ПРЕДИЗВИКАТЕЛСТВАТА НА СТЕГАНОГРАФИЯТА КЪМ ИНФОРМАЦИОННАТА СИГУРНОСТ И ОБУЧЕНИЕТО НА СПЕЦИАЛИСТИ*

СТАНИМИР С. СТАНЕВ, БОРИСЛАВ П. СТОЯНОВ

CHALLENGES OF STEGANOGRAPHY TO INFORMATION SECURITY AND TRAINING OF SPECIALISTS

STANIMIR S. STANEV, BORISLAV P. STOYANOV

ABSTRACT: *This work provides an overview of the latest trends in contemporary steganography and their challenges to information security, security services and training of specialists in the field of information defense. The possibilities of using online social networks, cloud services, and mobile applications for criminal purposes are marked, and some tools for steganological protection are shown. Special attention is paid to the training of specialists in steganography abroad and at Shumen University. The experience and the learning outcomes of students of the "Informatics" specialty at the University on the problems of computer and network security as a component of their professional training are summarized.*

KEYWORDS: *information security, information hiding, computer and network steganography, steganology, training steganography, parallel steganography, cloud computing, cloud security, insiders, sterilization.*

I. Въведение в терминологията и таксономията на стеганографията и стеганологията

Един от ефективните подходи за защитата на важна информация е скриването на съществуването ѝ (data hiding). Това направление включва много техники и методи – криптография, сигнални системи, условни знаци, маскировка, в това число и

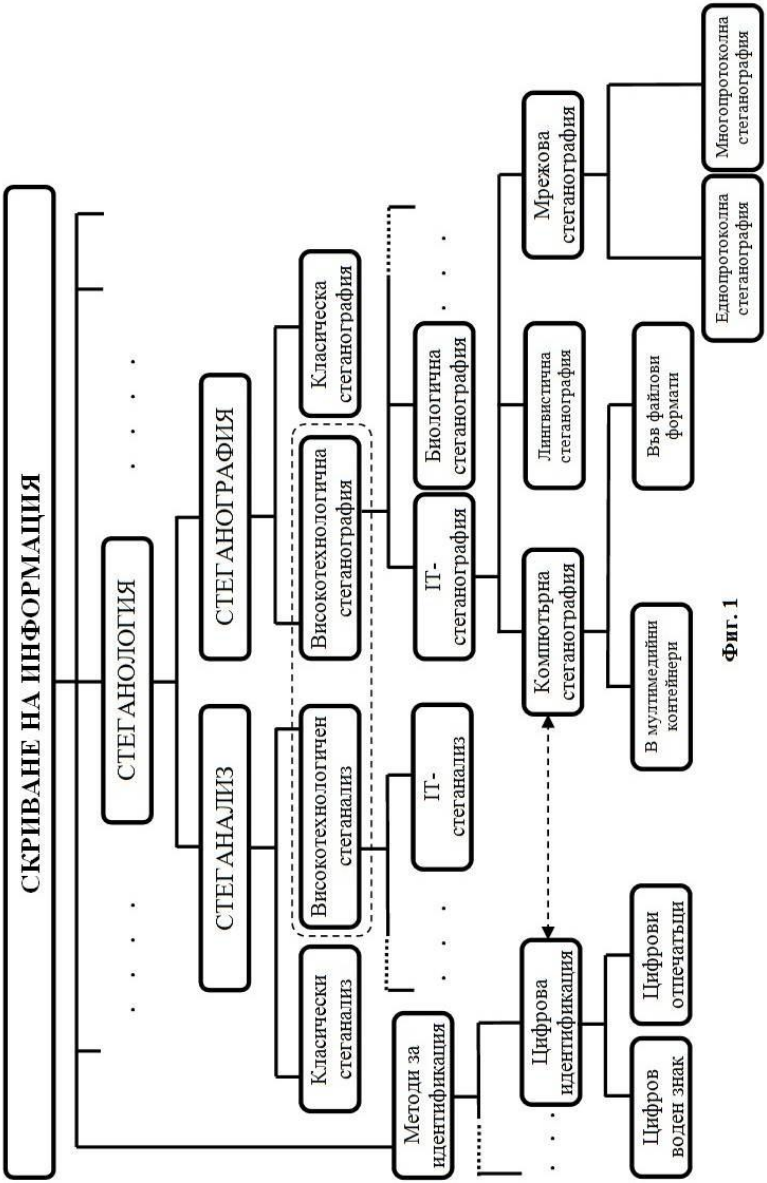
* Настоящата статия е финансирана от Фонд „Научни изследвания” към Шуменския университет „Епископ Константин Преславски“ по проект № РД-08-68/02.02.2016 г.

стеганографията [1, 2]. Тя има хилядолетна история и предлага много средства за скриване на съобщения (невидими мастила, микроточки, тайни канали и др.) [3]. Историческите извори разкриват факти за използването на стеганографски техники и в нашите земи от революционерите от периода на националното ни възраждане и от Апостола на свободата Васил Левски. Използваните от него и комитетите симпатични (невидими) мастила и шаблони (наричани „скари“, „лозинки“, „книги“), могат коректно да се класифицират като средства на класическата стеганография [4].

Стеганографията (steganography) е интердисциплинарна научно-приложна област, съвкупност от технически умения и изкуство за начините за скриване на факта на предаване (наличие) на информация [5]. От средата на първото десетилетие на XXI век сред специалистите се използва терминът стеганология (steganology), обхващащ два смислово противоположни компонента – стеганография и стеганализ (по аналогия с криптологията, състояща се от криптография и криптоанализ) [6]. Стеганализът (steganalysis) обединява методи и технологии за откриване на секретни стеганографски комуникации. Стегоатака е всеки опит да се открие, извлече или да се унищожи скрито чрез стеганография съобщение.

