УДК 004.056

Ворожбит М.В.
Куперштейн Л.М.

АНАЛІЗ МЕТОДІВ І ЗАСОБІВ ВИЗНАЧЕННЯ ПРИХОВАНИХ КАМЕР

Анотація

Робота присвячена дослідженню методів та засобів детектування прихованих камер спостереження. Проаналізовано як програмні інструменти на основі звичайного смартфону, так і спеціалізовані апаратні засоби.

Ключові слова: *засіб відеоспостереження, прихована камера, смартфон.*

Abstract.

The work is devoted to the study of methods and means of detecting hidden surveillance cameras. Both software tools based on a regular smartphone and specialized hardware are analyzed.

Keywords*: video surveillance device, hidden camera, smartphone.*

Вступ

На сьогодні візуально-оптичний канал витоку інформаціє є одним із найбільш використовуваних та технічно оснащених [1]. Зловмисники, які хочуть отримати секретну інформацію, зазвичай встановлюють мініатюрні закамуфльовані камери відеоспостереження в непомітних місцях. Крім того, сучасні засоби є досить технологічними і дозволяють отримувати не тільки відеоінформацію, але і у фото- та аудіоформаті. Також сучасні відеокамери можуть не тільки накопичувати значні об’єми в автономному режимі, але і передавати їх засобами технлогії WI-FI або GSM [1].

Небезпека таких засобів стоїть гостро не тільки для приватного сектора, але і державного також. Так, наприклад, у 2017-му р. у кабінеті співробітника НАЗК Олександра Писаренка було виявлено приховану камеру, на якій знайшли відеоматеріали із різними переговорами та інші робочі процеси співробітника [2].

Доступність засобів, що можуть використовуватися як приховані камери, та їх широкі функціональні можливості актуалізує розробку нових ефективних методів та засобів їх детектування.

Результати дослідження

До найпоширеніших місць, де можна заховати приховані камери в приміщенні можна віднести детектори диму, обладнання для повітряних фільтрів, книги, електричні розетки, настільні рослини, м’які ведмедики,

лампи та ін. [3]. Для їх виявлення прихованих використовують різні методи.

Перший метод. Оглядання приміщення у темряві з використанням звичайного електричного ліхтаря або ліхтаря мобільного телефону [4]. Якщо в темряві направити світло ліхтаря на стіни або стелі, можна буде побачити об'єктив камери. У місцях, де з'явилися відблиски, є ймовірність знайти приховане джерело відеоспостереження.

Другий метод. Використання власного смартфона без використання спеціального програмного забезпечення та спеціального обладнання [3].

Простий ліхтарик мобільного телефону підійде для огляду приміщення у темряві для виявлення відблиску лінзи прихованої камери. У деяких випадках можна навіть обійтися без ліхтарика. Багато шпигунських камер використовують інфрачервоне підсвічування для зйомки в темряві. Він невидимий для людського ока, але не для камери смартфона. Під час зйомки в темряві джерело інфрачервоного світла з’явиться на екрані у вигляді пульсуючої точки.

Серед переваг даного метода є його безкоштовність, відсутність необхідності мати спеціальні навички та спеціальне обладнання.

Серед недоліків можна віднести те, що не всі моделі телефонів підходять для роботи, такий процес забирає багато часу ну і при цьому можливі помилкові спрацьовування, а камери без інфрачервоного випромінювання не можна спостерігати взагалі.

Третій метод. Використання власного смартфона з використанням спеціального програмного забезпечення.

Програмне забезпечення таке як HCD [6], Spy Camera Detector, Spy Detector (IOS) з використанням технологій штучного інтелекту можуть в реальному часі розпізнавали приховані камери, які не змогли детектуватись людським оком [3].

Серед переваг даного метода є відсутність необхідності мати спеціальні навички та спеціальне обладнання.

Серед недоліків можна віднести значні витрати на розробку та навчання інтелектуальної системи, хибні спрацювання.

Четвертий метод. Використання спеціальних технічних засобів.

У даний час на ринку є багато різних засобів для виявлення прихованих камер, кожен із яких має свій метод роботи. До таких методів входять: перехоплення по радіо хвилях, виявлення через інфрачервоне випромінюванню, виявлення через електромагнітне випромінювання, візуальне виявлення [3].

