Наличие регулировки уровня ЭМПШ	Плавная регули-ровка на величину не менее 14 ДБ	Плавная регули-ровка уровня	Нет данных	Нет	Регулировка уровня	Нет	Нет	Нет	Режим «Пониже-ния мощнос-ти»
Наличие сигнализации исправной работы	Световая Отказ – «звукова я»	Нет данны х	Нет данных	Све-товая	Световая, звуковая	Выдача сигнала исправной работы на внешнее устройство	Отсут-ствует	Световая	Световая
Автомати-ческий контроль Наличие устройства блокировки	Выдача управля-ющей команды «Блоки-ровка»	Нет данны х	Отрут-ствует	Выдача управляю-щей команды «Блокиро в-ка»	Отсутствуе т	Отсут-ствует	Отсут-ствует	Выдача управляю щей команды «Блокиро вка»	Отсут-ствует
Вид антенны	Рамочны е, в 3-х плоскос-тях длиной до 12 м	Рамоч ные, в 3-х плоско с-тях длино й до 12 м	Рамоч-ная жесткая	Рамочны е, в 3-х плоскост ях	Заземляющ ий провод сетевого кабеля питания ПК	Рамочная мягкая, в каркасе системно го блока	Подстав-ка под монитор	Рамоч-ная мягкая, длиной 1,8м	Рамочная жесткая
Конструктивн ое исполнение	Стацио-нарный блок	Стаци-онар-ный блок	Стацио-нарный блок	Три выносны х малогаба -ритных блока	Установка в системный блок ПЭВМ на место НГМД 3,5	Бескорпу с-ной, устанав-ливается в блок компьют ера	Бескорпу с-ной, устанавл и-ваеяется в блок компьют ера	Выносно й блок	Малогаба -ритный блок с жесткой антенной
Назначение по применению	Защита ПК и помещен ия ВЦ	Защит а ПК и помещ ения ВЦ	Защита ПК	Защита ПК и помещен ия ВЦ	Защита ПК	Защита ПК	Защита ПК	Защита ПК	Защита ПК

Литература: ***1.*** *А. Д. Викторов, В. И. Генне, Э. В. Гончаров. Побочные электромагнитные излучения персонального компьютера и защита информации. //Защита информации. Конфидент, 1995, №1, с.38-42.* ***2.*** *В. П. Иванов, В. В. Сак. Маскировка информационных излучений средств вычислительной техники. //Защита информации. Конфидент, 1998, №1, с.144-148.* ***3.*** *В. Луценко, А. Архипов, В. Худяков. Особенности использования средств технической защиты информации от утечки за счёт побочных электромагнитных излучений и наводок //Сб. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – К: НТУУ «КПІ», СБУ. 2002- с. 178-182.*

УДК 681.3

ВИЯВЛЕННЯ ЦИФРОВИХ ДИКТОФОНІВ

Микола Нестеренко
Інформаційно-технічний центр КНУВС

Анотація: **Розглянуто технічне рішення виявлення цифрового диктофону за рахунок перехоплення та аналізу його паразитного електромагнітного випромінювання.**
Summary: **The technical decision of exposure digital is considered to the dictaphone due to the intercept and**

analysis of his parasite electromagnetic radiation.
Ключові слова: **Цифровий диктофон, випромінювання, виявлення, спектр.**

I Вступ

Цифрові диктофони (ЦД) набули широкого розповсюдження в різних сферах діяльності та побуті, завдяки своїм високим тактико-технічним та експлуатаційним характеристикам. Створюються загрози їх прихованого застосування з порушенням законодавства, прав і свобод людини. Тому, актуальним і, водночас, проблемним є своєчасне викриття ЦД, які застосовуються приховано. Деякі соціальні проблеми та загрози застосування сучасних високотехнологічних пристроїв, призначених для запису і передачі інформації, викладені в статтях [1, 2].

Наявність сервісних функцій (дистанційне керування, голосова активація запису тощо) і поєднання в одному пристрої різних функціональних можливостей підвищує ефективність використання цих пристроїв та ускладнює їх виявлення при здійсненні протиправних дій.

