УДК 004.056.55:621.391 (043.2)

В.О. Гнатюк к.т.н., доц., О.О. Матвійчук-Юдін
(Національний авіаційний університет, Україна)

Оптимізація стеганографічних методів для захисту службових даних

Окреслено сучасні стеганографічні методи, що спрямовані на забезпечення конфіденційності службових даних. Враховуючи актуальні загрози в інформаційній безпеці, запропоновано оптимізовані підходи для покращення стеганографічних алгоритмів, які використовуються для захисту інформації. Розглянуто підходи підвищення стійкості даних методів до різних типів атак, зменшення впливу на якість носія інформації та підвищення ефективності алгоритмів у контексті обробки великих обсягів даних.

Наразі відбувається стрімкий розвиток науки та техніки в різних сферах діяльності людини. Цей процес не оминув і глобальний цифровий інформаційний простір. Його динаміка обумовлена такими чинниками:

1. Створенням новітніх технологій для обміну інформаційними ресурсами, зокрема за допомогою бездротових засобів.
2. Впровадженням нових підходів до моделювання алгоритмів функціонування інформаційно-комунікаційних систем.
3. Зростанням попиту на використання цифрових каналів передачі даних у приватному та державному секторах.
4. Збільшенням обсягів інформації, необхідної для належного функціонування різних систем цивільного та спеціального призначення.

Забезпечення інформаційної безпеки державних інформаційних ресурсів є вкрай важливим завданням. Такі ресурси належать державі, і їх охорона регулюється відповідними правовими нормами [1]. Потреба у гарантуванні конфіденційності, цілісності та доступності державної інформації викликана наявністю можливих загроз. Під загрозою мається на увазі ризик порушення ключових аспектів безпеки [2]. Якщо загроза здійснюється навмисно зловмисником, вона перетворюється на цілеспрямовану атаку.

Виокремимо фактори, що зумовлюють потребу у підвищенні рівня захисту державних інформаційних ресурсів:

- виникнення новітніх високошвидкісних технічних засобів, здатних здійснювати несанкціоновані атаки на інформаційні системи;
- використання бездротових технологій при побудові каналів передачі даних;
- використання під час передачі інформаційних ресурсів стандартизованого програмного забезпечення, що знаходиться у вільному доступі.

Зі зростанням загроз інформаційній безпеці зростає і значення державних інформаційних ресурсів. Важливо зазначити, що ці ресурси використовуються для задоволення потреб держави. В процесі створення державних баз даних задіяно велику кількість фахівців та матеріальних ресурсів. На основі виокремленої інформації ухвалюються рішення для державних структур,

міністерств і силових органів. Будь-яка втрата або підміна частини такої інформації може завдати серйозної шкоди державі та підірвати її авторитет як на внутрішньому, так і на міжнародному рівнях.

Актуальні сучасні напрямки для забезпечення безпеки державного інформаційного ресурсу можна виділити наступні: рис.1.

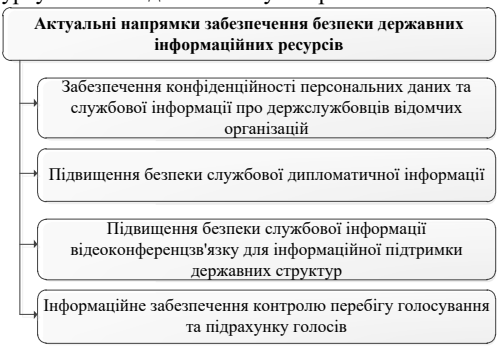

Рис.1. Напрямки забезпечення безпеки державного інформаційного ресурсу.

Різноманітність стеганографічних методів потребує їхньої систематизації. Втім, побудова стеганосистеми має враховувати наступні положення:

- стеганосистема повинна мати складність обчислення реалізації (тобто, прийнятну кількість арифметико-логічних дій для вбудовування повідомлення у стеганоконтейнер та вилучення з нього інформації);
- при виявленні факту існування вбудованого повідомлення порушник не повинен мати можливості дістати це повідомлення;
- методи приховування мають забезпечити цілісність вбудованого повідомлення для одержувача;
- повинна забезпечуватись необхідна пропускна здатність стеганоконтейнера;
- потенційний порушник має повне уявлення про існування і функціонування стеганосистеми, єдине, що йому не відоме – ключ, за допомогою якого можна визначити факт присутності повідомлення та його зміст;
- порушник має бути позбавлений будь-яких (технічних та будь-яких інших) переваг.

На рисунку 2 показано типову структурну схему стеганографічної системи.

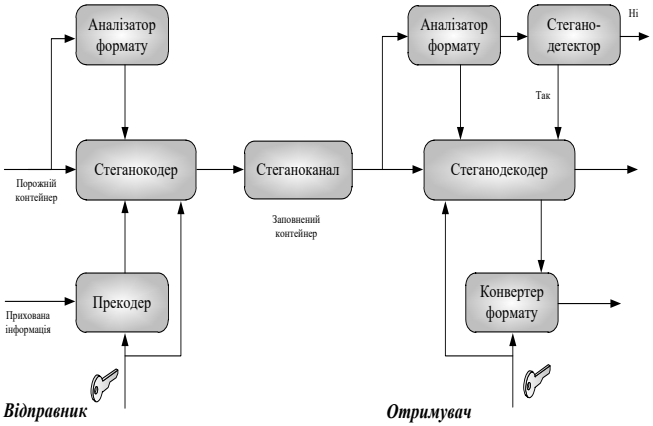

Рис. 2. Структурна схема типової стеганографічної системи з використанням попередньої обробки повідомлення

Основними поняттями у стеганографії є повідомлення та контейнер. Повідомлення $m \in M$ - певна закрита інформація, яку необхідно приховати. $M = \{m_1, m_2, ..., m_n\}$ - множина всіх повідомлень.