Серед переваг даного метода є: ефективність, можливість регулярних перевірок.

Серед недоліків можна віднести те що: коротка ефективна дальність, ціна, вимоги до часу та навичок.

В нижче в наведеній таблиці деякі засоби наведено приклади засобів для виявлення прихованих камер[5].

Таблиця 1 – Вигляд засобів для виявлення прихованих камер.

Фото	Назва	Технічні характеристики
	K68	Радіочастотний: Так Магнітний: Так Прихована лінза: Так Інфрачервоний: Так Діапазон частот: 1 МГц - 8 ГГц (GSM, Wi-Fi, BT, UHF) Дисплей сили сигналу: круглий світлодіодний 10-бар Ціна: 250 €
	Troncase A9	Радіочастотний: Так Магнітний: Так Прихована лінза: Так Інфрачервоний: Так Діапазон частот: 1 МГц - 8 ГГц (GSM, Wi-Fi, BT, UHF) Дисплей сили сигналу: круглий світлодіодний 12-бар
	Jepwco G4 Pro	Радіочастотний: Так Магнітний: Ні Прихована лінза: так Інфрачервоний: Ні Діапазон частот: 1 МГц - 6,5 ГГц (GSM, Wi-Fi, BT, UHF) Відображення потужності сигналу: 5-полосний світлодіод (6-е світло ввімкнено/вимкнено) Ціна: 102 €
	Latnex SPA-6G (Аналізатор спектру)	Радіочастотний: Так Магнітний: Ні Прихована лінза: Ні Інфрачервоний: Ні Діапазон частот: 15 МГц – 2,7 ГГц і 4,85 ГГц – 6,1 ГГц (Wi-Fi) Відображення потужності сигналу: 5-полосний світлодіод (6-е світло ввімкнено/вимкнено) Ціна: 389 $

	Kaxyuya (Детектор магнітного поля та електро-магнітних хвиль)	Радіочастотний: Так Магнітний: Так Прихована лінза: Так (окремо, в упаковці) Інфрачервоний: Ні Діапазон частот: 1 МГц - 6,5 ГГц (GSM, Wi-Fi, BT, UHF) Індикатор сили сигналу: 10-бар світлодіодний Ціна: 270 $

З наведеної таблиці видно, що всі засоби схожі по функціоналу. Але кожен із наведених пристроїв має своє вузьке направлення на детекцію.

Мінусом є те, що такі засоби є не дешевими, а також для роботи із ними потрібні спеціальні навички.

Висновки

В результаті аналізу методів і засобів визначення прихованих камер отримано, що кожен із методів й засобів мають свої плюси та мінуси.

Методи для не навченої людини будуть мало ефективні для виявлення камер. Оригінальні засоби мають великий набір функціоналу для детектування камер, але вони мають велику ціну.

Тому було б доцільно розробити програмний засіб з перевагами кожного методу та засобу та детекції на основі смартфона, навченого штучного інтелекту.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. https://studfile.net/preview/9650062/
2. https://gordonua.com/ukr/news/localnews/-u-kabineti-spivrobitnika-napk-pisarenko-znajshli-prihovanu-kameru-zmi-217253.html
3. https://www.kaspersky.com/blog/how-to-find-spy-cameras/43199
4. https://reolink.com/blog/how-to-detect-hidden-cameras/#-1-Scan-the-Environment-Carefully-to-Detect-Suspicious-Hidden-Video-Cameras
5. https://www.digitalcameraworld.com/buying-guides/best-hidden-camera-detector
6. https://www.hcdapp.com/

Ворожбит Михайло Вікторович – студент групи 2БС-18б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м.Вінниця, e-mail: misha_vorozhbyt@ukr.net

Куперштейн Леонід Михайлович – к.т.н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця email: kupershtein.lm@gmail.com

Vorozhbyt Mykhailo V. – Student of Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, e-mail: misha_vorozhbyt@ukr.net

Kupershtein Leonid M. — PhD, Associated Professor of Information Protection Chair, Vinnytsia National Technical University, Vinnytsia, email: kupershtein.lm@gmail.com