

АНОТАЦІЯ

Шеханін К.Ю. Розробка та аналіз стеганографічних методів приховування даних в структуру файлових систем. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття ступеня доктора філософії за спеціальністю 125 «Кібербезпека» (Галузь знань 12 – «Інформаційні технології»). – Харківський національний університет імені В. Н. Каразіна Міністерства освіти і науки України, Харків, 2021.

Дисертація присвячена розробці та удосконаленню стеганографічних методів приховування інформації у структуру файлової системи шляхом перемішування кластерів. Розробці способів оцінки зазначених методів та можливого способу використання.

Метою дисертаційної роботи є підвищення пропускну здатності кластерних стеганосистем при забезпеченні необхідної стійкості до несанкціонованого детектування прихованої інформації.

У першому розділі дисертації (*Дослідження технологій носіїв інформації та властивостей файлових систем*) виконано аналіз актуального стану розвитку технологій фізичних носіїв інформації. Зокрема, проаналізовані такі технології як HDD та SSD. Надано прогноз щодо розвитку технологій носіїв інформації. Також проаналізовані розповсюджені файлові системи, виконано їх порівняльний аналіз. За результатами аналізу обрано файлову систему для подальшого дослідження. Вирішена *перша часткова задача дослідження*: дослідження сучасних і перспективних методів зберігання інформації, властивостей фізичних носіїв та типів файлових систем, аналіз існуючих методів стеганографічного приховування у структурі файлових систем.

У другому розділі (*Розробка методу підвищення пропускної здатності кластерних стеганосистем та дослідження властивостей*) детально проаналізована файлова система FAT32, як еталона система із сімейства кластерних файлових систем. Також досліджені та проаналізовані властивості структури файлової системи що сприяють приховування повідомлення у структуру файлової системи. Надано математичну модель методу приховування інформації шляхом перемішування кластерів покриваючих файлів. Вирішено *другу часткову задачу дослідження*: розробка методу підвищення пропускної здатності кластерних стеганосистем. *Вперше отримано* метод підвищення пропускної здатності кластерних стеганосистем на основі урахування додаткової залежності місць розміщення кластерів у межах одного покриваючого файлу системи.

У третьому розділі (*Аналіз методів приховування інформації та удосконалення математичної моделі оцінки основних параметрів кластерних стеганосистем*) проаналізовано досліджувані методи на можливий розмір приховуваного повідомлення у залежності від різних вихідних параметрів. Отримано формули, за якими можливо оцінити максимально можливий розмір стеганограми у залежності від ключових параметрів (кількість, порядок та розмір покриваючих файлів). Наведено графіки, які наочно демонструють залежність розміру стеганограми від ключових параметрів методів.

Також оцінено рівень захищеності прихованого повідомлення до детектування, шляхом аналізу середнього рівня фрагментації файлової системи та фрагментації кожного покриваючого файлу. Результати оцінки отримано шляхом статистичного аналізу рівня фрагментації комп'ютерних систем із лабораторій Харківського національного університету імені В. Н. Каразіна. За результатами статистичного аналізу надано зліпок файлових систем з точки зору рівня фрагментації, найбільш фрагментованих типів файлів та способу використання комп'ютерних систем. За результатами даного аналізу надано дані щодо можливого розміру приховуваного

повідомлення у такий спосіб, щоб рівень фрагментації покриваючих файлів був у межах середнього рівня файлової системи.

У даному розділі була надана оцінка часових параметрів методів приховування повідомлення, виконана за допомогою розробленої програми «SteganoFAT». Дана оцінка залежить від технічних властивостей комп'ютерної системи та фізичного носія інформації, отже було виведено рівняння загальної обчислювальної складності у залежності від кількості покриваючих файлів та кількості стеганоблоків. Загальний час на приховування залежить від кількості переміщень зчитуваючої головки, кількості зчитувань та записів даних у кластери файлів. Результатом даного дослідження стали методи приховування інформації із послідовним та почерговим записом даних до оперативної пам'яті для базового методу (ПЗОП, ПчЗОП-I/II/III) та відповідні методи для модифікованого методу приховування інформації (ПЗОПм, ПчЗОПм-I/II/III). Для кожного методу теоретично отримано оцінку обчислювальної складності. Найоптимальнішим за часовими показниками та рівнем фрагментації є розроблений у даній дисертаційній роботі метод ПчЗОП-II (почергове завантаження даних із кластерів до оперативної пам'яті із послідовним впорядкування лише задіяних у повідомленні кластерів).