Цифрова апаратура запису та відтворення звуку має значні переваги порівняно з "традиційною" аналоговою апаратурою. Серед таких переваг:

– краща якість запису (більше співвідношення сигнал / шум);

– підвищена надійність роботи;

– стабільність параметрів запису;

– низький рівень паразитного випромінювання, а також безшумність роботи, що утруднює можливість виявлення диктофона;

– зручність та оперативність у роботі (розміщення записів у вигляді нумерованих файлів, яка дозволяє здійснювати практично миттєвий доступ до потрібного запису та можливість швидко видаляти фонограми);

– можливість оперативного перезапису фонограм на комп'ютер (через порт USB) без проміжних перетворень для подальшої обробки;

– стійкість до зовнішнього електромагнітного опромінювання та механічних навантажень;

– малі розміри диктофона та носія інформації тощо.

Технічне рішення, наведене нижче, спрямоване на вирішення проблеми витоку інформації і може бути використане в системах технічного захисту інформації та при проведенні пошукових заходів.

II Основна частина

Аналогові диктофони можуть бути виявлені спеціальною технікою на максимальній відстані від 0,2 м (носимі викривачі RM-100 (Росія), TRD-800 (США) до 0,6 м (стаціонарні викривачі диктофонів TRPC, RM-200 (Росія), PTRD 016 (США). Цифрові диктофони (ЦД) – на відстані від 0,2–0,3 м (носимий прилад ST-041 (Росія) до 0,5–0,7 м (стаціонарний комплекс ST-0110, Росія) [3].

Відомий носимий детектор радіопередавачів та диктофонів TRD-800 (США), який фіксує роботу лише аналогових диктофонів. Це відноситься і до стаціонарних детекторів TRFD-041 (Росія) і PTRD-081 (США) [4]. Для виявлення ЦД використовують портативний прилад ST–041 [5].

Відомий також стаціонарний програмно-апаратний комплекс ST 0110, який використовується для виявлення аналогових та цифрових диктофонів [6]. До складу даного пристрою входять: блок датчиків, блок комутації, блок підсилення і попередньої цифрової обробки сигналів, що надходять з датчиків, блок індикації, блок живлення, мінікомп'ютер. Принцип його роботи заснований на аналізі паразитних електромагнітних полів, які створюються працюючим аналоговим або цифровим диктофоном з наступною цифровою обробкою сигналів спеціально розробленими алгоритмами за допомогою комп'ютера. Загальними недоліками ST 0110 є:

– незначна відстань між пристроєм виявлення ЦД (детектором) і диктофоном та невелика надійність виявлення диктофону;

– значний час виявлення;

– необхідність оновлення програмного забезпечення з появою нових типів диктофонів;

– можливість застосування лише при стаціонарному режимі роботи;

- значне зниження надійності виявлення при роботі у складних електромагнітних обставинах.

Зазначені недоліки усуваються у запропонованому пристрої, заснованому на виявленні паразитних електромагнітних випромінювань працюючого ЦД, який відрізняється тим, що вихід рамкової антени з'єднаний з першим входом вузькосмугового приймача, перший вихід вузькосмугового приймача з'єднаний з першим входом блоку обробки і сканування, другий вихід вузькосмугового приймача з'єднаний з другим входом блоку управління і індикації, перший вихід блоку обробки і сканування з'єднаний з першим входом блоку управління і індикації, другий вихід блоку обробки і сканування

з'єднаний з третім входом вузькосмугового приймача, перший вихід блоку управління і індикації з'єднаний з другом входом вузькосмугового приймача, другий вихід блоку управління і індикації призначений для підключення засобів активного захисту, третій вихід блоку управління і індикації з'єднаний з першим входом вібросповісника, четвертий вихід блоку управління і індикації з'єднаний з другим входом блоку обробки і сканування та четвертим входом вузькосмугового приймача, перший вихід джерела живлення з'єднаний з входом стабілізатора живлення, другий вихід джерела живлення з'єднаний з другим входом вібросповісника, вихід стабілізатора живлення з'єднаний з п'ятим входом вузькосмугового приймача, третім входом блоку обробки і сканування та третім входом блоку управління і індикації [7].

Суть технічного рішення полягає в тому, що для виявлення ЦД використовується визначена кількість сканувань та його безперервність певних ділянок радіодіапазону і виявлення характерних частот випромінювання вузькосмуговим приймачем із подальшою обробкою одержаних даних шляхом застосування алгоритмів цифрової обробки сигналів та формування сигналу оповіщення.

Зазначені недоліки усуваються в запропонованому детекторі ЦД тим, що в ньому попередньо формується банк частот певних ділянок радіодіапазону, де знаходяться характерні частоти випромінювання різних диктофонів, які використовуються як критерії виявлення ЦД.

