ютерні мережі), повторювачі, сервери чи бази даних. Згідно з прогнозом половина передаваної інформації в Інтернеті буде зашифрованою через найближчий рік чи два. Тому актуальною є задача криптографічного захисту інформації та опрацювання методів атак на криптографічні алгоритми і засоби чи іншими словами методів криптоаналізу.

Серед відомих методів криптоаналізу можна відзначити такі:

- на підставі аналізу анаграм, зокрема на відтворенні властивого чергування замінних знаків (літер, проміжків, цифр, а також крапок та ком) із застосуванням таблиць частоти появи вибраних знаків в текстах і програмах;
- повний аналіз даних (атаки, в яких використовується мала довжина блоку): атака словникова, припасовування шифрограм, знаходження правдоподібних слів;
- математичний аналіз, в тому числі і статистичний;
- спроб і помилок;
- диференційний аналіз;
- лінійний аналіз.

Останнім часом все ширше використовують методи криптоаналізу, що безпосередньо направлені на апаратну реалізацію криптографічних алгоритмів, а саме:

- аналіз енергоспоживання (звичайний і диференційний) пристрою;
- аналіз часових затримок у роботі пристрою;
- диференційний криптоаналіз помилок;
- аналіз електромагнітного випромінювання пристрою під час роботи.

В доповіді детально висвітлені останні сучасні методи криптоаналізу, подані переваги та недоліки кожного з них, а також особливості та перспективи їх застосування в конкретних галузях економіки.