На фиг. 1 е показана класификация на стеганологията на съвременния етап на нейното развитие. Тази класификация може да се променя с развитието на новите методи.

Терминът „Класическа стеганография“ се използва само за обобщаване на съвкупността от огромния брой исторически развили се методи, системи, техники и приложения. Целта им е предаване или съхраняване на данни, така че противникът въобще да не се досеща за факта на наличието на скритите съобщения.


СКРИВАНЕ НА ИНФОРМАЦИЯ
СТЕГАНОЛОГИЯ
СТЕГАНАЛИЗ
СТЕГАНОГРАФИЯ
Класически стеганализ
Високотехнологичен стеганализ
ГГ-стеганализ
Методи за идентификация
Цифрова идентификация
Цифров воден знак
Цифрови отпечатъци
Класическа стеганография
Високотехнологична стеганография
ГГ-стеганография
Биологична стеганография
Компютърна стеганография
Лингвистична стеганография
Мрежова стеганография
В мултимедийни контейнери
Във файлови формати
Еднопротоколна стеганография
Многопротоколна стеганография

Фиг. 1

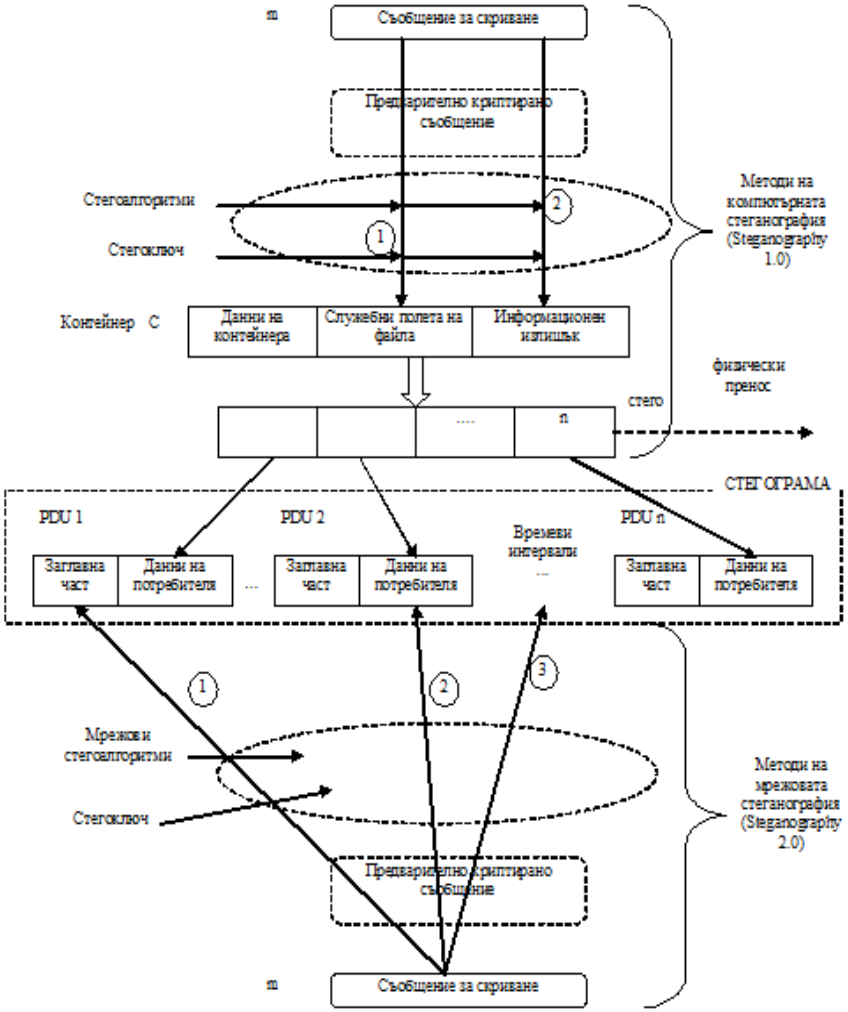
Високотехнологична стеганография (high-tech steganography) е термин за обобщаване на направленията за скриване на съобщения с използване на комуникационните и компютърни технологии, нанотехнологиите и съвременните постижения на биологията. От края на осемдесетте години на миналия век с внедряването на първите персонални компютри за решаване на стеганографски проблеми, датира и началото на съвременната IT-стеганография. IT-стеганографията използва бинарни последователности за контейнери и съобщения. Контейнер (container) е файл или протокол, който може да бъде използван за скриване на съобщение. Те са двоични последователности – компютърни файлове или протоколни единици на мрежите. В зависимост от използваните методи и контейнери, IT-стеганографията се дели на компютърна, мрежова и лингвистична стеганография [5].

Днес компютърната и мрежовата стеганография са самостоятелни научно-приложни направления за информационна сигурност, изучаващи проблемите на създаване на компоненти със скрита информация в явна информационна среда, генерирана от компютърните системи и мрежи. Компютърната стеганография има две основни направления за скриване на информация – използването на специалните свойства на компютърните формати и използване на преобразувани в дискретна форма сигнали, имащи непрекъсната аналогова природа (изображения, видео, звук).

През 2003 год. екипът на полския изследовател проф. Кшиштоф Шчипьорски (Krzysztof Szczypiorski) въведе термина мрежова стеганография (network steganography) в контекста на съвкупността от всички методи за скриване на информация , които могат да се използват за обмен на стегограми, вградени в мрежови протоколи [7]. Това е продължение на идеята за скритите мрежови канали (covert chanels) [8]. Мрежовата стеганография вгражда секретни данни в две части на протоколите - контейнери - заглавната част на протоколите или полетата за потребителските данни, или манипулира на времевите интервали между протоколните единици на някои мрежови протоколи – фиг. 2 [5]. Някои автори използват термина

цифрова стеганография (digital steganography) като синоним на компютърната стеганография. В други източници цифровата стеганография се представя като направление за използване на стеганографски методи за създаване на цифрови водни знаци (ЦВЗ) (digital watermarking), сигнатурни отпечатъци (digital finger prints) и надписи (captions). Методите за създаване на ЦВЗ вграждат информация в цифрови обекти (наричани произведение или творба), с цел защита на тяхното авторско право. Най-съществената разлика между скритото предаване на данни със стегометоди и вграждането на ЦВЗ се състои в това, че в първия случай нарушителите не знаят, но се стремят да открият скритото съобщение, а във втория всички знаят за това, че то съществува. Методите за ЦВЗ и за отпечатъци използват методи, аналогични на стеганографските. Но използването на стегометоди за ЦВЗ не е достатъчно основание те да бъдат разглеждани като цифрова стеганография.