Спектр електромагнітного випромінювання ЦД знаходиться в діапазоні частот від десятків кілогерц до сотень мегагерц. Він нерівномірний по амплітуді та має характерні частоти (частоти зі значною потужністю випромінювання), які використовуються для виявлення диктофона під час його роботи.

Наприклад, при порівнянні спектрів випромінювання ЦД фірми Samsung різних моделей (SVR-B410, SVR-P140, SVR-S820,SVR-P220, SVR-P750, SVR-S1330) та кількох диктофонів однієї моделі, була відмічена майже їх ідентичність. При цьому характерні частоти випромінювання виявляються дещо різними у різних моделей диктофона та у різних ЦД однієї моделі. Девіація характерних частот спостерігалася також при змінюванні напруги живлення. Наприклад, в діапазоні частот 40-150 МГц девіація характерних частот складала 200-300 КГц. Таким чином, працюючий ЦД можна виявити шляхом сканування певних ділянок радіодіапазону та визначення його характерних частот випромінювання за допомогою вузькосмугового сканувального приймача.

В стаціонарному варіанті роботи при необхідності можна застосувати зовнішню резонансну систему (антену) з екрануванням приміщення для збільшення відстані виявлення та надійності визначення ЦД.

Функціональна схема запропонованого детектора ЦД наведена на рис. 1.

Пристрій містить рамкову антену (РА) 1 з одним виходом, вузькосмуговий приймач (П) 2 з двома виходами і п'ятьма входами, блок обробки і сканування (БОС) 3 з двома виходами і трьома входами, блок управління і індикації (БУІ) 4 з чотирма виходами (один з яких – 8 призначений для підключення засобів активного захисту) і трьома входами, вібросповісник (ВС) 5 з двома входами, джерело живлення (ДЖ) 6 з двома виходами, стабілізатор живлення (СЖ) 7 з входом і виходом. РА 1 призначена для прийняття сигналів – паразитних електромагнітних випромінювань від працюючого ЦД. П 2 призначений для підсилення, селекції, детектування сканованих сигналів та виявлення частот сигналів, що перевищують заданий рівень. Крок сканування, частоти сканування та кількість сканувань окремих ділянок радіодіапазону зберігаються у банку пам'яті, що входить до складу П 2. БОС 3 призначений для видачі дозвільного сигналу сканування (СС) на П 2, обробки і обчислення сигналів, що надходять з П 2 та видачу сигналу присутності працюючого ЦД в контрольованій зоні. БУІ 4 призначений для синхронізації роботи блоків, що входять до пристрою – управління роботою пристрою, відображення наявності імпульсних завад на сканованій ділянці радіодіапазону (стан радіоканалу), вибір способу сповіщення (вібро або світлова індикація), видачі сигналу активації засобів активного захисту (вихід 8 пристрою), відображення присутності працюючого ЦД в контрольованій зоні. ВС 5 призначений для прихованого сповіщення присутності працюючого ЦД у носимому варіанті застосування пристрою. СЖ 7 призначений для забезпечення стабільною напругою електроживлення блоків пристрою. ДЖ 6 призначений для електроживлення блоків пристрою.

Вихід РА 1 з'єднаний з першим входом П 2, перший вихід П 2 з'єднаний з першим входом БОС 3, другий вихід П 2 з'єднаний з другим входом БУІ 4, перший вихід БОС 3 з'єднаний з першим входом БУІ 4, другий вихід БОС 3 з'єднаний з третім входом П 2, перший вихід БУІ 4 з'єднаний з другим входом П 2, другий вихід (вихід 8 пристрою) БУІ 4 призначений для підключення засобів активного захисту (умовно не показано), третій вихід БУІ 4 з'єднаний з першим входом ВС 5, четвертий вихід БУІ 4 з'єднаний з другим входом БОС 3 та четвертим входом П 2, перший вихід ДЖ 6 з'єднаний з входом СЖ 7, другий вихід ДЖ 6 з'єднаний з другим входом ВС 5, вихід СЖ 7 з'єднаний з п'ятим входом П 2, третім входом БОС 3 та третім входом БУІ 4.

