

АНАЛІЗ МЕТОДІВ ВИЯВЛЕННЯ ПРИХОВАНИХ ВІДЕОКАМЕР

Вінницький національний технічний університет

Анотація

У роботі розглянуто основні методи виявлення прихованих відеокамер, що використовуються для несанкціонованого відоспостереження, проаналізовано їх переваги та недоліки, а також визначено доцільність комбінованого використання різних технологій у залежності від умов середовища та характеру інформаційної діяльності.

Ключові слова: приховані камери, відеоспостереження, конфіденційність, безпека, методи виявлення прихованих камер.

Abstract

The article discusses the main methods of detecting hidden video surveillance cameras, analyzes their advantages and disadvantages, as well as the feasibility of combining different technologies depending on environmental conditions.

Keywords: hidden cameras, video surveillance, privacy, security, methods of detecting hidden cameras.

Вступ

З розвитком технологій зростає і ризик їх використання для несанкціонованого отримання інформації — особливу загрозу становлять приховані камери. Такі пристрої можуть бути непомітно вмонтовані в побутові предмети та працювати в різних режимах - від локального запису до передачі даних через Wi-Fi або GSM. Це становить реальну загрозу для конфіденційності та безпеки, як у приватному, так і в державному секторі, а малі розміри та методи маскування таких пристроїв значно ускладнюють їх виявлення. Мета цієї роботи - проаналізувати існуючі методи виявлення, порівняти їх, а також запропонувати інтегровану систему, що поєднає переваги кількох підходів для підвищення ймовірності виявлення.

Результати дослідження

Одними з найбільш доступних методів виявлення прихованих камер є візуальна перевірка та інфрачервоне виявлення. Ручна перевірка передбачає візуальний огляд приміщення з ретельним оглядом усіх елементів інтер'єру та предметів. Метод не вимагає спеціального обладнання та є ефективним у невеликих приміщеннях, однак його точність залежить від уважності користувача і розміру об'єкта. Інфрачервоне виявлення використовує камеру смартфона для фіксації ІЧ-випромінювання, яке випромінюють камери для зйомки в темряві. Воно невидиме для людського ока, але може бути зафіксоване як пульсуючі точки. Метод простий, доступний і не потребує витрат, однак залежить від моделі телефону та наявності ІЧ-підсвічування. У разі сильного ІЧ-фону можливі випадкові спрацювання. Підвищити ефективність можна за допомогою спеціалізованих пристроїв з більшою чутливістю або додатків для смартфонів, хоча останні можуть давати помилкові спрацювання через обмеження апаратного й програмного забезпечення [1].

Також, варто зазначити, що ефективним методом пошуку камер є також радіочастотні (RF) детектори, які дозволяють виявляти активну передачу даних від бездротових камер через сканування радіосигналів. Це метод, що дозволяє зафіксувати аномальні радіочастотні випромінювання, характерні для камер, які передають дані через Wi-Fi або Bluetooth. Наприклад, детектори, такі як K68 та Troncase A9, можуть виявляти широкий діапазон частот, що охоплюють найпоширеніші протоколи бездротових передач, такі як GSM, Wi-Fi та Bluetooth. Проте цей метод має свої обмеження: він не здатен виявляти камери, що не передають дані через бездротові канали, а також не реагує на камери, що записують інформацію на пам'ять або використовують нестандартні протоколи [2, 3].

Ще одним потужним методом є аналіз мережевого трафіку. За допомогою спеціальних алгоритмів

машинного навчання, таких як методи підтримки векторних машин (SVM), можна виявити характерні патерни даних, які передають камери через мережу. Цей метод дозволяє виявити бездротові камери, які активно передають дані в мережі, і використовуються для моніторингу великих мереж, де фізичний огляд може бути важким. Однак, як і у випадку з RF-детекторами, цей підхід не ефективний для камер, що не передають дані через мережу або використовують нестандартні канали передачі [4].

