Zygmunt Mazur, Hanna Mazur, Teresa Mendyk-Krajewska

Zastosowanie steganografii w sieciach komputerowych

Ekonomiczne Problemy Usług nr 117, 697-706

2015

ZESZYTY NAUKOWE UNIWERSYTETU SZCZECIŃSKIEGO
NR 852 EKONOMICZNE PROBLEMY USŁUG NR 117 2015

ZYGMUNT MAZUR, HANNA MAZUR, TERESA MENDYK-KRAJEWSKA
Politechnika Wrocławska[1]

ZASTOSOWANIE STEGANOGRAFII W SIECIACH KOMPUTEROWYCH

Streszczenie

Powszechna dostępność Internetu wiąże się z koniecznością ochrony przesyłanych i przechowywanych danych w systemach teleinformatycznych. Ich poufność zapewnia szyfrowanie, natomiast do oznakowania oryginalnych plików elektronicznych lub ukrycia faktu przekazywania treści (związanych np. z działalnością gospodarczą, polityczną lub przestępczą) stosuje się techniki steganograficzne. Rozwój steganografii pozwala na coraz skuteczniejsze ukrywanie informacji, stąd konieczne jest doskonalenie metod steganoanalitycznych związanych z wykrywaniem i analizowaniem steganogramów. Celem artykułu jest przedstawienie zagadnień dotyczących metod steganograficznych, które w połączeniu z mechanizmami kryptograficznymi stanowią skuteczne narzędzie zabezpieczania informacji przed jej wykryciem i odczytem.
Słowa kluczowe: ukrywanie informacji, steganoanaliza, cyfrowy znak wodny.

Wprowadzenie

Ochrona informacji ma na celu blokowanie do niej dostępu podmiotom nieuprawnionym oraz uniemożliwienie jej wykorzystania w razie przełamania zabezpieczeń.

Informacje zapisywane cyfrowo, przechowywane na różnych nośnikach bądź przekazywane podczas transmisji, mogą być szyfrowane i ukrywane. Metodami ukrywania informacji zajmuje się steganografia (gr. *steganos* – ukryty, *graphos* – pismo), której istotą jest przekazywanie informacji w sposób niezauważalny dla osób postronnych, pomimo jawności nośnika z ukrytą zawartością. W przypadku

[1] Wydział Informatyki i Zarządzania, Katedra Informatyki.

kryptografii fakt przekazywania czy przechowywania informacji jest jawny, ale treść jest niedostępna ze względu na jej zaszyfrowanie.

Do cyfrowego ukrywania informacji najczęściej wykorzystuje się pliki graficzne, tekstowe i dźwiękowe (np. o rozszerzeniach bmp, doc, gif, jpeg, mp3, txt, wav), ponieważ w prosty i niezauważalny sposób można do nich dodać nowy element lub usunąć powtórzenia, zastępując je wybraną treścią. Przykładowym sposobem ukrycia treści w pliku tekstowym może być wstawienie wysokiej rozdzielczości obrazu zminimalizowanego do wielkości kropki lub wstawienie tekstu w kolorze tła. Równolegle z rozwojem steganografii rozwijana jest steganoanaliza, dotycząca zagadnień związanych z wykrywaniem steganogramów (informacji ukrytych). Jej celem jest wykrycie użytej metody steganograficznej (steganoanaliza pasywna) lub zniszczenie steganogramu (steganoanaliza aktywna). Obie te dziedziny razem obejmuje się wspólną nazwą – steganologia.

1. Techniki steganografii

Duże zainteresowanie steganografią obserwuje się od wielu lat. Ten dział wiedzy zajmujący się ukrywaniem informacji rozwija się dynamicznie z uwagi na olbrzymie możliwości wykorzystania w tym celu plików elektronicznych (steganografia cyfrowa). Techniki stosowane w steganografii wykorzystują różne miejsca umieszczenia informacji, stąd wyróżnia się: steganografię lingwistyczną (do ukrycia tekstu wykorzystuje się inny tekst, czego przykładem jest akrostych – ukrytą treść można odczytać z ustalonych liter wyrazów[2]) oraz steganografię techniczną, wykorzystującą środki elektroniczne lub inne dostępne nośniki informacji.

