Державна служба України з надзвичайних ситуацій
Львівський державний університет безпеки життєдіяльності
Навчально-науковий інститут цивільного захисту
Кафедра управління інформаційною безпекою

«Допущено до захисту»
Начальник кафедри управління
інформаційною безпекою
_____Р.Л. Ткачук
«___» _____ 2021 року

ДИПЛОМНА РОБОТА МАГІСТРА

на тему Захист інформації в соціальних мережах з використанням стеганографічних алгоритмів

Виконав:
студент 2-го курсу, групи КБ-61м
спеціальності 125 "Кібербезпека"
_Сагановський Борис Анатолійович____
(прізвище, ім'я, по батькові)

Керівник ____Лагун А.Е._____
(прізвище та ініціали)

Рецензент____Машевська М.В._____
(прізвище та ініціали)

Львів – 2021

АНОТАЦІЯ

Сагановський Б.А. "Захист інформації в соціальних мережах з використанням стеганографічних алгоритмів". Дипломна робота магістра за спеціальністю 125 "Кібербезпека" складається з текстової частини, що містить 3 розділи, 88 с., 22 рис., 23 джерел.

Об'єкт – стеганографічні алгоритми.

Предмет – методи забезпечення захисту інформації у вигляді текстів і нерухомих зображень в соціальних мережах.

Мета роботи – використання стеганографічних методів для захисту інформації в соціальних мережах, зокрема методів текстової стеганографії та стеганографії в зображеннях.

Методи дослідження – вбудовування цифрових повідомлень з використанням двійкової системи числення, заміна молодшого значущого біта, перетворення Фур'є, вейвлет перетворення.

В роботі проведено аналіз та досліджено атаки в соціальних мережах та способи захисту від них. Здійснено класифікацію стеганографічних алгоритмів залежно від типів контейнерів і досліджено колірні моделі для формування цифрових нерухомих зображень. Виявлено можливості використання методів текстової стеганографії та стеганографії в зображеннях для захисту інформації в соціальних мережах. Розроблено програмне забезпечення для використання при передаванні інформації в соціальних мережах.

СТЕГАНОГРАФІЯ, СТІЙКІСТЬ, ШИФР, ЗОБРАЖЕННЯ, ТЕКСТОВИЙ ФАЙЛ, СОЦІАЛЬНА МЕРЕЖА, АТАКА.

ABSTRACT

Saganovsky B.A. “Protection of information in social networks using steganographic algorithms”. Master's diploma work of speciality 125 "Cybersecurity" consist of 3 chapters of the textual parts, 88 pages, 22 figures, 23 sources of the literature.

Object – steganographic algorithms.

Subject – methods of ensuring the protection of information in the form of texts and still images on social networks.

The purpose – use of steganographic methods to protect information in social networks, in particular methods of text steganography and steganography in images.

Research methods – embedding digital messages using a binary number system, replacement of the least significant bit, Fourier transform, wavelet transform.

The work analyzes and investigates attacks on social networks and ways to protect against them. Also are investigated the classification of steganographic algorithms depending on the types of containers is carried out and color models for the formation of digital still images.

At the next step we have been identified possibilities of using the methods of text steganography and steganography in images to protect information on social networks . The practical result is developing of software for use in the transmission of information on social networks.

STEGANOGRAPHY, STABILITY, CIPHER, IMAGE, TEXT FILE, SOCIAL NETWORK, ATTACK

ЗМІСТ

ВИСНОВКИ

1. У випадку забезпечення соціотехнічного захисту виділяються певні типи загроз від зловмисників, якими є такі, що пов’язані з комп’ютерами, різні види шахрайства з грошовими засобами, а також викрадення конфіденційної інформації.

2. При організації атак з використанням соціальної інженерії першими жертвами зловмисників є начальники, адміністратори і звичайні користувачі, які мають різні права доступу до інформаційних ресурсів, тому при використанні методів захисту варто застосовувати криптографічні та стеганографічні алгоритми.

3. Встановлено, що при побудові стеганографічних алгоритмів необхідно враховувати атаки на стеганографічні системи, які подібні до криптографічних атак, а саме атаку з використанням стеганограми, атаки з відомим і обраним контейнером, атаку з обраним повідомленням.

4. У випадку використання текстової стеганографії в соціальних мережах приховування даних в тексті використовуються методи довільного інтервалу, синтаксичні методи, які працюють з пунктуацією і семантичні методи, які пов’язані з маніпулюванням словами.

5. Якщо для приховування використовують нерухомі зображення, то у таких випадках використовуються методи приховування в просторовій і частотній областях. Перші з них є простими, але нестійкими до найпростіших стеганографічних, другі використовують перехід в спектральну область і основною проблемою є забезпечення точності.

1. Розроблено і досліджено програмне забезпечення мовою C++, яке реалізує методи текстової стеганографії і стеганографії з використанням нерухомих зображень.