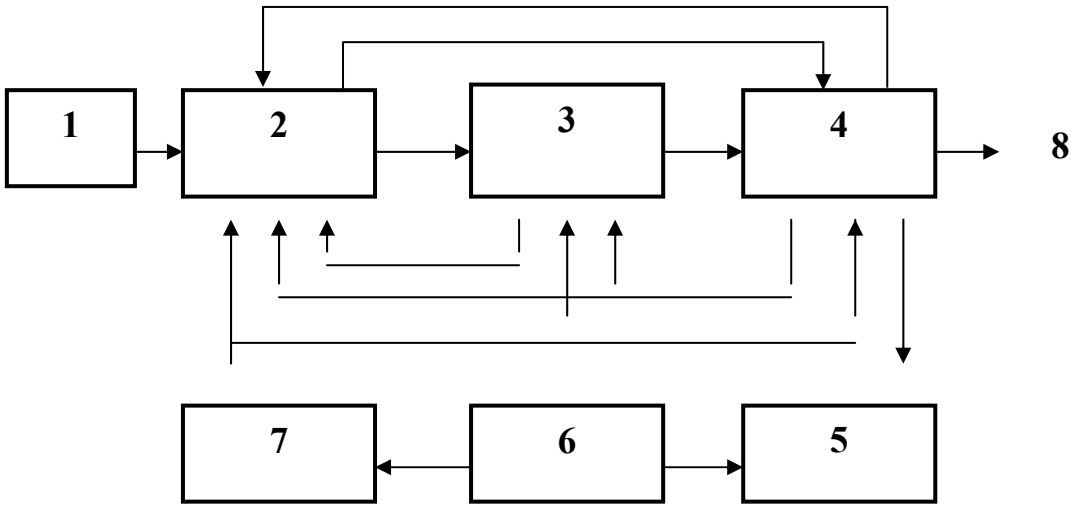

Рисунок 1 – Функціональна схема детектора цифрових диктофонів

1 – рамкова антена; 2 – вузькосмуговий приймач; 3 – блок обробки і сканування; 4 – блок управління і індикації; 5 – вібросповісник; 6 – джерело живлення; 7 – стабілізатор живлення; 8 – вихід на засоби активного захисту.

Калібрування пристрою проводиться при відсутності ЦД у контрольованій зоні. Перед початком роботи у БУІ 4 виставляється поріг на рівні шумової складової сканованого сигналу (можлива як ручна, так і автоматична адаптивна його установка), що приймається П 2, та про що сповіщає сигнал стану радіоканалу, який видається на БУІ 4 і фіксується світловим індикатором.

Пристрій працює таким чином. У початковому положенні роботи пристрою П 2 з заданою кількістю разів послідовно сканує попередньо занесені в банк пам'яті окремі ділянки радіодіапазону (ймовірного знаходження характерних частот) при дозвільному сигналі сканування, що надходить з БОС 4 на П 2.

При вмиканні ЦД, який перебуває в контрольованій зоні, випромінювання від нього приймається РА 1 і передається на П 2 із смугою прийому 10-12 кГц. На першому виході П 2 одержуємо імпульси, які перевищують поріг з тривалістю, що залежить від частоти сканування. Після подальшого їх формування, обробки та обчислення в БОС 3 за попередньо заданим алгоритмом на першому виході БОС 3 отримуємо сигнал присутності працюючого ЦД в контрольованій зоні. Про це сповіщає світлова індикація на БУІ 4 або ВС 5 (залежно від режиму роботи пристрою). На час роботи світлової індикації або ВС 5 (1 – 2 секунди) блокується робота П 2 відсутністю дозвільного СС з другого виходу БОС 3. При наявності сигналу присутності працюючого ЦД видається з БУІ 4 сигнал активації засобів активного захисту (вихід 8 пристрою) та з четвертого виходу БУІ 4 надходить сигнал на П2 та БОС 3 для блокування пристрою на час роботи засобів активного захисту.

При застосуванні детектора ЦД в стаціонарному режимі як зовнішню антену можна використати півхвильовий диполь, налаштований на діапазон знаходження характерних частот. Пристрій розміщується поряд з зовнішньою антеною для забезпечення індуктивного зв'язку з РА 1.

З метою підвищення надійності та збільшення відстані між пристроєм виявлення ЦД (детектором) і диктофоном в стаціонарних умовах у виділених для цього приміщеннях доцільно також проводити їх екранування від зовнішнього опромінювання (з урахуванням максимальної частоти зовнішнього електромагнітного опромінювання близько 2 – 3 ГГц). У приміщенні необхідно вимкнути всі джерела електромагнітного випромінювання (комп'ютери, радіотелефони тощо).

