

АНАЛІЗ МЕТОДІВ ВИЯВЛЕННЯ РАДІОЗАКЛАДНИХ ПРІСТРОЇВ

Вінницький національний технічний університет

Анотація

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

Ключові слова: радіозакладний пристрій, технічний захист інформації, метод виявлення, інформаційна безпека.

Abstract

The article introduces the main methods of detection of radio electronic embedded devices used for unauthorized collection of information are considered in the work, their advantages and disadvantages are analyzed, and the expediency of combined use of various technologies depending on the conditions of the environment and the nature of information activity.

Keywords: radio device, technical protection of information, detection method, information security.

Вступ

У сучасному інформаційному суспільстві захист конфіденційної інформації набуває особливої ваги, як у державному, так і в приватному секторах. Одним з найбільш небезпечних засобів несанкціонованого отримання інформації є радіоелектронні закладні пристрої (ЗП) — мініатюрні технічні засоби, здатні перехоплювати та передавати дані за допомогою радіохвиль. Завдяки стрімкому розвитку електроніки сучасні радіозакладні пристрої відзначаються високою компактністю, низьким енергоспоживанням і здатністю працювати в різних частотних діапазонах, що значно ускладнює їх виявлення. Загроза, яку становлять радіозакладні пристрої, є особливо актуальною в контексті гібридних конфліктів, комерційного шпигунства, а також для установ, діяльність яких пов'язана з обробкою персональних або державних таємниць.

Результати дослідження

Технічні засоби прихованого спостереження здатні передавати аудіо- або відеодані на відстані, використовуючи різні канали зв'язку, переважно в радіочастотному діапазоні. Їхня мініатюрність, автономність і можливість їх маскуванню під елементи інтер'єру або побутові прилади значно ускладнюють виявлення, особливо в умовах інформаційно насиченого середовища. Відповідно виникає потреба в чіткому розумінні існуючих методів виявлення радіозакладних пристроїв, їх класифікації, принципів дії та сфер доцільного застосування. Вибір відповідного методу обумовлюється низкою чинників: типом і характеристиками об'єкта обстеження, рівнем потенційної загрози, технічними параметрами ЗП, а також кваліфікацією персоналу, що здійснює пошук.

Закладні пристрої часто маскуються під звичайні предмети побуту, такі як наручні годинники, запальнички, калькулятори, попільнички тощо. Вони не відрізняються від звичних предметів, що дозволяє зловмисникам замінювати їх на схожі з вбудованими закладними пристроями. Для їх виявлення можна розібрати предмет або застосувати спеціальні методи виявлення, зокрема апаратні засоби [2]. Демаскуючі ознаки закладних пристроїв, які можна виявити за допомогою спеціальної техніки:

- наявність напівпровідникових елементів у пристрої;
- радіовипромінювання з модуляцією радіосигналу інформацією;

- наявність високочастотного сигналу в лінії електроживлення (зазвичай від 40 до 600 кГц, але можливі й сигнали до 7 МГц), що модулюється низькочастотним сигналом;
- зміна опору телефонної лінії від її звичайного значення при вимкненні телефону та закороченні лінії на розподільному щитку;
- падіння напруги (від кількох десятків до 1,5-2 В) в телефонній лінії при піднятій трубці, порівняно з іншими лініями, що підключені до того ж щитка [2].

Розгорнута класифікація методів виявлення радіозакладних пристроїв (ЗП), дозволяє глибше зрозуміти особливості різних підходів, які застосовуються у сфері технічного захисту інформації. Кожний з методів пошуку містить низку підходів, що базуються на специфічних властивостях радіозакладних пристроїв.

Перший - це метод пошуку ЗП як фізичних об'єктів. Вона охоплює традиційні способи виявлення, що не потребують високотехнологічного обладнання, але значною мірою залежать від досвіду та уважності оператора. Найпростішим, але все ще ефективним є візуальний огляд. Його суть полягає у ретельному обстеженні приміщення або об'єкта, в якому можуть бути приховані пристрої спостереження. Особлива увага приділяється місцям, де зміна зовнішнього вигляду або наявність додаткових елементів може свідчити про встановлення ЗП. До таких зон належать розетки, елементи освітлення, вентиляційні отвори, предмети інтер'єру або побутові прилади. Для підвищення ефективності огляду застосовують допоміжні засоби — дзеркала, ендоскопи, ліхтарі з направленим світлом, а також інфрачервоні або ультрафіолетові джерела світла, які можуть виявити сліди нещодавнього монтажу.

Також, до візуального контролю можна віднести контроль за допомогою засобів відеоспостереження. Йдеться про аналіз відеозаписів з камер, які могли зафіксувати момент встановлення ЗП або зміну обстановки в приміщенні. У сучасних умовах цей метод доповнюється алгоритмами комп'ютерного зору, що автоматично ідентифікують зміну об'єктів або появу сторонніх предметів. Проте сам по собі цей метод є непрямим: він не виявляє сам пристрій, а лише події, які могли свідчити про його встановлення.

