У даній роботі досліджуються методи стеганографічного захисту інформації, засновані на використанні складних дискретних сигналів і технології прямого розширення спектра. На прикладі вбудовування інформації в контейнер-зображення показане можливість організації каналу потайливої передачі даних (стеганоканала), досліджена ефективність стеганографічного перетворення з погляду забезпечуваної стійкості, пропускної здатності й величини внесених перекручувань у контейнер-зображення.

У результаті проведених досліджень показано, що використання в стеганографічних цілях прямого розширення спектра дискретних сигналів дозволяє здійснити потайливе вбудовування інформаційних повідомлень у нерухливі зображення. Завдання добування повідомлення на прийомній стороні стеганосистеми еквівалентні завданню виявлення інформації із суміші корисного сигналу й перешкоди в широкосмуговій системі зв'язку.

У ході досліджень виявлені наступні властивості стеганографічних систем з розширенням спектра дискретних сигналів: імовірність правильного добування убудованих даних залежить від величини внесених перекручувань, що у свою чергу залежить від забезпечуваної пропускної здатності стеганоканалу. Інакше кажучи, практична побудова стеганосистеми сполучена з пошуком компромісу між величиною внесених перекручувань, імовірністю правильно добування повідомлення на прийомній стороні й забезпечуваній пропускній здатності. Крім того, у ході досліджень встановлено, що ймовірність правильного добування убудованих даних безпосередньо залежить від статистичних властивостей використовуваного контейнера-зображення.

Перспективним напрямком подальших досліджень, є використання більших ансамблів слабокорельованих дискретних сигналів для побудови стеганосистем із прямим розширенням спектра. Це дозволить із однієї сторони без значного підвищення внесених перекручувань у контейнер-зображення істотно підвищити пропускну здатність стеганоканалу. З іншого боку, за рахунок адаптивного формування (вибору) дискретних сигналів за критерієм мінімізації коефіцієнта кореляції з контейнером зображенням це дозволить істотно знизити ймовірність помилкового добування убудованих даних.

Список літератури

1. Конахович Г. Ф., Пузыренко А. Ю. Компьютерная стеганография. Теория и практика. – К.: «МК-Пресс», 2006. – 288 с.
2. Горбенко И.Д., Стасев Ю.В. Анализ производных ортогональных систем сигналов // Радиотехника. – 1989. – № 9. – С. 16 – 18.
3. Стасев Ю.В., Кузнецов А.А. та ін. Формирование больших ансамблей дискретных сигналов с использованием избыточных кодов // Збірник наукових праць ХУ ПС.–Харків:ХУПС.–2008.–№2(17). – С. 102-109.
4. Стасєв Ю.В. Основи теорії побудови сигналів. – Х.: ХВУ, 1999. – 87с.

УДК 004.4

М.В. Старіцин
Науковий керівник – Конопліцька О.К., асистент
Кіровоградський національний технічний університет

Програмне забезпечення системи управління файлами в ОС Windows на основі технології EFS

Encrypting File System (EFS) – Шифрована файлова система – це базова технологія що дозволяє управляти файлами, які зберігаються на томах з файловою системою NTFS, з метою збереження конфіденційності. Файлова система EFS

інтегрована в NTFS, відрізняється простотою керування й стійкістю до атак. Користувачі можуть вибирати файли, якими потрібно управляти з метою збереження конфіденційності, але розшифровувати файли вручну перед використанням не потрібно – можна просто відкрити файл і змінити їх, як звичайно. Файли, управління якими реалізовано з метою збереження конфіденційності, будуть захищені навіть у тому випадку, якщо зловмисник одержить фізичний доступ до комп'ютера. Крім того, навіть користувачі, що мають право на доступ до комп'ютера (наприклад, адміністратори), не мають доступу до файлів, якими потрібно управляти з метою збереження конфіденційності, за допомогою файлової системи EFS іншими користувачами. Проте файлова система EFS підтримує призначені агенти відновлення. При їхньому правильному настроюванні можна гарантувати відновлення даних при необхідності. Файлова система EFS в Windows 7/8 і Windows Server 2012 була вдосконалена за рахунок наступних основних можливостей: підтримка зберігання ключів шифрування на смарт-картах; централізоване адміністрування політик захисту файлової системи EFS; шифрування клієнтського кеша (автономних файлів) для кожного користувача; шифрування системного файлу підкачування; спрощення відновлення ключів шифрування за допомогою майстра повторного створення ключів.

Таким чином, виходячи з вищеперерахованого, розробка програмного забезпечення системи управління файлами в ОС Windows на основі технології EFS є актуальною задачею.

Список літератури

1. Галатенко В.А. Основы информационной безопасности . М.: ИНТУИТ.РУ "Интернет-университет информационных технологий", 2003.
2. Горбатов В.С., Полянская О.Ю. Доверенные центры как звено системы обеспечения безопасности корпоративных информационных ресурсов .Информационный бюллетень Jet Info, № 11 (78), 1999.
3. Столлингс В. Криптография и защита сетей: принципы и практика (2-е издание). / Пер. с англ. — М.: Издательский дом «Вильямс», 2001.

УДК 004.056(043.2)

Д.В. Таратайко
Науковий керівник – Пепа Ю.В., канд. техн. наук, доцент
Національний авіаційний університет

Технологія застосування електронного цифрового підпису на державному підприємстві “Укрзалізниця”

Вступ. Захист власної інформації, а також її основних властивостей – цілісності, доступності та конфіденційності, для державних та комерційних підприємств, являє собою першочергову задачу, щодо зниження ризиків від можливих інцидентів інформаційної безпеки [1]. Важливе місце в системі заходів захисту інформації займає використання систем електронного цифрового підпису (ЕЦП) [1]. Послуги ЕЦП надаються центрами сертифікації ключів, які здійснюють свою діяльність в сфері електронного документообігу. Електронний підпис застосовується органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями всіх форм власності, іншими суб’єктами господарської діяльності та фізичними особами.