Якщо система виявлення ЦД входить до складу інтегрованої системи технічного захисту інформації, то прилади активного захисту повинні працювати в режимі розділення часу із роботою системи виявлення ЦД.

III Висновки

Запропонований детектор ЦД дозволяє:

– скоротити час виявлення диктофона за рахунок того, що скануванню та оцінці піддаються лише характерні ділянки спектру, а не весь спектр паразитного випромінювання ЦД;

– виявляти цифрові диктофони будь-яких моделей (пошук цифрових диктофонів з іншим спектром випромінювання здійснюється після доповнення банку характерних частот);

– динамічно формувати банк пам'яті характерних частот залежно від поставлених задач та умов роботи (надійність виявлення, час виявлення, наявність завад тощо);

– застосовувати пристрій у носимому або стаціонарному варіантах використання;

– значно підвищити відстань виявлення та надійність визначення ЦД за рахунок використання високочутливого вузькосмугового приймача.

Література: ***1.*** *Нестеренко М. П., Шорошев В. В. Соціальний та правовий аспекти масового застосування стільникових телефонів // Науковий вісник НАВСУ. Науково-теоретичний журнал. – Випуск № 2 . Частина 1. – К.: НАВС України, 2005 р. – С. 173 – 180.* ***2.*** *Шорошев В. В., Нестеренко М. П. Суспільно небезпечні дії з використанням стільникових терміналів // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. Науково-технічний збірник. – Випуск 10. – К.: ПП "ЕКМО", 2005. – С. 181 – 185 .****3.*** *Нестеренко М. П., Бєгов Д. Д. Цифровий диктофон – сучасний засіб фіксації звуку // Сучасні технології у судовій акустиці: Матер. міжнар. наук.-практ. семін. – К.: НАВС України, 2003. – С. 117 – 120.* ***4.*** *Защита информации. Поисковая техника. Звукозапись. // Каталог DAS. – К.: ООО "D.A.S", 1999. – С. 211.* ***5.*** *В. В. Домарев. Безопасность информационных технологий. Методология создания систем защиты. – К.: ООО "ТИД "ДС" , 2001. – С. 201.* ***6.*** *Защита информации. Звукозапись. Видеонаблюдение. Сигнализация // Каталог DAS. – К.: ООО "D.A.S", 2002. – С. 16.* ***7.*** *Патент України на винахід № 74218 С2, G 01 R 23/00 Детектор цифрових диктофонів / Жаріков Ю. Ф., Кондратьєв Я. Ю., Нестеренко М. П., Орлов Ю. Ю., Сущенко В. Д., Циганок О. Г. Національна академія внутрішніх справ України. - №2003054667; Заявл. 22. 05. 03. Опубл. 15. 11. 05. Бюл. № 11, 2005 р.*

УДК 681.3.06

ОРГАНИЗАЦИОННЫЕ И МЕТОДОЛОГИЧЕСКИЕ АСПЕКТЫ ЭКСПЕРТНОЙ ОЦЕНКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

Сергей Гладыш

Харьковский национальный университет радиоэлектроники

Аннотация: **Рассмотрена суть метода и основные этапы процедуры экспертной оценки. Выявлены особенности экспертной оценки информационной безопасности телекоммуникационных систем. Разработаны организационно-методические рекомендации по проведению экспертизы при оценке информационной безопасности телекоммуникационных систем.**

Summary: **The essence of method and the basic stages of expert evaluation procedure is considered. The features of information security expert evaluation of telecommunication systems are exposed. Organizationally-methodical recommendations are developed on the procedure of information security expert evaluation of telecommunication systems.**

Ключевые слова: **Экспертная оценка, риск, управление, информационная безопасность, телекоммуникационные системы, комплексная система защиты информации.**

I Введение

Современные информационно-телекоммуникационные системы (ИТС) предъявляют новые, более высокие требования к информационной безопасности (ИБ) [1, 2]. Актуальным направлением повышения эффективности комплексных систем защиты информации (КСЗИ) является применение в процессе управления ИБ адекватных математических методов и моделей. Однако, полная математическая формализация задач ИБ часто неосуществима вследствие их качественной новизны и сложности [3 – 5]. В связи с этим все шире используются экспертные методы, под которыми понимают комплекс логических и математико-статистических методов и процедур, направленных на получение от специалистов