УДК 004.056.53

В. Я. Усатюк
В. С. Катаєв

АНАЛІЗ МЕТОДІВ ВИЯВЛЕННЯ ШПИГУНСЬКИХ ПРИСТРОЇВ

Вінницький національний технічний університет

Анотація

Дана робота присвячена аналізу методів виявлення шпигунських пристроїв, які становлять серйозну загрозу інформаційній безпеці. Розглянуто різні типи шпигунських пристроїв, їх технічні характеристики та принципи роботи. Особливу увагу приділено технічним та візуальним методам виявлення, включаючи радіочастотний аналіз, огляд нелінійних переходів, тепловізійний аналіз. Розглянуто особливості виявлення в різних умовах використання шпигунських пристроїв та профілактичні заходи.

Ключові слова: закладні пристрої, шпигунство, несанкціонований доступ, захист інформації.

Abstract

This work is devoted to the analysis of methods for detecting spy devices that pose a serious threat to information security. Various types of spy devices, their technical characteristics and principles of operation are considered. Particular attention is paid to technical and visual detection methods, including radio frequency analysis, inspection of nonlinear transitions, thermal imaging analysis. Features of detection in different conditions of use of spy devices and preventive measures are considered.

Key words: embedded devices, espionage, unauthorized access, information protection.

Вступ

У сучасному світі, де інформація є ключовим ресурсом, а різноманітні пристрої для несанкціонованого отримання інформації широко поширені і практично знаходяться у вільному доступі, питання інформаційної безпеки набуває особливої актуальності. Шпигунські пристрої, такі як приховані камери та мікрофони, GPS-трекери становлять серйозну загрозу для конфіденційності та безпеки, як окремих осіб, так і організацій. Таким чином, постає питання аналізу сучасних методів виявлення шпигунських пристроїв та можливості їх застосування на реальних об’єктах інформаційної діяльності.

Результати дослідження

Шпигунське обладнання, яке раніше було доступне лише спецслужбам, тепер може придбати практично кожен, дане обладнання використовується для крадіжки особистих даних, промислового шпигунства та стеження за конкурентами. Можливість виявляти шпигунські пристрої є критично важливою для захисту конфіденційності, а ігнорування цієї загрози може призвести до витоку цінної інформації, фінансових втрат та порушення особистої безпеки.

Велику частину загроз становлять закладні пристрої (далі ЗП) або апаратні закладки. Вони являють собою мініатюрні передавачі, що встановляються безпосередньо у приміщенні де циркулює інформація з обмеженим доступом, а сигнали від них модулюються інформаційними сигналами. Проблема полягає у тому, що ЗП для знімання інформації можуть використовувати більшість існуючих каналів. Однак, найчастіше закладки слугують для перехоплення акустичної (мовної) та видової інформації, для цього можуть використовуватись:

- портативні диктофони, провідні мікрофони та мініатюрні відеокамери для прихованого звуко- або відеозапису;
- радіозакладки для передавання інформації з допомогою радіосигналів;
- мережеві закладки для передавання інформації по лініях електроживлення, телефонного зв’язку і т.д;
- акустичні телефонні закладки типу «електронне вухо».

Виявлення ЗП може здійснюватися двома способами: організаційним (візуальним) та технічним. Перший – це аналітична робота з визначення можливих місць встановлення ЗП із врахуванням особливостей їх роботи і візуальний огляд приміщення та пошук певних демаскуючих ознак в місцях можливого знаходження даних пристроїв. Другий – це локалізація апаратних закладок з допомогою спеціальної пошукової апаратури. Причому цей спосіб повинен враховувати всі технічні характеристики та особливості роботи ЗП, адже від принципу роботи закладки буде залежати і метод, яким можна буде цю закладку виявити.

Розберемо метод візуального огляду, який не вимагає спеціалізованого обладнання, але потребує уваги до деталей, зокрема існують певні ознаки, які вказують на потенційну загрозу, а саме [1]:

1) Нетипова поведінка технічних пристроїв. Іноді шпигунське обладнання видає себе через збої в роботі техніки:

- сторонні звуки під час телефонних розмов, незвичні шуми або перешкоди можуть свідчити про перехоплення сигналу.
- погіршення якості мобільного зв'язку, закладні пристрої, такі як радіожучки або приховані камери, можуть використовувати ті самі частоти, що й мобільні пристрої, що призводить до проблем зі з'єднанням.
- швидке розрядження акумулятора смартфона або іншого пристрою може бути наслідком роботи програм для моніторингу.