2. Набільшу ефективність з розроблених для використання в соціальних мережах має програма, що приховує текст в нерухомому зображенні за

допомогою методу молодшого значущого біта. Найбільшою проблемою в цьому випадку є забезпечення стеганографічної стійкості зображення із прихованою інформацією, особливо до атак з використанням афінних перетворень.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бурнашов С. В. Проектування та розроблення відкритих wifi-мереж з функцією збирання інформації про пристрої / С. В. Бурнашов, Ящук В. І. // Інформаційна безпека та Інформаційні технології: збірник тез доповідей IV Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 27 листопада 2020 року. Львів, ЛДУ БЖД, 2020, 249 с. (С.121-124).
2. Бурячок, В.Л. Алгоритм оцінювання ступеня захищеності спеціальних інформаційно-телекомунікаційних систем / В.Л. Бурячок // Захист інформації. – 2011. – № 3 (52). - С. 19-27.
3. Бурячок, В.Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа. – К.: ДУТ, 2015.- 288 с.
4. Войтович В.С., Гриник Р.О. Дослідження проблематики кібербезпеки України. Зб. наук. праць XII Міжнар. наук.-практ. конф. молодих вчених, курсантів та студентів “Проблеми та перспективи розвитку системи безпеки життєдіяльності” (м. Львів, 23-24 березня 2017 р.). [в 2 ч.]. Ч. 2. – Львів: ЛДУ БЖД, 2017. С. 11–12.
5. Войтович В.С., Гриник Р.О. Основні безпекові проблеми кіберпростору України. Зб. тез доповідей Міжнародна науково-практична конференція “Інформаційна безпека в сучасному суспільстві” (м. Львів, 24-25 листопада 2016 р.). Львів : ЛДУБЖД, 2016. С. 23–24.
6. Иванов В. Текстовая стеганография: метод двойных пробелов между словами [Электронный ресурс] / Иванов В. – 2012. – Режим доступа : http://www.nestego.ru/2012/05/blog-post_12.html
7. Конахович Г. Ф. Компьютерная стеганография. Теория и практика / Г. Ф. Конахович, А. Ю Пузыренко. – К. : МК-Пресс, 2006. – 249 с.
8. Кузнецов, М.В. Социальная инженерия и социальные хакеры / М.В. Кузнецов, И.В. Симдянов. – СПб.: БХВ-Петербург, 2007. - 368 с.
9. Кухарська Н. П. Аналіз стеганографічних методів довільного інтервалу / Кухарська Н. П. – Вісник ЛДУ БЖД. – 2016. – № 14. – С. 7-16.
10. Лагун А.Е. Використання стеганографічних алгоритмів для приховування текстової інформації / А.Е. Лагун // Збірник наукових праць «Вісник ЛДУ БЖД». – Львів : ЛДУ БЖД, 2018. –№ 18. – С. 49-56.
11. Лагун А.Е. Особливості приховування інформації в зображеннях з використанням молодшого значущого біта / А.Е. Лагун, О.І. Полотай // Збірник

наукових праць «Вісник ЛДУ БЖД». – Львів : ЛДУ БЖД, 2020. –№ 20. – С. 17-22.

12. Лагун А.Е., Полотай О.І. Особливості приховування інформації в зображеннях з використанням молодшого значущого біта. Вісник ЛДУ БЖД. – 2019. –№ 20. – С. 17-22.

13. О.Белей, Н.Мальцева, О.Полотай Фізичний зміст комп'ютерної стеганографії. Вісник Львівського Державного університету безпеки життєдіяльності Том 23 (2021): С. 27-32.

14. Полотай О.І., Гриник Р.О. Застосування генетичного алгоритму для розкриття ранцевої криптосистеми Меркля-Хелмана Вісник ЛДУ БЖД. – 2016. – Т. 21, № 2. – С. 201-206.

15. Полотай О.І., Гриник Р.О. Побудова інтелектуальної моделі криптоаналізу шифру Рабіна на базі генетичного алгоритму. Інформаційна безпека та комп'ютерні технології" ("Information Security and Computer Technologies"): Збірник тез доповідей Міжнародної науково- практичної конференції, 24-25 березня 2016 року, м. Кіровоград: КНТУ, 2016. – С. 24-26.

16. Семенов, Ю.А. Обзор по материалам ведущих фирм, работающих в сфере сетевой безопасности [Електронний ресурс] / Ю.А. еменов.— Режим доступу: http://book.itep.ru/10/2012.htm

17. Ящук В. І. Онтологія наукових досліджень та методологія наукового пізнання / В.І. Ящук // Економіка в контексті глобальних змін суспільства: матеріали Міжнародної науково-практичної конференції (м. Дніпро, 18 липня 2020 р.). – Дніпро: НО «Перспектива», 2020. – 140 с. (С.100-104).

18. BMP file format. Wikipedia, the free encyclopedia. Retrieved from https://en.wikipedia.org/wiki/BMP_file_format.

19. Examining port scan methods – Analyzing Audible Techniques [Електронний ресурс]. – Режим доступу: http://www.windowsecurity.com/whitepapers/xamining_port_scan_methods_Analyzing_Audible_Techniques.html.

20. Lagun A. Embedding of the hidden information with the use of Discrete Fourier Transform [Electronic resource] / A. Lagun, N. Kukharska // Automatic Control and Information Technology (ICACIT'17) : 4th International Conference, 14-16 December 2017 : Proceedings. – Cracow, 2017. – 1 electr. opt. disk (CD-ROM).

21. O.Polotai, Kukharska, N., Lagun, A. The steganographic approach to data protection using arnold algorithm and the pixel-value differencing method. Proceedings of the 2020 IEEE 3rd International Conference on Data Stream Mining and Processing, DSMP 2020, 2020, pp. 174–177.

22. Peter Neumann. Computer-Related Risk. ACM Press/Addison Wesley, 1995.

23. Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. 2nd ed. / B. Schneier. – New York : John Wiley and Sons, 1996.