Możliwości ukrywania informacji w cyfrowym zapisie danych (zdjęciach, filmach wideo, nagraniach dźwiękowych) są olbrzymie – stąd tak duże zainteresowanie zastosowaniem steganografii w sieciach komputerowych.

Steganogramy mogą być umieszczone w różnych miejscach i na wiele sposobów. W Internecie nośnikami (tzw. kontenerami) ukrytych wiadomości mogą być teksty, odsyłacze, adresy stron WWW, filmy, komentarze, wszelkie elementy graficzne, pliki muzyczne, kody źródłowe stron internetowych, reklamy itd. Wprowadzaną informacją może być tekst, liczba, obraz lub identyfikator (np. dla stwierdzenia obecności znaku wodnego). Wprowadzone informacje mogą być widoczne[3], ukryte lub dodatkowo szyfrowane, mogą różnić się odpornością na modyfikacje pliku nośnika (być odporne bądź ulotne) czy sposobem dekodowania.

---

[2] Przykładem jest hymn Holandii od 1932 r. (tekst z lat 1568–1572), w którym pierwsze litery zwrotek tworzą imię księcia WILLEM VAN NAZZOV, na którego cześć został napisany.

[3] W wielu sytuacjach wystarczy posłużyć się widzialnym cyfrowym znakiem wodnym identyfikującym plik (obraz) dla uniemożliwienia jego nielegalnego wykorzystania.

Ukrywanie informacji jest wykorzystywane do znakowania dokumentów i utworów elektronicznych (obrazów, książek, utworów muzycznych) cyfrowym znakiem wodnym. Metoda ta jest wykorzystywana do walki z nielegalnym kopiowaniem plików i ich rozpowszechnianiem. Techniki wstawiania cyfrowych znaków wodnych można sklasyfikować według różnych kryteriów, np. według odporności znaku na zakłócenia, sposobu jego dekodowania czy dziedziny, w jakiej znak jest wprowadzany.

Spośród stosowanych metod steganograficznych można wymienić metody transformacyjne (Fouriera, Falkowa, DCT[4]), substytucji (np. LSB, BCBS, modyfikacji kolorów indeksowanych), zniekształceniowe (wprowadzanie zakłóceń w losowych miejscach nośnika), rozproszonego widma (wykorzystujące całe pasmo częstotliwości do rozproszenia ukrywanych danych, dodatkowo rozpraszanych w całym nośniku), statystyczne (U.C.L. – obraz dzielony jest na bloki, w których ukrywane są kolejne bity wiadomości), czy generacji nośnika (nośnik generowany jest po przeanalizowaniu danych do ukrycia) (Garbarczuk, Kopniak 2005; Marciniak 2009).

Metoda substytucji LSB (*Least Significant Bit*) polega na wstawieniu danych na najmniej znaczące bity bajtów pliku nośnika. Wprowadzane zmiany są mniej widoczne w wielobarwnych plikach graficznych (np. 1 piksel – 3 bajty RGB) i wówczas, gdy zmiany są dokonywane w obrębie koloru niebieskiego lub czerwonego, na które to barwy oko ludzkie jest mniej wyczulone niż na kolor zielony (proporcje dla czułości percepcji wynoszą 3:1:6) (Kosedowski 2009).

Dla zapewnienia skuteczności ukrycia należy odpowiednio dobrać rodzaj i wielkość pliku transportującego do rozmiarów steganogramu. Na ogół im mniejszych rozmiarów informację (plik) chcemy ukryć, wykorzystując do tego kontener o dużej pojemności[5], tym jej przesył jest mniej zauważalny. Jednak w przypadku plików graficznych pełniących funkcję nośnika istotne jest równomierne rozłożenie wprowadzanych zaburzeń i wówczas ukrywana informacja nie może być zbyt mała w stosunku do rozmiarów pliku źródłowego.

