# РЕФЕРАТ

**Актуальність**. Сьогодні нерідко виникає необхідність передати конфіденційне повідомлення невеликого обсягу, при цьому використання складних криптографічних систем по ряду причин важко. Однією з таких причин є неможливість використання надійних продуктів, які, як правило, є комерційними і для рядового користувача комп'ютера недоступні. У сучасному інформаційному суспільстві велика кількість послуг забезпечується за допомогою комп'ютерних мереж та інформаційних технологій. Інформація, що представлена в цифровому вигляді, має бути надійно захищена від багатьох загроз: несанкціонованого доступу та використання, знищення, підробки, витоку, порушення ліцензійних угод, відмови від авторства та ін. Захист інформації є вкрай важливим як в комерційній, так і в державній сферах. Законом України "Про основи національної безпеки України" від 19.06.2003 р. серед загроз національним інтересам і безпеці України в інформаційній сфері зазначені: комп'ютерні тероризм та злочинність; розголошення таємної чи конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави; маніпулювання суспільною свідомістю, зокрема, шляхом поширення недостовірної інформації. Таким чином, питання розроблення ефективних методів захисту цифрової інформації, зокрема методів комп'ютерної стеганографії та стеганоаналізу, актуальні та мають важливе значення для держави й суспільства.

**Зв'язок роботи з науковими програмами, планами, темами.** Робота виконана на філії кафедри автоматизованих систем обробки інформації та управління в Інституті кібернетики ім. В.М. Глушкова НАН України в рамках науково-дослідної теми «Розробити оптимальні за точністю та швидкодією алгоритми розв'язання задач: інтегрування швидкоосцилюючих функцій, цифрової обробки сигналів та зображень, дистанційного моніторингу об'єктів, інформаційної безпеки» (номер державної реєстрації: 0114U000357).

**Мета і завдання дослідження** – аналіз стійких до типових операцій обробки методів комп'ютерної стеганографії та методів стеганоаналізу для виявлення найбільш поширених графічних стеганоконтейнерів.

Для досягнення мети необхідно виконати наступні **завдання**:

- виконати огляд існуючих стеганографічних алгоритмів;
- здійснити порівняльний аналіз різних стеганографічних алгоритмів;
- запропонувати метод підвищення стеганостійкості;
- визначити ефективність створеного рішення.
- виконати аналіз отриманих результатів.

**Об'єкт дослідження** – процес захисту інформації, вкрапленої в графічний контейнер.

**Предмет дослідження** – методи та алгоритми комп'ютерної стеганографії і стеганоаналізу для зображень.

**Методи дослідження**, застосовані у даній роботі, базуються на стеганографічних алгоритмах.

**Наукова новизна одержаних результатів** полягає у наступному.

Запропоновано алгоритм комп'ютерної стеганографії для цифрових контейнерів у вигляді зображення, що відрізняється підвищеною ефективністю, який дозволяє здійснювати операції з нанесення тексту на зображення.

**Публікації.** Матеріали роботи представлено у двох наукових статтях на міжнародних конференціях ISCIENCE 2017 та ISCIENCE 2018, Переяслав-Хмельницький, Україна.

СТЕГАНОГРАФІЯ, ЗАХИСТ ІНФОРМАЦІЇ, СТЕГАНОКОНТЕЙНЕР, ВКРАПЛЕННЯ ІНФОРМАЦІЇ, СТЕГАНОАНАЛІЗ