Стегосистема, (stegosystem) е съвкупността от средства и методи, които се използват за формиране на скрит канал за предаване на информация. Функцията на стегосистемата се нарича скриване на съобщение (hiding the message). Съобщението е файл от произволен тип, който трябва да бъде скрит. Вграждането (embedding) е действие на стегосистемата по поставяне на съобщението в контейнера. Стего (stego) или стегофайл, е сумарният файл – контейнерът с вграденото съобщение, който се предава (съдържа) скритото съобщение. Извличането (extracting) е действие по изваждане, декодиране на съобщението от контейнера от потребителя, за когото е предназначено. Стегометод (steganographic method) е конкретен метод, техника за скриване на информация. Стегометодът е абстрактно обобщение на клас от стегоалгоритми, които се базират на определен стеганографски метод. Например методът LSB в BMP изображения е стегометод, но на базата на този метод могат да бъдат разработени различни стегоалгоритми. Стегоалгоритъм (stegoalgoritm) е алгоритъм за реализация на стегометод. Той определя двете действия – вграждане и извличане.


m
Съобщение за скриване
Предварително криптирано съобщение
Стегоалгоритми
Стегоключ
Методи на компютърната стеганография (Steganography 1.0)
Контейнер С
Данни на контейнера
Служебни полета на файла
Информационен излишък
физически пренос
стего
n
СТЕГОГРАМА
PDU 1
PDU 2
PDU n
Времеви интервали
Заглавна част
Данни на потребителя
Мрежови стегоалгоритми
Стегоключ
Методи на мрежовата стеганография (Steganography 2.0)
Предварително криптирано съобщение
m
Съобщение за скриване

Фиг.2

Методите на компютърната стеганография основно вграждат информация в излишъка от битове в служебната и „потребителската“ част на файловете. Важен параметър в стеганографията е стегокапацитетът. Стегокапацитет (steganographic capacity) е максималният размер на съобщението (в битове), което може да бъде вградено в контейнер, без да може да бъде открито. Основната цел на стеганографията е да се увеличи стегокапацитета и да се подобри неоткриваемостта. Така ефективността на стегометода зависи от две противоречиви изисквания – количеството данни, които могат да бъдат вградени (стегокапацитет) и трудността за откриване, определяна като незабелижимост на тези данни.

Важен елемент в стегосистемата е стегоключът (stegokey) – секретен ключ, необходим за скриване на информацията. Под този термин най-общо се разбира уговорената процедура и средствата за скриването на съобщенията (използван стегометод, стегопрограма, един или повече контейнера за едно съобщение, разпределение на частите на съобщението в контейнера и др.) [5]. В широкият смисъл на термина, стегоключът е неизвестен на противника способ за скриване на информация. В тесен смисъл стегоключът е секретен параметър/(и) на използвания стегоалгоритъм, без познаването на който е невъзможно извличането на скритото в стего съобщение. Стегоключът не криптира данните, а скрива тяхното местоположение в контейнера. Друг е въпросът със секретното разпространение на стегоключовете. Авторите считат, че разпространението на стегоключовете е по-целесъобразно да става с помощта на методите на мрежовата стеганография, а не с методи на компютърната стеганография с мултимедийни контейнери. Разбира се, по принцип не е изключено секретното предаване на стегоглючове и с други подходи и методи. Стегоключът включва и криптоключ, чрез който предварително може да бъде криптирано съобщението, подлежащо на скриване. Стеганографските алгоритми, криптографските протоколи за обмен на ключове, биометричната идентификация, симетричното криптиране или удостоверяването са ползватели на

псевдослучайни числа. През последните две десетилетия се наблюдава бързо нарастващ интерес към нелинейни динамични системи като основа за разработка на генератори на псевдослучайни числа (ГПСП).

Моделирани псевдослучайни генератори на двоични числа са предложени в [9] и [10]. Модофицирани псевдослучайни генератори, изградени чрез Chirikov standard map и свиваща функция, Tinkerbell map, Zaslavsky map и Chebyshev map са предложени в [11] и [12]. Вграждането на съобщение в контейнер може да стане с помощта на един, или даже няколко стегоключа. Числата, породени от ГПСП могат да определят позициите на модофицираните пиксели (в случай на фиксиран графичен контейнер) или интервалите между тях при поточен контейнер. По аналогия с правилото на Керхоф в криптографията, много от специалистите по стеганология считат, че по принцип устойчивостта на стегосистемата се определя само от секретността на стегоключа.

Най-кратко принципа на създаване на стегофайл може да бъде представен по този начин:

Стего (файл) = Контейнер + Секретно съобщение + Стегоключ.

Стеготехниките могат да се прилагат както за целите на защитата на данните в областта на военните и правителствени комуникации, защитата на авторското право, и при решаването на други задачи по осигуряване на информационната сигурност, така и за незаконни цели – например за създаване на скрити канали за изтичане на забранени документи и за комуникация на престъпници [3]. Прилагането на стегометоди за скриване на съобщения в цифрови изображения е еквивалент на шпионския тайник "dead drop", но в киберпространството. Има данни, че терористи от Al-Qaeda са използвали стеганографията [13]. Актуалността на разглеждания проблем изисква запознаването с основите на съвременната стеганология на по-широк кръг от специалисти, чиято задача е не само разработването, анализа или противодействието на стеганосредствата, но и квалифициран избор на съществуващите стеготехнологии и тяхното умело

използване за решаване на конкретни приложни задачи в областта на защитата на информацията. Това е особено важно за бъдещите специалисти в областта на информационната сигурност.