Метод виявлення електромагнітного випромінювання також має свою важливу роль у виявленні прихованих камер. Камери під час роботи випромінюють електромагнітні сигнали, і спеціалізовані системи здатні використовувати амплітудно-модульовані коливання цих сигналів для виявлення камер, незалежно від способу передачі даних. Цей метод має суттєву перевагу, оскільки здатен виявляти як бездротові, так і дротові камери, проте для його застосування необхідне спеціалізоване обладнання, таке як програмно-визначене радіо (SDR) [5].

Термальна зйомка є ще одним перспективним методом, що дозволяє виявляти теплові сигнатури, які створюються активними електронними компонентами камер. Завдяки компактним тепловізійним сенсорам, таким як HeatDeCam, можна виявити камери, що активно працюють, за їх тепловими слідами. Однак цей метод також має свої обмеження, зокрема залежність від температурних умов навколишнього середовища та впливу зовнішніх факторів, таких як освітлення або температура [2].

Для маленьких приміщень, таких як готельні номери, оптимальним є поєднання ручної візуальної перевірки з ліхтариком та інфрачервоного виявлення за допомогою смартфона. Це дозволить швидко виявити видимі камери або ті, що знімають в темряві. У разі необхідності можна використовувати радіочастотний детектор для перевірки бездротових камер. Для великих приміщень, як офіси чи конференц-зали, найкращими методами будуть аналіз мережевого трафіку за допомогою алгоритмів машинного навчання та радіочастотні детектори. Це дозволить виявити камери, які передають дані через Wi-Fi чи інші бездротові канали. Додатково можна застосувати метод виявлення електромагнітного випромінювання для пошуку прихованих камер. У складних умовах, як сховища чи складські приміщення, ефективно працюватимуть термальні камери для виявлення теплових слідів камер, а також метод електромагнітного виявлення для фіксації сигналів від працюючих пристроїв.

Висновки

Аналіз існуючих методів виявлення прихованих камер показав, що кожен з них має свої переваги та обмеження в залежності від конкретних умов. Для ефективного виявлення необхідно комбінувати різні технології, такі як інфрачервоне виявлення, радіочастотний аналіз, термальну зйомку. Інтегровані системи, що поєднують кілька методів, дозволяють підвищити точність та ефективність виявлення, що особливо важливо для великих або складних об'єктів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. How to find hidden cameras (5 methods for detection). Norton AntiVirus, Privacy, Identity, & Advanced Scam Protection. URL: <https://us.norton.com/blog/how-to/how-to-find-hidden-cameras> (date of access: 06.04.2025).
2. Zhiyuan Yu, Zhuohang Li. HeatDeCam: Detecting Hidden Spy Cameras via Thermal Emissions. CCS '22: 2022 ACM SIGSAC Conference on Computer and Communications Security.
3. Lee D. M., Juniper A. The best hidden camera detector: easily find bugs, trackers and spy cams. digitalcameraworld. URL: <https://www.digitalcameraworld.com/buying-guides/best-hidden-camera-detector> (date of access: 06.04.2025).
4. Cowan K. K. Detecting Hidden Wireless Cameras through Network Traffic Analysis : thesis. 2020. URL: <http://hdl.handle.net/10919/100148> (date of access: 06.04.2025).
5. CamRadar / Z. Liu et al. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies. 2022. Vol. 6, no. 4. P. 1–25. URL: <https://doi.org/10.1145/3569505> (date of access: 06.04.2025).

Григорук Надія Романівна – студентка групи 2БС-226, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: grigoruknadia15@gmail.com

Катаєв Віталій Сергійович – асистент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Вінниця, kataev@vntu.net

Григорук Надія - student of group 2BS-22b, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: grigoruknadia15@gmail.com

Vitaliy Kataiev – assistant of the Department of Management and Security of Information Systems; Vinnytsia National Technical University, Vinnytsia, kataev@vntu.net