Dane w prosty sposób można ukryć w pliku graficznym za pomocą polecenia DOS-a (*Disk Operating System*), np. łącząc plik graficzny i skompresowany:

```
copy /B obraz1.jpg + folder.zip obraz2.jpg
```

gdzie obraz1.jpg jest plikiem graficznym, w którym ma zostać ukryty skompresowany katalog o nazwie folder.zip, a plik obraz2.jpg jest plikiem wynikowym (Kołacz 2010). Po otwarciu pliku obraz2.jpg widoczny jest obraz bazowy (obraz1.jpg),

---

[4] DCT (*Discrete Cosine Transform*) – dyskretna transformata cosinusowa.

[5] Pojemność kontenera rozumiana jako stosunek liczby bitów steganogramu do liczby bitów przekazu jawnego niezbędnych do ich ukrycia, np. jeśli 1 bit można ukryć w 10 bitach, to pojemność kontenera wynosi 0,1 (10%).

natomiast po zmianie rozszerzenia na zip plik obraz2.zip udostępnia ukryte dane. Opisany sposób można zastosować do ukrycia plików także innych formatów (np. txt, exe).

Prawie każda metoda ukrycia pozostawia pewne ślady, lecz są one trudne do zlokalizowania, głównie ze względu na różne techniki ukrywania i ogromną liczbę potencjalnych nośników. Dużą skuteczność wykrywania tajnego przekazu dałyby automatyczne metody weryfikacji.

Techniki steganograficzne są wykorzystywane do ochrony praw autorskich i źródeł informacji, w celu przeciwdziałania wyciekom informacji i do zapewnienia poufności danych. Niestety, ukryte kanały mogą być użyte także do przekazywania informacji uzyskanych nielegalnie (np. danych gospodarczych), do przesyłania szkodliwego oprogramowania lub zabronionych treści.

2. Steganoanaliza

Obecnie steganografia cyfrowa stosowana w plikach multimedialnych jest niezauważalna dla osób postronnych bez użycia zaawansowanych metod analizy.

Zagadnieniami identyfikowania informacji ukrytych zajmuje się steganoanaliza. Można wyróżnić wiele technik steganoanalitycznych, zależnie od dostępnych analitykowi elementów (algorytm ukrywania, czysty plik nośnika, nośnik z ukrytą wiadomością) o różnym stopniu skuteczności (Mosorov 2014). Jedna z nich polega na porównywaniu dwóch obiektów (plików) i analizowaniu rozbieżności między nimi (rozmiarów, map bitowych itp.). Utrudnieniem w zidentyfikowaniu steganogramu może być brak wzorca do porównania.

W celu przeprowadzenia ataku wykorzystuje się różne metody, np.:

- *Steganography-only attack* – przeprowadzane są weryfikacje za pomocą różnych metod steganograficznych; skuteczność ataku jest stosunkowo niska ze względu na dużą liczbę możliwych sposobów;
- *Known-carrier attack* – gdy atakujący ma dostęp zarówno do wersji oryginalnej, jak i zmodyfikowanej;
- *Known-message attack* – jeśli znana jest poszukiwana wiadomość, natomiast celem jest złamanie algorytmu ukrywania;
- *Chosen-steganography attack* – gdy znany jest algorytm ukrywania (prawdopodobieństwo wykrycia wiadomości jest bardzo duże);
- *Chosen-message attack* – metoda polegająca na poddawaniu próbki przygotowanych informacji działaniu różnych algorytmów w celu wykrycia podobieństwa lub wzorca do znanej metody (technika przypomina siłową metodę łamania haseł dostępowych);
- *Known-steganography attack* – atakujący zna użyty algorytm oraz posiada nośnik oryginalny i zmodyfikowany.

Dla utrudnienia steganoanalizy, a tym samym dla zwiększenia poziomu bezpieczeństwa steganogramu, plik wykorzystywany jako kontener nie powinien wzbudzać podejrzeń i najlepiej, żeby nie był dostępny w wersji oryginalnej (bez ukrytej wiadomości). W tym celu można wykorzystać własnoręcznie zrobione zdjęcie o dużej różnorodności kolorów.