Контейнер $c \in C$ - множина відкритих даних, яка використовується для вбудовування закритої інформації. $C = \{c_1, c_2, ..., c_q\}$ - множина всіх контейнерів, причому $q >> n$.

Порожній контейнер – такий контейнер c, який не містить закритої інформації. Заповнений контейнер – такий контейнер c, який містить приховану інформацію (c_m). Заповнений контейнер, який не має візуально відрізнятися від порожнього.

Контейнери бувають двох типів: потокові та фіксовані [3]. Потокові контейнери – це послідовність бітів, яка постійно змінюється. Повідомлення вбудовується у нього в реальному режимі часу, тому заздалегідь невідомо, чи вистачить розміру даного контейнера для передачі повідомлення повністю. Фіксовані ж контейнери мають фіксований розмір, тому є можливість обрати оптимальній контейнер для передачі повідомлення. Розмір контейнера повинен, принаймні, у декілька разів перевищувати розмір повідомлення, і, чим більше дане співвідношення, тим надійніше приховане повідомлення. Для підвищення рівня захищеності секретної інформації повідомлення можна попередньо зашифрувати стійким криптографічним алгоритмом. Також часто використовується завадостійке кодування.

Процес звичайного стеганографічного перетворення описується наступними залежностями:

$$E : C \times M \to S; \qquad (1)$$

$$D : \ S \to M; \qquad (2)$$

де

$S = \{(c_1, m_1), (c_2, m_2), ..., (c_q, m_q)\} = \{s_1, s_2, ..., s_q\}$ - множина заповнених контейнерів (стеганограм).

Залежність (1) описує процес приховування інформації, залежність (2) – витягування прихованої інформації. Однією із обов'язкових умов при цьому є відсутність «перетину», тобто, якщо $m_a \neq m_b$ (причому $m_a, m_b \in M$, а $(c_a, m_a), (c_b, m_b) \in S$), то $E(c_a, m_a) \cap E(c_b, m_b) = \varnothing$.

Тож в загальному випадку стеганосистема – це сукупність $\sum (C, M, S, E, D)$ - контейнерів, повідомлень та перетворень, що їх зв'язують. Майже завжди контейнери C обираються таким чином, щоб заповнений контейнер майже не відрізнявся від порожнього контейнера. Стеганосистема може вважатися надійною, коли $sim\,[c, E(c, m)] = 1$ (де sim – функція подібності). Контейнер може обиратися двома способами: довільно (сурогатний метод) та підбором найбільш придатного у конкретному випадку контейнера, який зміниться найменше при перетворенні. Умова вибору найбільш придатного контейнеру описується наступним виразом::

$$c = \max sim[x, E(x, m)] \qquad (3)$$

Тут sim – функція подібності; E – пряме стеганографічне перетворення, c – стеганографічний контейнер.

В будь-якому випадку пряме та зворотне перетворення (E та D) мають відповідати одне одному та підлягати умові, що незначне викривлення контейнера (на величину δ) не має призводити до викривлення прихованої інформації (залежність (4)):

$$E(c, m) \approx E(c + \delta, m) \quad \text{або}$$
$$D[E(c, m)] \approx D[E(c + \delta, m)] = m \qquad (4)$$

Для зрівняння та аналізу існуючих стеганографічних систем необхідно сформулювати систему показників ефективності стеганографічних перетворень.

Це дозволить виявити такі методи, які дозволять оптимально вирішити завдання підвищення безпеки державного інформаційного ресурсу.

Висновок: В результаті дослідження, можна констатувати важливість забезпечення конфіденційності службової інформації для державних структур і відомчих організацій. Підвищена значимість такої інформації для функціонування інформаційних систем у державних інтересах, а також зростання загроз для її конфіденційності, підкреслюють необхідність надійного захисту даних. Запропонований підхід, що передбачає використання методів цифрової стеганографії для прихованої передачі службових даних, демонструє потенціал для підвищення безпеки інформації. Розглянуто основні принципи функціонування стеганографічних систем, що підтверджує їх ефективність як інструменту захисту від несанкціонованого доступу та розкриття. Використання стеганографічних методів може суттєво посилити заходи з безпеки службової інформації, сприяючи таким чином більшій стабільності та захищеності державних інформаційних ресурсів..

Список літератури

1. O.Y. Lavrynenko, D.I. Bakhtiyarov, G.F. Konakhovich analyzed the effectiveness of the voice identification system based on MFCC and GMM-SVM under the influence of interference in the communication channel. - Scientific technologies, 2023. Vol. 59. No. 3. p. 289.

2. V Barannik, O Ignatyev, G Pris, Y Sidchenko A Method of Encoding Video Information to Increase its Reliability in an Information and Telecommunications Network . - 2023 IEEE 5th International Conference on Advanced, 2023. pp. 203-206.

3. Конахович Г.Ф., Прогонов Д.О., Пузиренко О.Ю. Комп'ютерна стеганографічна обробка та аналіз мультимедійних даних [підручник] – К.: «Центр учбової літератури», 2018. 558 с.