II. Развитие на методите на ИТ-стеганографията

Най-често използвания мултимедиен контейнер в компютърната стеганография е графичния файл поради масовото му използване и сравнително по-лесната му обработка. Съществуват различни методи, алгоритми и подходи, използващи един или повече контейнери за вмъкване на съобщението. Размерът, видът и броят на контейнерите е в пряка зависимост от размера на скритото съобщение, конкретния стего алгоритъм и други фактори, касаещи подбора на контейнер. Използването на неподходящ контейнер може да стане причина за компрометиране дори на много надежден стего алгоритъм.

Според използваният принцип на вграждане на скритите съобщения, методите на компютърната стеганография с мултимедийни файлове се разделят на няколко основни класа:

- Методи в пространствената област (алтернативни названия и означения – методи в пространствения домейн; адитивни методи; директни методи; прости методи; методите за непосредствена смяна; субституционни методи; методи в битовата област; Spatial Domain, Image Domain, Bit Wise Method, Substitution) – те използват излишъка на информационната среда в пространствената област (за изображенията) или временната област (за звуците).

- Методи в честотната област (алтернативни названия и означения – честотен домейн, област на преобразованията,методи с трансформация (Transform Domain). Наричат се още спектрални методи, защото в тях се използва спектрално представяне на елементите на контейнера (разни коефициенти на масивите на дискретно-косинусовите преобразования – ДКП (DCT), преобразования на Фурие – DFT, Карунен-Лоев – KL, Адамар, Хаар и др.) [5].

- Стеганография с разпръснато вграждане (Spread Spectrum) – при тази техника скритото съобщение се разпръсква по цялия носещ файл и това прави откриването доста трудно [6].

- Статистически методи – това са методи, които вграждат скритата информация чрез извършване на промяна на някои статистически свойства на носещия файл и използват изследване на хипотези в процеса на извличане.

- Деформиращи методи – тази техника използва нарочна деформация на носещия файл (сигнал) и измерва девиацията между оригиналния и стегофайла.

- Изграждащи методи – тези методи скриват съобщението заедно със създаването на носещ файл.

- Хибридни методи.

Според използвания контейнер, методите на компютърната стеганография се разделят на три основни вида:

- в графични изображения;
- в аудиофайлове;
- във видеофайлове.

Директните методи вграждат информация непосредствено в битовете на контейнера (при изображения в пикселите). Един от най-добрите литературни обзори за тази стеганография е направен в [8]. Този вид стеганография включва методите на най-младшия бит (НМБ) LSB (Least Significant Bit) и BPCS (Bit Plane Complexity Segmentation). Един от най-ранните методи за компютърна стеганография с идеята на метода LSB е предложен в началото на 90-години на миналия век в [14]. Този метод за замяна на най-младшия бит е най-разпространения метод сред методите за промяна в пространствения домейн. Най-младшият бит (НМБ) в едно изображение носи в себе си най-малко информация. Известно е, че човешките възприятия не могат да усетят промяна в този бит. Фактически промяната в НМБ е шум, който може да се използва за вграждане на скрито съобщение. В изображения, в които всеки пиксел се кодира с един байт, размера на вградената информация по този метод може да достигне до 1/8 от размера на контейнера.

Сравнителен анализ на съвременни стегометоди и стегоалгоритми е направен в [15].

Всички методи за скриване на информация, които могат да се използват за обмен на стегограми в телекомуникационните мрежи могат да бъдат класифицирани с общия термин скрит канал (covert channels) или мрежова стеганография (network steganography). За разлика от стеганографските методи, които използват цифрови контейнери (изображения, аудио- и видеофайлове), мрежовата стеганография използва управляващите елементи на комуникационните протоколи и тяхната основна присъща функционалност. Резултатите от работата с такива методи са по-трудни за разкриване и елиминиране. Типичните мрежови стегометоди включват модифициране на протоколните единици (PDU), над временните интервали между обменяните PDU, или и над двете (т.н. хибридни методи). Нещо повече, възможно е да се използват отношенията между два или повече мрежови протокола за осъществяване на секретна комуникация. Това приложение се нарича междупротоколна стеганография (inter-protocol steganography). Повечето методи манипулират IP Internet протокола, който е фундаментална част от всяка Интернет комуникация (текстова или гласова). Този протокол е добър за нечувствителни към реда на предаване електронни писма или статични уеб-страници, но не е походящ за гласови или видео- поточни файлове, когато кратко мрежово закъснение може да разруши секунди от видео файла. За да се избегне този недостатък, мрежовите експерти са разработили протокола Voice over Internet Protocol (VoIP). През 2007 год. от полските специалисти е поставено ново начало и на т.н. стеганофония (steganophony) – скриването на съобщения във VoIP – разговори, например на забавените или повредени пакети, които обикновено се пренебрегват от приемника (този метод се нарича LACK – Lost Audio Packets Steganography), или като алтернатива, скриване на информация в неизползвани заглавни полета. Стегометодите позволяват да се скрият секретни съобщения в трафика VoIP без забележимо влошаване на качеството на разговора. Тази технология изисква и

допълнителна апаратура от двете страни на канала за връзка. WLAN стеганографията се базира на стегометоди, които предават стегограми в безжичните локални мрежи. Практически пример за такава стеганография е системата HICCUPS (Hidden Communication System for Corrupted Networks) [16]. През 2003 год. са разработени видеопоточни стеганографски методи по подобие на стеганографията в изображения, но позволяващи скритото транспортиране на голямо количество секретна информация в поточни графични файлове.