3. Steganografia sieciowa

Nośnikiem ukrytej informacji mogą być protokoły sieciowe (steganografia wewnątrz- i międzyprotokołowa) oraz usługi realizowane drogą elektroniczną. Do steganografii sieciowej można wykorzystać między innymi bezprzewodowe sieci lokalne WLAN, systemy VoIP (*Voice over Internet Protocol*) oraz protokoły, które stosują mechanizmy obsługi pakietów IP. Informacje można ukryć w pakietach transmisyjnych (np. w numerach ich nagłówków lub w stemplach czasowych), co zapobiega ich wykryciu przez zapory sieciowe.

Duży wkład w rozwój steganografii wniosła utworzona w 2002 r. na Politechnice Warszawskiej grupa zajmująca się bezpieczeństwem sieciowym (Lubacz i in. 2010). W 2003 r. zespół ten zaproponował, aby do przesyłania danych ukrytych w sieciach Wi-Fi użyć ramek z uszkodzonymi sumami kontrolnymi (Szczypiorski 2003), a w 2006 r. opracował koncepcję steganograficznego routera, która została wykorzystana w systemie TrustMAS (*Trusted Communication Platform for Multi-Agent Systems*) dla amerykańskich sił zbrojnych. W kolejnych latach członkowie zespołu zaproponowali, by do przesyłania ukrytych danych w VoIP wykorzystać celowo opóźnione w nadajniku pakiety, i zaprezentowali nową metodę ukrywania danych w protokole TCP opartą na retransmisjach pakietów. Wynikiem prowadzonych prac jest dedykowany dla sieci WLAN system ukrytej komunikacji dla „zepsutych" sieci o nazwie HICCUPS (*Hidden Communication System for Corrupted Networks*) oraz system LACK (*Lost Audio Packets Steganography*) przeznaczony dla telefonii IP.

HICCUPS to pierwszy system steganograficzny mający zastosowanie w bezprzewodowych sieciach lokalnych. Dostępne na żądanie pasmo do transmisji steganogramów tworzą ramki z błędnymi sumami kontrolnymi. W systemie tym wyróżnia się trzy ukryte kanały:

- K1 – oparty na polach adresowych MAC (źródła i przeznaczenia) lub innych polach nagłówka ramki,
- K2 – oparty na niepoprawnych sumach kontrolnych,
- K3 – oparty na polu użytkowym ramki (tryb uszkodzonych ramek).

W przypadku systemu VoIP dla potrzeb steganografii wykorzystuje się dwie z czterech grup protokołów używanych przez system. Jedną tworzą protokoły sygnalizacyjne umożliwiające zestawianie połączeń między dwoma komunikującymi

się węzłami (np. protokołów SIP – *Session Initialization Protocol*), drugą grupę stanowią protokoły do przesyłu konwersacji (np. UDP).

Przykładem użycia dla potrzeb steganografii protokołów sieciowych stosu TCP/IP jest metoda RSTEG (*Retransmission Steganography*) wykorzystująca mechanizm retransmisji utraconych pakietów. Z kolei w przypadku ukrywania informacji w protokołach stosujących mechanizmy obsługi pakietów IP można wskazać kilka miejsc w nagłówku pakietu, które mogą być wykorzystane do ukrywania steganogramów: pole Type of Service, pole identyfikacji, pole flag fragmentacji i pole opcji.

Do ukrycia informacji można wykorzystać też internetowy protokół SCTP (*Stream Control Transmission Protocol*) działający w warstwie transportowej, używany m.in. do przenoszenia ruchu sygnalizacyjnego w sieciach konwergentnych bazujących na IP. Zdefiniowano już wiele metod steganograficznych dla potrzeb tego protokołu.

Przykładem steganografii międzyprotokołowej może być metoda PadSteg (*Padding Steganography*), w której wykorzystuje się oddziaływanie między protokołem sieci lokalnej Ethernet a protokołami internetowymi, takimi jak: TCP, UDP i ICMP. Urządzenia komunikujące się przy użyciu metody PadSteg dla znalezienia się w sieci lokalnej używają protokołu ARP (*Address Resolution Protocol*), zaś ukryta komunikacja jest możliwa dzięki potrzebie uzupełnienia ramek krótszych niż 64 bity, by nie zostały odrzucone jako uszkodzone.