2) Нетипові предмети або зміни в обстановці.

- несподівані зміни в звичній обстановці, наприклад, поява нових розеток, світильників або елементів декору.
- сторонні предмети, залишені в несподіваних місцях, такі як ручки, годинники або брелоки.
- будь-які предмети, походження яких невідоме, повинні викликати підозру.

Постійний аналіз даних пунктів у приміщенні і являє собою метод візуального пошуку закладних пристроїв, головною перевагою даного методу є легкість його реалізації, оскільки він не потребує ніяких додаткових витрат, що робить його максимально доступним, але недоліком є низька надійність виявлення загроз.

Другий або технічний спосіб виявлення включає: контроль сигналів у лініях зв’язку та електроживлення; контроль радіовипромінювань у області об’єкту; контроль інфрачервоних випромінювань; використання приладів нелінійної локації, металодетекції та тепловізійних систем. Відповідно, цей спосіб вимагає великої бази різних пошукових пристроїв, при чому, в деяких випадках, конкретний пристрій може використовуватись для виявлення ЗП, які мають лише конкретні складові або характеристики.

Наприклад, для виявлення прихованих відеокамер використовується пристрій, робота якого заснована на ефекті "зворотного відблиску", суть якого полягає в створенні оптичного променю, який при попаданні на об’єктив відеокамери відбивається і поширюється у вузькому куті точно в напрямку зондуючого випромінювача при однопозиційній локації.

Використання тепловізорів для пошуку закладних хоч і має суттєві обмеження, все одно широко поширено, оскільки будь-який закладний пристрій буде нагріватись під час роботи, і навіть якщо він буде закамуфльований під якийсь об’єкт, то зміну температури все одно можна буде зафіксувати, при чому процес виявлення однаково ефективний для будь-якого типу закладки.

Найбільш проблемними з точки зору детектування є закладні пристрої, які не мають основних демаскуючих ознак у вигляді випромінювань сторонніх сигналів у радіоефір або у провідні мережі, а також пристрої, які працюють лише у визначений момент часу. Прикладом таких закладок можуть бути портативні диктофони, неактивні радіозакладки тощо. Для виявлення таких пристроїв використовують нелінійні локатори, принцип їх роботи оснований на опроміненні напівпровідникових елементів, що входять до складу закладок, зондуючим НВЧ-сигналом та аналізі перевипромінених сигналів [3].

Висновки

На сьогоднішній день шпигунські пристрої стали доступними для будь-кого, тому питання вміння їх знаходити, щоб захистити себе є актуальним. Як ми вияснили, іноді для вирішення цієї задачі достатньо уважно оглядати приміщення на підозрілі предмети та зміни у елементах інтер’єру, однак для більш складних випадків все ж необхідно використовувати спеціальні прилади, що можуть

виявляти приховані камери та мікрофони. Найкраще поєднувати обидва методи, оскільки деякі пристрої важко виявити лише одним шляхом. Важливо постійно дізнаватися про нові способи шпигунства, щоб бути в безпеці.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Як відбувається пошук шпигунського обладнання - етапи робіт | IT Ресурс. Resit. URL: https://resit.com.ua/yak-vidbuvaetsya-poshuk-zhuchkiv-ta-inshogo-shpigunskogo-obladnannya/ (дата звернення: 12.03.2025).
2. Яремчук Ю.Є., Катаєв В.С., Гижко М.Ю. Можливості практичного застосування тепловізорів у питаннях захисту інформації. — "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні" — 2016 — №1.- С.99-105.
3. Катаєв В.С. Дослідження проблеми локалізації закладних пристроїв при застосуванні нелінійної локації Тези доповідей, Тези доповідей II-ої Міжнародної науково-технічної конференції «Інформаційна безпека в сучасному суспільстві». – Львів, 2016. – С. 50–51.

Усатюк Віталій Ярославович – студент групи 1БКС-22Б, Факультет інформаційних технологій комп'ютерної інженерії, Вінницькйи національний технічний університет, Вінниця, vitalijusatuk582@gmail.com

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

Vitaly Usatyuk – student of group 1BKS - 22B, Faculty of Information Technologies of Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: vitalijusatuk582@gmail.com

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