От края на деветдесетте години на XX век досега в Интернет са разпространени над 2000 стеганографски, и стотици стеганалитични програми от 8 поколения с различен лицензионен статут. Съществуват много източници за обзор на тези стеганографски програми (т.н. steganography tools), данни за най-популярните от тях са обобщени в [5,15,17,18]. Методите в пространствената област се използват най-често от стегопрограмите заради доброто скриване (незабележимост) на съобщенията, големия стегокапацитет и лесната реализация. Два нови алгоритъма за стеганографска защита може да са представени в [34] и [35]. Според специалистите, полезни за практиката съвременни софтуерни средства от Интернет сега са OpenPuff v.4.0, SecretLayer Pro, Our Secret, QuickStego и Ultima Steganography. Желаещите да използват достъпните в Интернет стегопрограми обаче трябва да са наясно, че вероятността за откриване на скрити с тях съобщения от правоохранителните органи е почти 100%. Стегопрограмите, които имат приемлива надеждност в това отношение, са с голяма изчислителна сложност за кодиране на данни в реално време. Такива програми едва ли се предоставят за публично ползване [19].

Има и други съвременни технологии и средства за скриване на съобщения – холографски технологии; инфрачервени програмируеми устройства за ръчно управление на компютри; пейджери; цветни стъкла, които филтрират всички дължини на вълните, без предназначените да направят видими скритите послания; различни магнитни, фотохромни и термохромни мастила; жаргонен език и HTML код. Този списък не трябва да

се счита за изчерпателен, има много други възможности [15]. Съществуват и методи за скриване на данни в изображения, с използване на судоку-пъзелите като ключ. Възможните ключове са колкото са възможните решения на судоку, т.е те са 6,71x1021. Това е еквивалентно почти на 70-битов ключ, което го прави много по-силен отколкото 56-битовия ключ, използван в криптиращия метод DES.

Развитието на компютърните технологии позволи използването на „некомпютърни” контейнери, базиращи се на постиженията на биохимията. Съвременните микробиологични технологии дават възможност за практическото използване на ДНК – молекулите като стегоконтейнери. Тези молекули имат микроскопични размери и при това съдържат огромно количество информация. Най-елементарният начин за скриване на информация е генерирането на молекула ДНК, зависеща само от изходното съобщение и секретния ключ. ДНК-контейнерът може да се смеси с мастило и да се изпрати в писмо по пощата, или да се внедри в генетичната структура на организма, на когото принадлежи модела на използваната ДНК-молекула [20].

III. Използването на он-лайн глобалните услуги и мобилните комуникции за стеганографска комуникация

От първите он-лайн социални мрежи – ОСМ (OSN), стартирани в Интернет през 1999 г., досега в киберпространството са известни над няколко стотин такива мрежи. Най-популярни ОСМ са Facebook, Twitter, Linkedin, Pinterest,Google Plus+, VK, Flickr, MeetMe и ClassMates. Докато нормалните потребители на ОСМ използват тази технология за комуникация и информационен обмен, същата технология се използва като инструмент на тероризма за комуникация, кибер-атаки, пропаганда, набиране на нови членове, обучение и др.Сега 90 % от терористичната дейност в Интернет се осъществява с използване на инструментите на ОСМ [21] .

Разкриване на скритите канали в ОСМ изисква изучаването и тестването на различни стегано техники и софтуер в условията на платформите, предоставяни от операторите на мрежите.

Направените изследвания в три социални мрежи – Facebook, Badoo и Google+ показват, че Facebook е сравнително най-добре защитена срещу използването й за стегокомуникации [22]. Екипи от лаборатория „Компютърна сигурност“ на Шуменския университет и ГИНХ-Махачкала, с участието на студенти от Русия и България, проведоха тестове за ОСМ Facebook, Google+, Одноклассники, Вконтакте (VK), Мой Мир, Instagram, Tumblr и Linkedin [23]. Като контейнери при тестовете се използваха графични и аудиофайлове и различни хардуерни платформи, за взаимодействие със социалните мрежи. Проведените експерименти потвърдиха, че не е възможно използването на безпрепятствена стеганография в албуми във Facebook и VK. При споделяне на снимки чрез Google+ е реализиран успешно целият цикъл на стеганографска комуникация от вграждане до извличане на скрити съобщения със формати JPEG, PNG, BMP и GIF.

Наред с предимствата на облачните услуги възникват и редица проблеми, един от най-сериозните от които е сигурността и защитата на потребителските и фирмените данни. Основните доставчици на облачни услуги, като Google (Gmail, Google Doc), Microsoft (Azure), Amazon (Amazon Web Services), Cisco (WebEx) използват понякога сложни протоколи и инфраструктури, подходящи и за контейнери – носители на секретни данни. Стеганографията трябва да се счита за нарастваща заплаха за изчисленията в облак [24].

Поради разнообразието и сложността на облачните услуги, специалистите са песимисти относно създаването на универсални и ефективни стеганалитични методи и средства.

Стеганографията чрез мобилните телефони и PDA е по-трудна, защото изисква достъп до операционната система на мобилното устройство.

Вече има разработени програмни продукти за мобилни телефони, много от които са общодостъпни (фиг. 3). Популярни стеганографски приложения за ОС Android са Steganography, Photo Hidden Data, Steganografia, Steganography Application, Stegosaurus. Steganography Master, Steganography Image, Stegano Imessage, Stegano Lookup, Barcode Steganography, Pocket Stego,

MobiStego, Da Vinci Secret Image Pro, Stegais, PixelKnot, Secret Letter, Crypsis Eye, Stegos. С тези приложения секретно съобщение може да бъде скрито в графично изображение или фотографии, направени с камерата на мобилното устройство.

