УДК 004.056

Є.В. Мелешко[1]
Кіровоградський національний технічний університет

Метод визначення джерела витоку таємної державної інформації на основі стеганографічних маркерів

На сьогоднішній день актуальною є задача захисту секретної й приватної інформації від витоку й незаконного використання або поширення. В умовах інформаційної війни велике значення має задача захисту локальних мереж державних організацій від злому. Навіть якщо локальна мережа добре захищена криптографічними алгоритмами й адекватною політикою безпеки, найслабшим місцем, як і раніше, є людський фактор.

Для того, щоб, як мінімум, встановити особу зловмисника при виникненні витоку секретної інформації, а, як максимум, запобігти протиправним діям нечесних співробітників, у даній роботі пропонується вбудовувати у файли невидимі маркери методом стеганографії. Дані маркери повинні містити ідентифікатор співробітника – одержувача таємної інформації, дату і час створення маркера та ідентифікатор співробітника – відправника інформації.

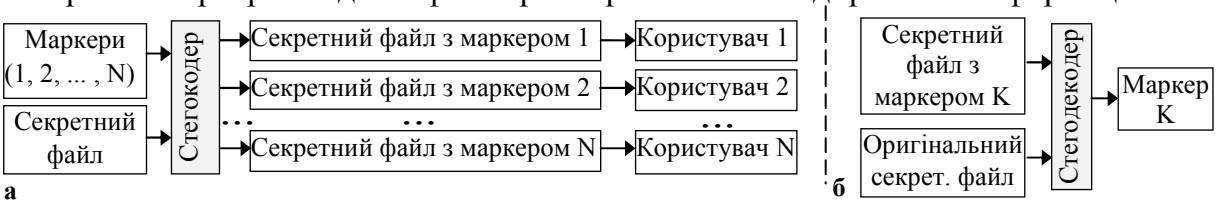

Рисунок 1 – Структурні схеми вбудовування (а) та вилучення (б) стегомаркерів

Рисунок 2 – Формат стегомаркера

При вилученні маркера з файлу може виникнути 3 варіанти: 1) маркер цілий та вказує на порушника, 2) маркер пошкоджений чи знищений, 3) маркер замінений та містить ідентифікатор невинного співробітника. Випадки (1) та (3) програмно розрізнити неможливо, тому реальні обставини повинне встановлювати слідство. Випадок (2) може виникнути при так званих *атаках змовою* на стегосистему – коли 2 чи більше користувачів, порівнявши свої файли, визначили розташування маркерів та пошкодили їх. Є різні способи протистояння атакам змовою (наприклад, [1], [2]), але всі вони базуються на наступній ідеї: треба вбудувати маркери так, щоб $M_A \cap M_B \neq \emptyset$ та $M_A \cap M_B = M_{AB}$, де M_A – множина бітів, що містять маркер A; M_B – множина бітів, що містять маркер B; M_{AB} – множина бітів, зі спільною інформацією для маркерів A та B. Тоді у разі змови між співробітниками A та B, вони зможуть визначити та змінити $M_A \Delta M_B$, але не зможуть визначити частину маркера M_{AB}, яка буде вказувати на них обох.

Список літератури

1. Соловьёв Т.М. Множества идентификационных номеров, устойчивые к атаке сговором / Т.М. Соловьёв, Р.И. Черняк // Прикладная дискретная математика. – Томск: НИТГУ. – 2012 – Вып. № 1. – с. 60-68.

2. Wade Trappe, Min Wu, Z. Jane Wang, K. J. Ray Liu Anti-collusion Fingerprinting for Multimedia // IEEE Transactions on signal processing, VOL. 51, NO. 4, APRIL 2003. – P. 1069-1087.

[1] кандидат технічних наук, доцент кафедри програмного забезпечення