4. Steganografia w praktyce

Istotą steganografii jest przekazywanie informacji bez wzbudzania podejrzeń. Metody steganograficzne są wykorzystywane m.in. do znakowania plików oryginału (zdjęć, plików wideo, muzycznych) i dokumentów elektronicznych w celu zapewnienia autentyczności i identyfikacji autora czy właściciela.

Przykładów zastosowania steganografii cyfrowej w sieciach komputerowych jest wiele. Wśród licznych jej zastosowań można wymienić:

- podpisywanie obrazów (tytuł, autor, numer seryjny, dane nabywcy itp.),
- ochrona praw autorskich (dowód autorstwa, legalnego zakupu),
- ochrona przed modyfikacją pliku oryginału (wykrywanie zmian w obrazie, ich lokalizacja),
- monitorowanie nielegalnej dystrybucji (walka z piractwem komputerowym),
- sekretna komunikacja (steganografia właściwa, stosowana np. przez służby wywiadowcze).

W zależności od potrzeb umieszczanym w plikach znakom (treściom) stawia się różne wymagania. Pożądane cechy niewidocznych znaków to: ścisłe związanie z zawartością nośnika, zabezpieczenie trudne do wykrycia i usunięcia, niedostrze-

galność pogorszenia jakości pliku nośnika, odporność na pakowanie plików metodami kompresji stratnej, odporność na modyfikacje (kadrowanie, obracanie, zmianę rozmiaru i formatu pliku).

Zwykle przekazanie tajnych treści w ogólnodostępnym pliku, np. w wiadomości zamieszczonej w Internecie lub w zdjęciu umieszczonym na portalu społecznościowym, nie wzbudza podejrzeń i umożliwia szybkie ich dotarcie do adresata. Niestety, w przypadku przechwycenia steganogramu przez osobę nieuprawnioną jego treść narażona jest na odczytanie bądź na niedostarczenie.

Do realizacji procesu ukrywania informacji służy wiele specjalistycznych narzędzi programowych (wiele z nich jest darmowych), jak na przykład:

- Cloak – jedno z najprostszych narzędzi do ukrywania plików dowolnego typu w obrazach o formacie bmp z użyciem szyfrowania, zoptymalizowanej kompresji i systemem haseł;
- Steganos 3 Security Suite – jest jednym z najlepszych programów steganograficznych, który szyfruje dane przed ich ukryciem, umożliwia wybór pliku nośnika i użycie hasła dostępu;
- 3-Tools – dane ukrywane są w plikach graficznych (bmp, gif) i dźwiękowych (wave), można je szyfrować za pomocą wybranych algorytmów, ukrywać wiele wiadomości w jednym nośniku (na trzech najmniej znaczących bitach każdego bajtu, niezależnie od formatu pliku);
- Hide and Seek – do umieszczania danych w plikach gif (wykorzystywany jest najmniej znaczący bit każdego bajtu, stosowane pseudolosowe rozproszenie ukrytych danych w całym nośniku), możliwa ochrona hasłem;
- Hydan – umożliwia ukrycie informacji w plikach wykonywalnych z wykorzystaniem technik polimorficznego kodowania;
- Steghide – pozwala ukryć różne typy danych w plikach graficznych (jpg, bmp) i muzycznych (wave, au), wybrać algorytm szyfrowania i hasło;
- OpenPuff – oferuje duże możliwości, pozwalając na zapisanie informacji w wielu formatach: obrazy (bmp, jpg, pcx, png), pliki audio (aiff, mp3, au, wave) i wideo (3gp, mp4, mpg, vob) oraz flash (flv, swf, pdf), pozwala na wybór poziomu ukrycia wiadomości i ochronę hasłem.

Inne znane aplikacje tego typu to: Hide In Picture, Ultima Steganography, SecurEngine, 1-2-Free Steganography lub Secret Media. Do niezauważalnego umieszczenia na dysku plików lub folderów można wykorzystać takie programy jak WinMend Folder Hidden czy SecretFolder. Niedawno opracowano także narzędzie steganograficzne dla komunikatora Skype (Szczypiorski, Karaś 2013).