Нелінійні радіолокатори (НР) у технічному захисті інформації використовуються для виявлення радіоелектронних закладних пристроїв, зокрема коли ці пристрої не є явними джерелами електромагнітних випромінювань. Принцип роботи НР базується на наявності в складі закладного пристрою радіоелектронних компонентів з нелінійними характеристиками (мікросхеми, транзистори, діоди тощо), що дозволяють збагачувати розсіяний сигнал від пристрою гармоніками. Джерелами помилкових спрацьовувань можуть бути контакти металів з оксидними шарами, які також здатні розсіювати перетворений спектр сигналу[3].

Наступний метод пошуку ЗП передбачає роботу з їхніми електромагнітними проявами, наприклад використання індикаторів поля. Це компактні пристрої, які фіксують наявність електромагнітного випромінювання в діапазонах, характерних для радіозакладок. Вони виявляють сигнал, який надходить у момент активної передачі інформації, а також фонове випромінювання, що може виходити від пристрою у режимі очікування. Водночас ці пристрої малочутливі до слабких сигналів, які маскуються в зашумленому середовищі або використовують сучасні способи модуляції.

Більш точним та гнучким інструментом є застосування спеціальних приймачів — таких як широкосмугові сканери, SDR-приймачі, спектроаналізatori. Вони дають змогу здійснювати високоточний аналіз спектра, визначати тип і параметри переданих сигналів, а також реєструвати дані для подальшого аналізу. Застосування таких засобів дозволяє виявляти навіть замасковані сигнали, особливо коли ЗП використовують нестандартні частоти або способи модуляції. Водночас ці засоби вимагають професійної підготовки оператора та достатнього рівня технічної оснащеності.

Комплекси радіоконтролю — це автоматизовані багатофункціональні системи, які поєднують у собі функції сканування, запису, аналізу та ідентифікації сигналів. Вони можуть працювати у фоновому режимі, постійно моніторити ефір і сигналізувати про появу невідомих або підозрілих джерел випромінювання. До складу таких комплексів входять приймальні антени, аналізатори спектра, бази даних дозволених сигналів, а також програмні модулі для порівняння та ідентифікації [4].

Таким чином, кожна з наведених методик має свої сильні сторони і обмеження, і в більшості випадків ефективно виявлення радіозакладних пристроїв передбачає комплексне використання кількох підходів, із залученням як візуального контролю, так і високотехнологічних електронних засобів виявлення. Це дозволяє мінімізувати ймовірність пропущених загроз і забезпечити надійний

рівень технічного захисту інформації.

Висновки

Отже, радіозакладні пристрої є реальною загрозою інформаційній безпеці, особливо в умовах широкого використання бездротових технологій та мініатюризації електроніки. Існуючі методи їх виявлення базуються на різних принципах – від аналізу фізичних ознак до виявлення електромагнітної активності, що дозволяє класифікувати підходи відповідно до технічних характеристик об'єкта спостереження. Комплексне використання технічних засобів та методик значно підвищує ймовірність успішного виявлення ЗП. Проте ефективність таких методів залежить від умов обстеження, типу загрози та кваліфікації персоналу.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Демаскуючі ознаки закладних пристроїв. ni.biz.ua - Навчальна Інформація для українських студентів. URL: http://ni.biz.ua/18/18_7/18_70375_demaskiruyushchie-priznaki-zakladnih-ustroystv.html (дата звернення: 09.04.2025).
2. Напівпровідникова радіореволюція та її наслідки - iac.com.ua. URL: <https://iac.com.ua/uk/news/napivprovidnikova-radiorevolucziya-ta-ii-naslidki/> (дата звернення: 14.04.2025).
3. Ідентифікаційні ознаки спектрального складу випромінювання демаскуючого розсіювача в нелінійній радіолокації [Текст] : дис. канд. техн. наук : 05.12.17 / Во Зуї Фук ; Нац. техн. ун-т України "Київ. політехн. ін-т ім. Ігоря Сікорського". - Київ, 2017. - 134, [3] арк. : рис., табл. - Бібліогр.: арк. 114-127.
4. Опорний конспект лекцій з дисципліни "Технічні засоби захисту інформації" для студентів освітньо-кваліфікаційного рівня «бакалавр», спеціальність «Кібербезпека» [Текст] / ЗУНУ. – Тернопіль : Західноукраїнський національний університет, 2023. – [87].

Василина Анастасія Василівна – студентка групи 2БС-226, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: nstvsln@gmail.com.

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

Anastasiia Vasylyna – Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia.

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