На правах рукопису

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Одеська національна академія харчових технологій
Навчально-науковий інститут холоду,
кріотехнологій та екоенергетики
Факультет інформаційних технологій та кібербезпеки

XVI Всеукраїнська науково-технічна конференція молодих вчених, аспірантів та студентів

“СТАН, ДОСЯГНЕННЯ І ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ”

Матеріали конференції

Одеса
25–26 квітня 2016 р.

Стан, досягнення і перспективи інформаційних систем і технологій / Матеріали XVI Всеукраїнської науково-технічної конференції молодих вчених, аспірантів та студентів. Одеса, 25–26 квітня 2016 р. - Одеса, Видавництво ОНАХТ, 2016 р. - 176 с.

Збірник включає матеріали доповідей її учасників, які об'єднані по секціях кафедр: комп'ютерної інженерії (КІ), інформаційних технологій та кібербезпеки (ІТтаКБ).

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Голова – д.т.н., проф., **Єгоров Б.В.,** ректор ОНАХТ.

Співголови :
Капрельянц Л.В. – д.т.н., проф., проректор з наукової роботи та міжнародних зв′язків,
Косой Б.В. – д.т.н., проф., в.о. директора ННІХКтаЕ ОНАХТ,
Котлик С.В. – к.т.н., доц., декан ФІТта КБ ОНАХТ,
Волков В.Е. – д.т.н., доц., директор ННІМАтаКС ОНАХТ,
Хобін В.А. – д.т.н., проф., завідувач кафедри автоматизації виробничих процесів ОНАХТ,
Невлюдов І.Ш. – д.т.н., проф., завідувач кафедри технології і автоматизації виробництва радіоелектронних і електронно-обчислювальних засобів ХНУРЕ,
Мельник А.О. – д.т.н., проф., завідувач кафедри ЕОМ НУ "Львівська політехніка",
Тарасенко В. П. – д.т.н., проф., завідувач кафедри СПіСКС НТУУ «Київський політехнічний інститут»,
Жуков І. А. – д.т.н., проф., директор інституту комп'ютерних технологій Національного авіаційного університету.

<u>Члени оргкомітету:</u>
Плотніков В. М. – д.т.н., проф., завідувач кафедри інформаційних технологій та кібербезпеки ОНАХТ.
Артеменко С.В. – д.т.н., проф., в.о. завідувача кафедри комп'ютерної інженерії ОНАХТ.
Князєва Н.О. – д.т.н., проф. кафедри комп'ютерної інженерії ОНАХТ.
Грищенко І.В. – к.т.н., заступник декана ФІТта КБ ОНАХТ.
Шамрай О.А. – к.т.н., доц. кафедри ТДтаВЕ ОНАХТ.

Матеріали подано українською, російською та англійською мовами.
Редактор збірника Шамрай О.А.

СТЕГАНОГРАФІЯ ДЛЯ КІБЕРБЕЗПЕКИ

Беденко А.Б., студент ОКР „бакалавр" факультету ІТ та КБ
Одеська національна академія харчових технологій, м. Одеса
Керівник – ст. викл. каф. КІ Бондаренко В.Г.

Захист інформації від несанкціонованого доступу є не вирішеною до сьогоднішнього дня питанням. Стеганографія - словосполучення слів steganos (секрет, таємниця) і graphy (запис), з'явилася вона раніше, ніж писемність (умовні знаки і позначення) це додаток до криптографії, яке захищає інформацію завдяки кодуванні повідомлення і, засекречуючи, так що б про цю передачу ніхто не знав. Секретний текст розкидається по основному повідомленням, а витягується лише знаючи прінцип по якому йшла розбивка (розсіювання послання).

Основні принципи базування стенографії:

• роботоздатності аудіофайлів, відеофайлів, зображень або інших файлів при оцифрування змінюється, але їх функціональність зберігається;

• Людина не відрізнить найдрібніші зміни в зображенні або звуці.

Наприклад, при відправці закодованого повідомлення, різні користувачі відкривають свої мобільні електронні пристрої та отримане зображення. Але при пропущенні через фільтр, що виділяє кожен біт і перетворює його в таємне послання.

