Кожен метод захисту має свої переваги і недоліки, а тому не є ідеальним. При його використанні слід враховувати не тільки суто програмно-технічні аспекти, а й економічні чинники. Впроваджувати ці технології слід з урахуванням необхідного рівня захисту, який повинен бути сумірним з вартістю програм, що захищаються. При цьому можна піти як по шляху застосування вже готових професійних рішень, так і за рахунок розробки власних алгоритмів перевірки прав на використання програм, що захищаються.

## Список літератури

1. Касперски К. Техника и философия хакерских атак – записки мыща / Касперски К. – М.: СОЛОН-Пресс, 2004. – 272с.
2. Касперски К. Искусство дизассемблирования / Касперски К., Рокко Е. – СПб.: БХВ-Перербург, 2008. – 896 с.
3. Панов А.С. Реверсинг и защита программ от взлома / Панов А.С. – СП.: БХВ – Петербург, 2006. – 256 с.

УДК 004.7

**П.С. Молдавський**
Науковий керівник – Мелешко Є.В., канд. техн. наук, доцент
*Кіровоградський національний технічний університет*

# Розробка програмного забезпечення вбудовування прихованих маркерів у файли для відстежування їх поширення по комп'ютерній мережі

В останні десятиліття все більш важливим стає як поняття інформації, так і сама інформація. А з розвитком комп’ютерних технологій – цифрова інформація. Цифрові фотографії, відео- та аудіоматеріали, звичайна текстова інформація, відкритий програмний код, чи, власне, самі програмні засоби – для певних осіб або організацій можуть мати чимале значення, а тому і вартість, що може досягати дев’ятизначних сум, або навіть коштувати людського життя.

В зв’язку з тенденцією стрімкого розвитку комп’ютерних мереж – як локальних, так і глобальних, – все більшого значення набуває захист цифрових даних від несанкціонованого доступу, використання та поширення. Адже більшість інформації в наш час є продуктом діяльності людського розуму та інтелекту, і потребує захисту прав власності. Одним із способів захисту інформації від незаконного використання, тиражування та розповсюдження є обмеження її використання, коли доступ до неї може мати тільки певна кількість осіб, або й такий варіант, коли доступ надається всім, але не дозволяється копіювати її та використовувати у корисливих – часто комерційних, – цілях. Для запобігання випадків незаконного розповсюдження інформації з обмеженим доступом та виявлення правопорушників, досить доречно відстежувати її поширення.

Одним з методів відстежування є вбудовування у файли, що містять важливу інформацію, прихованих маркерів. За допомогою таких маркерів, в залежності від реалізації, можна здійснювати три способи захисту – окремо чи комплексно: 1) вбудовування певної зашифрованої інформації у файли; 2) приховування самого факту присутності вбудованої інформації; 3) локалізація поширення інформації.

Перший спосіб може забезпечити використання зашифрованої інформації тільки тими, хто має права доступу до неї. Другий спосіб приховує сам факт наявності певної

інформації та запобігає її виявленню і розшифруванню користувачами, що не мають прав доступу до неї. Третій же спосіб дозволяє відстежити шлях розповсюдження файлу в комп’ютерній мережі, та визначити, хто став джерелом, тобто початком його поширення.

Метою роботи є розробка програмного забезпечення вбудовування прихованих маркерів у файли для відстежування їх поширення по комп’ютерній мережі.

Методи дослідження базуються на теорії алгоритмів, теорії зв’язку і телетрафіку, використанні булевої алгебри та чисельних методів, а також математичного апарату теорії захисту інформації, зокрема основ криптографії та стеганографії.

Наукова новизна результатів, отриманих автором, полягає у наступному:

1. Розроблено вдосконалений метод шифрування даних та вбудовування їх у файли у вигляді прихованих маркерів.
2. Розроблено вдосконалений метод відстежування джерел та шляхів несанкціонованого поширення файлів по комп'ютерній мережі.
3. Розроблено вітчизняний продукт системи відстежування поширення інформації в комп’ютерних мережах на основі обміну даними за допомогою клієнт-серверних технологій та алгоритмів самомодифікації.

Практична значимість роботи забезпечується можливістю використання розробленого програмного забезпечення досить широким колом користувачів. Ними можуть бути як окремі особи, що бажають захистити продукт своєї інтелектуальної діяльності від несанкціонованого використання будь-ким, так і організації і установи, які піклуються про безпечність обміну важливою інформацією. Програмний продукт було вирішено будувати на основі нових програмних рішень – в середовищі Microsoft Visual Studio 2010-2012, з використанням технологій Microsoft .NET Framework, – що забезпечує сумісність та широку функціональність в сучасних ОС сімейства Windows.

## Список літератури

1. Стеганография, цифровые водяные знаки и стеганоанализ: Монография / [А. В. Аграновский, А. В. Балакин, В. Г. Грибунин, С. А. Сапожников]. – М.: Вузовская книга, 2009. – 220 с.
2. Корнышев Ю.Н., Пшеничников А.П., Харкевич А.Д. Теория телетрафика: учебник для вузов. – М.: издательство «Радио и связь», 1996г, 272 с.
3. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. / Василенко О.Н. – М.: МЦНМО, 2003.–328 с.

УДК 004.051 (043.2)

**К.І. Пулеко**
Науковий керівник – Гнатюк С.О., канд. техн. наук, доцент
*Національний авіаційний університет*

# Застосування методу кластеризованих ранжировок при експертній оцінці рішень в галузі інформаційної безпеки

У галузі інформаційної безпеки особам, що приймають рішення досить часто доводиться здійснювати вибір між тими чи іншими технічними і організаційними рішеннями, які мають приблизно однакові технічні і вартісні показники, або навпаки, різко відрізняються за технічними показниками чи вартістю. У цьому випадку математична задача оптимізації прийняття рішення стає векторною і