Фиг. 3

IV. Информационната сигурност и стеганологична подсистема за защита на информацията (СПСЗИ)

Система за защита на информацията (СЗИ) е комплекс от мерки, реализирани от няколко подсистеми за защита – антивирусна, защитна стена, криптозащита и др. Изграждането им трябва да се осъществява на базата на моделирането на

заплахите и атаките към компютърните системи на потребителите [25].

Като всяка технология за сигурност, стеганографията не е идеална и не покрива всички изисквания за секретност, но тя удовлетворява много от изискванията за секретна комуникация, понякога в комбинация с други методи като криптографията.

Стеганологичната защита (стегозащита) е комплекс от организационни и апаратно-програмни мерки за предотвратяване на стегоинциденти. Може да се определят два основни аспекта на стегозащитата:

1. Защита на секретна информация срещу изтичане с използване на методи на стеганализа.

2. Стегозащита на информацията срещу несанкциониран достъп чрез скриване на malware в безобидни на пръв поглед мултимедийни файлове [5].

Системният подход при разработването на СЗИ изисква стегозащитата да се реализира от стеганологична подсистема за защита на информацията (СПСЗИ) е част от СЗИ. СПСЗИ е съвкупност от апаратни и програмни средства за защита на информацията в компютърните системи и мрежи чрез методите на стеганографията и стеганализа.

Варианти на архитектури на СПСЗИ са представени в [5,26].

Разкриването на каналите за изтичане на конфиденциална информация и организиране на ефективно противодействие на съществуващите възможности за използване на стеганографските методи е важна задача с цел пресичане на престъпната дейност [27].

За защита от стегоинциденти трябва да се използват най-съвременни програмни методи и средства. Едно от тези решения са системите DLP (Data Leakage/Lost Prevention). Обаче повечето от разпространените версии на тези системите за защита от изтичане на данни или нямат в състава си модули за стеганализ, или той не е активиран. Разработват се перспективни системи за стеганализ на данни – SDP (Stegano-graphy Detection Prevention).

Стерилизацията на изображения може да има важно приложение в областта на информационната сигурност и защита. В този сценарий, зашумяването на съобщение, без да променят характеристиките на изображението, е възможна защита от злоупотреби със стеганография. Проблемите на стерилизацията се разглеждат в [28].

Стеганологията широко се коментира в Интернет, най-новите са на Steganology.com и хеш-тага #steganology от https://twitter.com/hashtag/steganology.

Според много специалисти, StegAlyzerRTS (Steganography Analyzer Real-Time Scanner) на Backbone Security е най-добрият достъпен на пазара стеганалитичен програмно-апаратен комплекс за мрежова сигурност. Той открива в режим на реално време стеганографски приложения и техните сигнатури, скрити в безобидни на пръв поглед файлове, които се изпращат на външни получатели по електронна поща или към общо достъпни сайтове [29].

Постоянно развиващите се стегометоди отправят нови предизвикателства към стеганалитиците и компютърните следователи. Универсалните инструменти, които могат да открият и класифицират стеганографска активност все още се намират в стадий на начално разработване.

Допълнително като мерки за стегозащита м трябва да се отбележи и възможността за защита на информацията чрез използването на възможностите на стеганографията за вграждане на стегомаркер с информация за произхода, собственика, разпределението и предоставянето на секретни документи. Маркерите са вградени по такъв начин, че дори когато обектът е променен или преправен, те остават.

Започвайки от 1996 год., всяка година расте броя на публикациите, посветени на стеганографията и стеганализа. Широко се използват резултатите и постиженията на такива учени като J. Fridrich, H. Kim, R. Anderson, C. Cachin, N. Provos, H. Farid, K. Sullivan, G. J. Simmons, P. Honeyman, W. Bender, I. Pitas, Cox и др. Интересна книга в тази област е [6], в която са цитирани 470 публикации от целия свят. Чрез Интернет са

достъпни и редица дисертации от САЩ, Русия и Великобритания.

V. Обучението на специалисти по стеганология в чужбина и у нас

Несъмнено една от основните мерки за стеганологична защита е създаването на добре подготвени специалисти в тази област. За целта фирми-производители на апаратни и програмни средства за защита, като MacFee, Wetstone, Backbone Security и др. провеждат краткосрочни и дългосрочни курсове за обучение. С това се занимават и редица академии, фондации и организации.

В много висши учебни заведения по света се работи активно по обучението на специалисти по защита на информацията, и се провежда сериозна изследователска работа по създаване на програмни и технически средства за защита. Научните изследвания като правило се финансират от мощни корпорации и заинтересовани държавни агенции. В редица учебните курсове по информационна сигурност, а даже и като отделни дисциплини се преподават въпросите на стеганологията. Известни са частични данни за обучението на специалисти в университети на САЩ, Великобритания, Русия, Германия, Полша, Чехия, Китай, Индия, Финландия,Румъния, Турция, Белгия, Испания, Португалия, Нова Зеландия и др.

Известната специалистка по стеганология проф. Jesica Fridrich от SUNY Bingham University, NY, САЩ, преподава от 2006 год. дицсиплината „Fundamentals of steganography“ и развива научно-изследователска дейност в областта на стеганографията и стеганализа, основно със студенти. В Полша екипът на проф. Krzysztof Szczypiorski във Варшавската политехника работят по авангардни проекти по мрежова стеганография със студенти. В Русия въпроси на стеганографията се преподават в над 110 висши учебни заведения [30].

Интересна форма за развитие на методите за стеганализ от млади изследователи е периодично провежданото международно състезание по стеганализ BOSS (Break our steganography system) за разбиването на специално разработения за целта стегометод HUGO [31]. През м. юни 2011 г. състезанието е спечелено от

студентския отбор на проф. Fridrich с коефицент на откриваемост при стеганализа – 0,82.