Steganografia znajduje też zastosowanie do oznaczania zrzutów ekranu np. poprzez niejawne zapisanie IP komputera i daty ich sporządzania.

5. Steganografia a regulacje prawne

W przyjętej przez Radę Europejską w 2003 roku Europejskiej Strategii Bezpieczeństwa (wspartej zaaprobowanym w grudniu 2008 r. Raportem Sekretarza Generalnego ds. Wspólnej Polityki Zagranicznej i Bezpieczeństwa) jednym z trzech głównych celów jest przeciwdziałanie zagrożeniom, głównie terroryzmowi, przestępczości zorganizowanej oraz zagrożeniom cybernetycznym.

Rada Europejska w lutym 2007 r. podjęła decyzję w sprawie bezpieczeństwa i ochrony wolności w latach 2007–2013 (Decyzja Rady z 12 lutego 2007). W szczegółowym programie pt. *Zapobieganie, gotowość i zarządzanie skutkami terroryzmu i innymi rodzajami ryzyka dla bezpieczeństwa* uznała za istotne działania „w zakresie analizy, audytu i kontroli, wymiany informacji, szkolenia i wymiany ekspertów oraz działania związane z podnoszeniem świadomości i rozpowszechnianiem informacji" (*Program szczegółowy: Zapobieganie…*).

W styczniu 2013 r. do walki z przestępczością związaną z systemami informatycznymi i danymi elektronicznymi powołano w Hadze w ramach Europejskiego Urzędu Policji (Europolu) Europejskie Centrum ds. Walki z Cyberprzestępczością (EC3). Globalny charakter działań przestępczych wymaga jednak współpracy także z krajami pozaeuropejskimi i korporacjami międzynarodowymi związanymi z działalnością teleinformatyczną, internetową i bezpieczeństwem informacji.

Na podstawie zarządzenia Ministerstwa Obrony Narodowej z 29.04.2013 r. powstało w Polsce Narodowe Centrum Kryptologii, którego zadaniem jest zwalczanie cyberterroryzmu w systemach teleinformatycznych. Możliwości wykorzystania kryptografii i steganografii są przedmiotem badań i analiz wielu ośrodków. Dotyczą one m.in. wykorzystania publicznych kanałów do tajnego przekazu wiadomości, co pomimo stosowania wielu środków zapobiegawczych jest nadal możliwe. Nawet w przypadku wykrycia steganogramu są trudności z ustaleniem jego nadawcy.

Ogólnie dostępne sieci komputerowe umożliwiają skuteczne wykorzystywanie steganografii. Rozwój nowych technologii, postępująca cyfryzacja oraz zmiana sposobów prowadzenia działalności przez banki, podmioty medyczne i urzędy administracji państwowej oraz firmy i przedsiębiorstwa (w tym o strategicznym znaczeniu dla funkcjonowania państwa) stwarzają warunki do rozwoju przestępczości internetowej oraz nadużyć prowadzonych z wykorzystaniem sieci komputerowych. Równolegle rozwijana jest informatyka śledcza (ang. *computer forensics*), która obejmuje m.in. sposoby naruszania zabezpieczeń dowodów elektronicznych. Uregulowania prawne muszą być na bieżąco modyfikowane i szybko dostosowywane do aktualnych potrzeb. Wiele prawnie usankcjonowanych rozwiązań stosowanych w celu zapewnienia bezpieczeństwa cybernetycznego narusza niestety prywatność obywateli.

Zagadnienia związane z ochroną danych (do których nielegalnego przekazywania są wykorzystywane techniki steganografii) regulują w Polsce m.in.: ustawa o ochronie danych osobowych, ustawa Prawo bankowe, kodeks cywilny i kodeks karny, np. § 1 art. 266 *Przestępstwa przeciwko ochronie informacji*[6], § 1 art. 287 *Oszustwo komputerowe*[7], czy art. 276 *Przestępstwa przeciwko wiarygodności dokumentów*[8].

Podsumowanie

Gwarancję na skuteczną ochronę informacji przed nieupoważnionym dostępem stwarza połączenie metod steganografii z kryptograficznymi.