Отже, стенографія - це об'єднання методів і засобів, за допомогою яких проводиться створення таємного каналу для пересилання інформації. При її створенні ви повинні знати що конкурент знає про стеганографії. Але не знає ключ потрібний для розшифровки, який допоможе знайти шифровку в тексті і розкодувати її. А для цього ви повинні створити всі умови для того що б противник не мав можливості в розшифровці таємних послань використовуючи різний вигляд послання.

Процес стеганографії разделяється на кілька етапів.

1. Вибір файлу який треба приховати.

2. Вибір файлу який ми будемо використовувати для приховування інформації з огляду на що він повинен у вісім разів перевищувати розмір файлу для приховування

3. Вибір програми для стенографії. Наприклад S-Tools, Steganos for Wm, Contraband.

4. Далі виробляємо кодування файлу т.е.устанавліваем захист файлу по паролю.

5. Відправляємо одержувачу зашифроване повідомлення і при бажанні його ключ для розшифровки.

Сам процес відносно легкий, але увелічіваеться розмір графічного зображення і це визначити під силу навіть не підготовленому користувачу при перевірці контрольних сум.

Так як стенографія допомагає у вирішенні питання про конфіденційність інформації, для злочинців це засіб так само для планування і приховування інформації, як приклад, що Аль-Каїда використовувала стеганографії для прихо-

вування повідомлень в зображеннях, а після передавала їх по електронній пошті і Usenet з метою підготовки терактів 11 вересня. Принцип стенографії так само використовується шкідливим софтом, щоб збільшити шанси на приховування шкідливого коду від антивірусних сканерів (наприклад, банківський троян Zeus, який вбудовується в байт-код графічного файлу і постає з точки зору користувача, як звичайний файл фотографії.) Обчислення шкідливого софту можливо тільки шляхом порівняння розмірів «чистого» і «шкідливого» файлу або в режимі bitmap.

Актуальність питання інформаційної безпеки постійно зростає і це стіму¬лірует інтерес до розвитку методів до стенографії та пошуку інших варіантів для вирішення проблеми захисту інформації. Але, при бурхливому розвитку Інтернет, виникають проблеми, такі як захист авторського права і права на особисту таємницю, і електронна торговля, яка найчастіше призводить до комп'ютерної злочинності або до кібертероризму..

Список літератури

1. Kahn D. The Codebreakers. N-Y, 1967.
2. Жельников В. Криптография от папируса до компьютера. М., 1996.
3. Pfitzmann B. Information Hiding Terminology, in Information Hiding, Springer Lecture Notes in Computer Science, v.1174, 1996, 347-350.
4. N.F. Johnson, S. Jajodia. Exploring Steganography: Seeing the Unseen, IEEE

ІНФОРМАЦІЙНИЙ АСПЕКТ ПІДГОТОВКИ МЕНЕДЖЕРІВ

Білецька Д.О. асистент кафедри «МіА» УкрДУЗТ м. Харків

На теперішній час сьогодення зобов’язує йти підприємства пліч-о-пліч з розвитком інформаційних технологій. Одна з вимог до менеджера високого рівня – знання програмного забезпечення для професійної роботи з документами. Ці вміння мають постійно оновлюватися, адаптовуватися до вимог зарубіжних партнерів, тощо.

В Україні, в більшості, підприємства працюють з документами в програмах Word різної модифікації. З огляду на спрямованість на європейський простір, та маючи досвід співпраці з зарубіжними підприємствами, можна сказати, що Word втрачає свої позиції, як програма першочергового використання.

Однією з популярних програм є Nitro. Вона схожа на звичний для українських менеджерів Acrobat reader, але її особливості у роботі з документами формату pdf, такі як можливість редагування документів у повному обсязі та одразу, вставка підпису керівництва та інші переважають над Acrobat reader. Ці пріоритети дають суттєві можливості, наприклад, значна економія часу та дає змогу не використовувати принтер для ланцюга «друк – мокра печатка та підпис – сканування - відповідь»,що, безумовно, прискорює процес роботи з партнерами.