УДК 621.391+681.3.06

М.М. Мандрона[1], О.І. Гарасимчук[2]

[1]Національний університет «Львівська політехніка», Львівський державний університет безпеки життєдіяльності, Львів
[2]Національний університет «Львівська політехніка», Львів

КЛАСИФІКАЦІЯ КРИПТОАНАЛІТИЧНИХ АТАК

У даній роботі проводиться аналіз найбільш поширених криптоаналітичних атак та показано способи їх реалізації. Розроблено класифікацію криптоаналітичних атак на основі принципу їх здійснення. Показано, що кожна з атак, має різну складність для криптоаналітика і потребує різної тривалості часу, обчислювальних та інших можливостей.

Ключові слова: *криптоаналітичні атаки, зловмисник, криптоаналітик, шифротекст, відкритий текст, ключі шифрування, генератори псевдовипадкових чисел.*

На даний час, проблема захисту інформаційних ресурсів набуває все більшого значення. Необхідність використання на підприємствах різних форм власності і у фінансових установах криптографічних систем зростає з кожним днем. Деякі криптографічні системи втрачають свою надійність, якщо їх невірно використовують. Безпека таких систем часто залежить від даних, які повинні бути відомі лише авторизованим користувачам, і які повинні бути важко вгадуванні для зловмисника. Ще одним недоліком криптографічних засобів є генератори випадкових чисел. На жаль, багато криптографічних програм не є надійним джерелом випадкових послідовностей, замість цього доводиться використовувати генератори псевдовипадкових чисел (ГПВЧ), які отримують на вхід потік даних від джерела з низькою ентропією і намагаються його перетворити в послідовність значень, які практично неможливо відрізнити від справжньої випадкової послідовності [1].

Більшість ГПВЧ побудовані на основі криптографічних алгоритмів шифрування, тобто, при успішній атаці можна розкрити багато криптографічних систем незалежно від того наскільки ретельно вони були спроектовані. Саме тому метою цієї роботи є, опис категорії і типів криптоаналітичних атак на алгоритми шифрування ГПВЧ, щоб у майбутньому побудувати абсолютно стійкий ГПВЧ.

Криптоаналіз полягає в отриманні доступу до відкритого тексту зашифрованого повідомлення. В ході успішного криптоаналітичного дослідження криптосистеми можуть бути знайдені не тільки відкритий текст, а й сам ключ.

Спроба криптоаналізу називається атакою. Успішна криптоаналітична атака зветься зломом, або розкриттям [2].

Здійснюючи атаку, криптоаналітик може ставити собі за мету вирішення наступних завдань:

1) отримання відкритого тексту із зашифрованого;

2) обчислення ключа шифрування.

Атаки на алгоритми шифрування прийнято класифікувати в залежності від набору інформації, який зловмисник має перед здійсненням своєї атаки. Перш за все, криптоаналітичних атаки можна розділити на дві категорії: пасивні та активні атаки [2-3].

В результаті проведеного аналізу літературних джерел, нами була запропонована класифікація найбільш відомих криптоаналітичних атак, які проаналізовані, у порядку зростання вразливості інформації, яка є доступною для криптоаналітика або в порядку спадання рівня складності для нього [2].

Запропонована нами класифікація криптоаналітичних атак, дозволяє чітко визначити напрямки подальших досліджень щодо розробки та побудови ефективних і надійних генераторів псевдовипадкових чисел.

Список літератури

1. Фергюсон Н. Практическая криптография / Н. Фергюсон, Б. Шнайдер – М.: Изд-во «Вильямс», 2005. – 432 с.

2. Криптоаналитические атаки. [Електронний ресурс]– Режим доступу до ресурсу.: http://chhm.net/index.php?articles=165

3. Юдін О.К. Захист інформації в мережах передачі даних / О.К. Юдін, О.Г. Корченко, Г.Ф. Конахович – К.: Вид-во «DIRECTLINE», 2009. — 714 с.