Получените резултати от научно-изследователската работа на водещите университети имат такава практическа ценност, че много от техните автори доброволно спират да ги публикуват в научния печат за да предотвратят тяхното използване от престъпни елементи и групировки.

У нас по проблемите на стеганографията се извършва научно-изследователска работа в Шуменският Университет „Епископ Константин Преславски“, ТУ-Варна, ТУ-София, ИИТ на БАН и др. За пръв път във висше учебно заведение у нас от 2010 год. в Шуменския Университет се преподава учебната дисциплина „Компютърна стеганография” за студенти от специалностте „Компютърна информатика“ и „Компютърни информационни технологии“ [32]. От 2004 год. досега са защитени над 23 бакалавърски и магистърски дипломни работи, има над 36 съвместни научни публикации на преподаватели и студенти. За подпомагане на обучението на студентите, от преподавателите от катедра КСТ на ФМИ са издадени монографията „Стеганологична защита на информацията“, и „Ръководство за упражнения по стеганография“ [5,33]. В рамките на научно-техническия обмен с ПГУТИ-Самара са обменени 2 учебни пособия и софтуер за мрежова стеганография.

Повишава се научната квалификация на преподавателите – през 2014 г. са защитени 2 докторски дисертации в тази област и е избран един професор. Осъществява се научно-техническо сътрудничество с Института по отбраната, университети във Варшава, Русия (Москва, Самара и Махачкала), ИИТ на БАН, УНИБИТ и НВУ, Политехника- Букурещ и др. През 2012 в учебно- изследователската лаборатория „Компютърна сигурност“ бе монтирана клъстерна компютърна система „Радиан-М“, разработена от колектив от ШУ. В тази лаборатория се работи по стеганография и стеганализ в паралелна компютърна среда, реализирани са 8 проекта по стеганология, с участие на преподаватели, студенти и докторанти. Постепенно се формира

ново направление не само за ШУ – компютърна стеганология в паралелни компютърни среди.

През 2014 и 2016 год. в Шуменския Университет бяха организирани и проведени два международни научни семинари по стеганография – ШУСТЕГ14 и ШУСТЕГ16. Специалисти в областта на стеганографията и стеганализа от нашата страна и чуждестранни университети обсъдиха направления за практически изследвания в областта на стеганографията и стеганализа във ВУЗ, и се обсъждаха научни публикации по тематиката на семинара.

Развитието на компютърните технологии и мобилните комуникации неминуемо ще отправят нови предизвикателства към обучението на специалисти по високотехнологична стеганография, и те трябва да има готовност за тяхното посрещане. Ролята на висшите учебни заведения трябва да остане водеща в процеса на обучението им.

Стеганографията ще се развива в съответствие със степента на изучаването на средата, в която се предават секретните съобщения. За предаване и скриване на ценни данни ще се използват фантастични от днешна гледна точка методи и контейнери. Заедно с такива, които използват зрителни и акустични образи, най-вероятно ще се използват и контейнери, свързани с други човешки чувства – осезание, обоняние, вестибуларен апарат. В най-бизко време стеганографията и противодействието на стеганографията ще имат същата актуалност, както проблемите с новите концепции BigData или Internet of Things (IoT), могат да се очакват и нови заплахи за информационната сигурност. Създателите на зловреден софтуер, престъпните организации, терористите и др. организации, за да прикрият своите криминални дейности, е не само вероятно, но и сигурно, че ще развият и използват нови методи на стеганографията и други авангардни технологии. Специалистите в областта на информационна сигурност трябва да са готови да посрещнат тези предизвикателства.

ЛИТЕРАТУРА

1. **Cox, I., Miller, M., Bloom, J. Fridrich, J., T. Kalker.** Digital Watermarking and Steganography, Second Edition. Elsevier, Morgan Kaufmann Publishers, 2008.
2. **Аграновский, А., А. Балакин , В. Грибунин, С. Сапожников.** Стеганография, цифровые водяные знаки и стеганоанализ. Москва, Вузовская книга, 2009. ISBN 978-5-9502-0401-2.
3. **Conway, M.** Code Wars: Steganography, Signals Intelligence, and Terrorism. Knowledge, Technology and Policy (Special issue entitled ‘Technology and Terrorism’) Vol. 16, No. 2 (Summer 2003): [онлайн]. [прегледан 28.05.2012]. http://doras.dcu.ie/494/1/know_tech_pol_16 _2_ 2003.pdf.
4. **Илиев, И.** Симпатични мастила, „скари“ и цифрови шифри, използвани от Васил Левски в периода 1870–1872 г.В:Исторически преглед, 2005, № 5–6, 62–63.
5. **Станев, С.** Стеганологична защита на информацията. Университетско издателство „Епископ Константин Преславски”. Шумен, 2013. ISBN 978-954-577-825-4. 320.
6. **Fridrich, J.** Steganography in Digital Media: Principles, Algorithms, and Applications. Cambridge University Press, 2010.437 p. ISBN 978-0521190190.
7. **Network Steganography Principles.** [онлайн]. [прегледан 20 февруари 2013] http://www.stegano.net/tutorial/net-steg.html.
8. **Zielinska,E., W. Mazurczyk, K. Szczypiorski.** The Advent of Steganography in Computing Environments.[онлайн].[прегледано 20 май 2013]. http://arxiv.org /ftp/arxiv/papers/ 1202/ 1202 .5289.pdf.
9. **Stoyanov, B.P.** Using Circle Map in Pseudorandom Bit Generation, in 6th AMiTaNS’14, AIP CP 1629, 2014, pp. 460–463, doi: 10.1063/1.4902309.
10. **Kordov, K.** Modified pseudo-random bit generation scheme based on two circle maps and XOR function, Applied Mathematical Sciences, Vol. 9, 2015, no. 3, 129-135.
11. **Stoyanov, B., Kordov, K.** A Novel Pseudorandom Bit Generator Based on Chirikov Standard Map Filtered with Shrinking Rule, Mathematical Problems in Engineering 2014, Article ID 986174, 2014, 1-4.
12. **Stoyanov, B.** Pseudo-random Bit Generation Algorithm Based on Chebyshev Polynomial and Tinkerbell Map, Applied Mathematical Sciences, Vol. 8, 2014, no. 125, 6205-6210, http://dx.doi.org/10.12988/ams.2014.48676.