Duży ruch sieciowy uniemożliwia jego precyzyjną analizę w czasie rzeczywistym, a tym samym zauważenie, zlokalizowanie i odpowiednie zaklasyfikowanie wszelkich niezgodności czy nieprawidłowości, pomimo stosowania nowoczesnych metod steganoanalizy (z wykorzystaniem sieci neuronowych, algorytmów genetycznych i logiki rozmytej).

W dobie informacji cyfrowej steganografia nabiera szczególnego znaczenia dzięki możliwościom zastosowania różnorodnych metod dających duże prawdopodobieństwo skutecznego ukrycia faktu przekazywania wybranych treści.

Literatura

1. Decyzja Rady z 12 lutego 2007 ustanawiająca na lata 2007–2013, jako część ogólnego programu w sprawie bezpieczeństwa i ochrony wolności, szczegółowy program *Zapobieganie, gotowość i zarządzanie skutkami terroryzmu i innymi rodzajami ryzyka dla bezpieczeństwa* (2007/124/WE, Euratom), Dz. Urz. UE 2007.
2. Garbarczuk W., Kopniak P. (2005), *Steganologia: współczesne metody ochrony informacji (przegląd)*, PAK, nr 3.

[6] „Kto, wbrew przepisom ustawy lub przyjętemu na siebie zobowiązaniu, ujawnia lub wykorzystuje informację, z którą zapoznał się w związku z pełnioną funkcją, wykonywaną pracą, działalnością publiczną, społeczną, gospodarczą lub naukową, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2".

[7] „Kto, w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody, bez upoważnienia, wpływa na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych lub zmienia, usuwa albo wprowadza nowy zapis danych informatycznych, podlega karze pozbawienia wolności od 3 miesięcy do lat 5".

[8] „Kto niszczy, uszkadza, czyni bezużytecznym, ukrywa lub usuwa dokument, którym nie ma prawa wyłącznie rozporządzać, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2".

3. Kołacz M. (2010), *Ukrywanie plików w obrazach JPEG (JPG)*, techformator.pl/ukrywanie-plikow-w-obrazach-jpeg-jpg.
4. Kosedowski M. (2009), *Steganografia*, pcworld.pl/artykuly/334607/Steganografia.
5. Lubacz J., Mazurczyk W., Szczypiorski W. (2010), *Steganografia sieciowa*, „Przegląd Telekomunikacyjny", rocznik LXXXIII, „Wiadomości Telekomunikacyjne", rocznik LXXIX, nr 4/2010, krzysiek.tele.pw.edu.pl/pdf/pt-steg.pdf.
6. Marciniak M. (2009), *Tajny znak*, computerworld.pl/artykuly/343070_1/Tajny.Znak.
7. Mosorov W (2014), *Steganografia cyfrowa. Sztuka ukrywania informacji*, Wydawnictwo Uniwersytetu Łódzkiego, Łódź.
8. *Program szczegółowy: Zapobieganie, gotowość i zarządzanie skutkami terroryzmu (2007–2013)*, europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33262_pl.htm.
9. Szczypiorski K. (2003), *HICCUPS: Hidden Communication System for Corrupted Networks*. In Proc. of: The Tenth International Multi-Conference on Advanced Computer Systems, pp. 31–40, October 22–24, Międzyzdroje.
10. Szczypiorski K., Karaś M. (2013), *Opublikowano dokumenty dotyczące nowej metody tajnych rozmów przez Skype*, websecurity.pl/tag/steganografia.

APPLICATION OF STEGANOGRAPHY IN COMPUTER NETWORKS

Summary

The widespread availability of the Internet requires protection of data transmitted and stored in ICT systems. Their confidentiality is provided by encryption, while to watermark the original electronic files or hide the fact that the transmission of contents occurs (e.g. in relation to economic, political or criminal activity) steganographic techniques are used. The development of network steganography allows for more effective information hiding, so it is necessary to improve steganalitics related to identifying and analyzing steganograms. The aim of the article is to present issues concerning steganographic methods which, combined with cryptographic mechanisms, are an effective tool for protecting information against detection and readout.
Keywords: information hiding, steganalitics, digital watermark.

Translated by Zygmunt Mazur