Виконано *третю часткову задачу дослідження*: удосконалено математичну модель оцінки основних параметрів кластерних стеганосистем за рахунок додаткового урахування елементів конфігурації стеганосистеми, що дозволяє більш повно оцінити пропускну здатність системи.

Також вирішено *четверту часткову задачу дослідження*: удосконалення методу приховування інформації у структурі кластерних стеганосистем. Удосконалення полягає у раціональному використуванні оперативної пам'яті. Також інше удосконалення полягає у спеціальному розрахунку таблиць перестановок таким чином, щоб зменшити кількість переміщуваних кластерів. Це дозволило значно зменшити час на приховування повідомлення.

Отримано *другий науково-обґрунтований результат*: удосконалено математичну модель оцінки основних параметрів кластерних стеганосистем за рахунок додаткового урахування елементів конфігурації стеганосистеми, що дозволяє більш повно оцінити пропускну здатність системи.

Та отримано *третій науково-обґрунтований результат*: удосконалено метод приховування інформації у структуру кластерних стеганосистем за рахунок генерації відповідного набору перестановок кластерів, що дозволяє зменшити час приховування інформації.

У четвертому розділі (*Розробка програмної реалізації методів приховування інформації*) розроблено програмну симуляцію, що наочно дозволяє продемонструвати принцип роботи методів приховування інформації у структуру файлової системи шляхом перемішування кластерів покриваючих файлів та емпірично оцінити ефективність способів приховування (ПЗОП, ПчЗОП-I/II/III). Надано повний опис розробленої програмної реалізації із посиланням на відкритий репозиторій, описано алгоритмічні особливості методів приховування інформації та надано фрагменти коду функціоналу приховування повідомлення.

За допомогою розробленої програми було отримано емпіричну оцінку обчислювальної складності стосовно кожного методу приховування інформації, кожного способу. За результатами порівняння теоретично отриманої та емпірично розрахованої оцінки обчислювальної складності виявлено, що способи модифікованого методу у даній програмній реалізації мають гіршу обчислювальну складність ніж теоретично очікувалось. Та було описано вдосконалений алгоритм роботи модифікованого методу, який дозволяє зменшити рівень обчислювальної складності.

Була виконана *п'ята часткова задача дослідження*: розробка програмної реалізації запропонованих методів та проведення експериментальних досліджень.

У п'ятому розділі (*Напрямки використання методів приховування інформації*) описані можливі системи що використовують методи приховування інформації у структуру файлової системи. Такими системами є:

- система прихованого збереження даних;
- система прихованої передачі даних;
- система верифікації фізичного носія інформації чи файлів, що збережено на носії.

По кожній системі надано опис із аналізом ефективності такої системи у залежності від конфігураційних параметрів.

Також надано опис розповсюджених програмних реалізацій що імплементують описані вище системи використання методів приховування інформації. Зроблено порівняльний аналіз та надано оцінку відомих програмних реалізацій як би вони також використовували розроблені у даній роботі методи приховування інформації, як компонент у свої алгоритмах. Надано висновок, що описані методи дозволяють значно розширити функціонал реалізованих програм та/або методи можуть надати альтернативу, у разі коли внутрішні інструменти програм використовувати недоречно.

Ключові слова: метод приховування інформації, стеганографічні методи, файлова система, носій інформації, FAT, статистичний аналіз, структура файлової системи, пропускна здатність, обчислювальна складність, програма симуляція, StarForce.