13. **Террористы и стенография.** [онлайн]. [прегледан 11 ноември 2014]. http://anmal.narod.ru/crypto-gram/steganography.html].
14. **Judge, J.** Steganography: Past, Present, Future. SANS Insitute, 2001. [онлайн].[прегледан 19 април 2012]. http://www.sans.org/reading_room/ whitepapers/stenganography/steganography-past-present-future/552.php.
15. **Ilchev, S., Z. Ilcheva.** A new approach to Data Hiding for Web-based Applications. Prof. Marin Drinov Academic Publishing House, Sofia, 2014. ISBN 978-954-322-780-8, 151.
16. **Lubacz, J., W. Mazurczyk, K. Szczypiorski.** Voice over IP. IEEE Spectrum, February, 2010, 37-46.
17. **Станев, С.** Софтуерни продукти за стеганализ. В: Сборник научни трудове на Научна конференция 2013 „Защита на личните данни в контекста на информационната сигурност“, Факултет АПВОКИС на НВУ „В.Левски“. Шумен, 2013, 157-164.
18. **Алиев, С., Д. Тончев.** Нови стеганографски програми в Интернет. В: Сборник научни трудове на международната научна конференция MATTEX14, Том 1, ISBN 1314-3921. Шумен, 2014. стр.167-172.
19. **Ghost stories.** [онлайн]. [прегледан 11.12.2012]. http://vault.fbi.gov/ ghost-stories-russian-foreign-intelligence-service-illegals/documents/item-87/view.
20. **Алексеев, А., В. Орлов.** Стеганографические и криптографические методы защиты информации (Учебное пособие). Самара, ИУНЛ ПГУТИ , 2010 . 330 с. ISBN 978-5-904029-12-8.
21. **Ishengoma, F.R.** Online Social Networks and Terrorism 2.0 in Developing Countries. International Journal of Computer Science & Network Solutions. December.2013-Volume1.No 4. ISSN 2345-3397. [онлайн].[прегледан 11 юни 2014]. http://arxiv.org/ftp/arxiv/papers/1410/1410.0531.pdf.
22. **Chee, A.** Steganographic Techniques on Social Media: Investigation Guideline. [онлайн]. [прегледан 20.10.2013]. http://aut.researchgateway.ac.nz/bitstream/handle/ 10292/ 5577/CheeA.pdf?sequence=3.
23. **Галяев, В.** О некоторых экспериментах по передаче стегосообщений через социальные сети. В: Сборник научни трудове на международната научна конференция MATTEX14, Том 1, ISBN 1314-3921. Шумен, 2014. 119-122.
24. **Mazurczyk, W., K. Szczypiorski.** Is Cloud Computing Steganography-proof? [онлайн].[прегледан 20.10.2014] http:// arxiv.

org/ftp/arxiv/papers/1107/1107.4077.pdf.
25. **Nachev, A., S. Zhelezov.** Assessing the efficiency of information protection systems in the computer systems and networks. Информационные технологии и безопасность, Журнал Акад. наук Украины. Спец. выпуск, Киев, 2013, 79-86.
26. **Zhelezov, S., H. Paraskevov, H. Hristov, P. Boyanov, B. Uzunova-Dimitrova.** An architecture of staganological subsystem for information protection. Proceedings of ICBBM 2014, Volume 10, RTU Press, Riga, 2014. ISBN 978-9934-10-573-9. 123-128.
27. **Станев, С., Х. Христов, Д. Апостолов.** Предизвикателства на компютърната и мрежова стеганография към дейността на фирмените служби за сигурност. В: Наука, образование,сигурност. София: Издателство на НБ, 2013. 277-284. ISBN:978-954-535-796-1.
28. **Goutam, P., I. Mukherjee.** Sterilization of Stego-images through Histogram http://worldcomp-proceedings.com/proc/p2012/SAM9764.pdf.
29. **Steganography Analyzer Real-Time Scanner (StegAlyzerRTS).** [онлайн]. [прегледан 5.05.2013]. http://www.sarc-wv.com/products /stegalyzerrts/learn_more.aspx.
30. **Галяев, В.** Современный уровень преподавания стеганографии в России. В: Сборник научни трудове на международната научна конференция MATTEX14, Том 1, Шумен, 2014. стр.115-119. ISBN 1314-3921.
31. **HUGO.** [онлайн]. [прегледан 21.05.2013]. http:// www.agents.cz/boss/.
32. **Станев, С., С. Железов, Х. Параскевов.** Обучението по компютърна стеганография в Шуменския университет „Епископ Константин Преславски“. Наука, образование, сигурност. София: Издателство на НБУ, 2013. стр.445-451. ISBN:978-954-535-796-1.
33. **Станев, С., С. Железов, Х. Параскевов, Х. Христов.** Ръководство за упражнения по стеганография. Университетско издетелство „Епископ Константин Преславски“, 2015, ISBN 978-619-201-011-9. 140.
34. **Zhelezov, S.** Modified Algorithm for Steganalysis. Mathematical and Software Engineering 1(2), 2015, 31-36, http://varepsilon.com/index.php/mse/article/view/9.
35. **Stoyanov, B., Zhelezov, S., Kordov, K.** Least Significant Bit Image Steganography Algorithm Based on Chaotic Rotation Equations. Comptes rendus de l'Académie bulgare des Sciences 69(7), 2016, 845-850. http://www.proceedings.bas.bg/PDF16/g_07_03.pdf.