УДК 621.37

Б.М. Клешня
О. П. Войтович

ДОСЛІДЖЕННЯ ВИКОРИСТАННЯ ІНДИКАТОРІВ ЕЛЕКТРОМАГНІТНОГО ВИПРОМІНЮВАННЯ

Вінницький національний технічний університет

Анотація

Статтю присвячено вивченню особливостей використання індикаторів електромагнітного випромінювання для пошуку та виявленні закладних пристроїв.

Ключові слова: закладні пристрої, радіозакладки, індікатори електро-магнітного випромінювання, перехоплення інформації.

Abstract

This article is dedicated to electromagnetic emission indication using features researching and eavesdropping devices search and detecting.

Keywords: eavesdropping devices, radio-eavesdropping devices, electromagnetic emission indicator, information intercepting.

Вступ

За сучасних умов інформаційне забезпечення стало важливою областю процесу управління. Воно полягає в зборі і переробці інформації, необхідної для прийняття управлінських рішень [1].

Незалежно від стрімкого поширення цифрових технологій у світі, невід'ємною частиною повсякденності залишаються голосові перемовини між людьми. Людина не завжди спроможна оцінити важливість інформації, що вона висловлює. Цим можуть скористуватись зловмисники, які, серед всього потоку речової інформації можуть вилучити дуже корисні, а іноді і секретні дані.

Сьогодні дуже широке поширення для незаконного отримання інформації знайшли радіомікрофони, або «жучки», як їх називають у просторіччі. Як і будь-який електронний пристрій, закладки мають певне електромагнітне випромінювання. Виявити це випромінювання і є завданням для індикаторів електромагнітного випромінювання [2].

Індикатори (детектори) електромагнітного поля дозволяють виявляти закладні пристрої, які в ході своєї роботи випромінюють електромагнітні хвилі. Детектори ефективно використовуються для виявлення і, що важливо, локалізації малогабаритних закладних пристроїв. Принцип дії подібних індикаторів полягає у виявленні місця з максимальним рівнем випромінювання і детальному огляді цього місця[3].

Дослідження методів виявлення закладних пристроїв

Основним каналом витоку на сьогодні є технічні засоби [4]. Це означає що перекриття цього каналу є важливим завданням для служб інформаційної безпеки.

Основні способи протидії несанкціонованому впливу на інформацію за допомогою технічних засобів поділяються на: виявлення закладних пристроїв, захист від несанкціонованого доступу до інформації шляхом перекриття технічних каналів витоку інформації за допомогою технічних засобів захисту інформації.

Виявлення закладних пристроїв складається з наступних методів:

1 – Методи пошуку закладних пристроїв як фізичних об'єктів з певними властивостями та характеристиками. До таких методів можна віднести: візуальний огляд місць можливого розташування закладного пристрою, також за допомогою застосування засобів спеціального підсвічування, дзеркал, збільшувального скла, контролювання важкодоступних місць за допомогою засобів відеоспостереження, використання металодетекторів, використання рентгенівського випромінювання.

2 – Методи пошуку, що використовують властивості закладних пристроїв як електронних систем. Дані методи складаються з: використання індикаторів поля, які реагують на наявність випромінювання закладного пристрою за рахунок використання радіо каналу при передачі інформації, а також дозволяють локалізувати їх місцезнаходження, використання спеціальних радіоприймачів для пошуку сигналу за заданими характеристиками та аналізу електромагнітного поля, використання автома-

тизованих комплексів радіоконтролю та виявлення закладного пристрою, дослідження та аналіз приміщення за допомогою нелінійних радіолокаторів [5].

Найбільш зручним в використанні способом виявлення закладних пристроїв є застосування індикаторів електромагнітного випромінювання. Ці пристрої володіють приймачами з дуже низькою чутливістю, що дозволяє точно виявити місцезнаходження пристрою.

Для передачі перехопленої інформації заставні пристрої можуть використовувати різні канали, однак їх можна розділити на дві великі групи - провідні та безпровідні. Закладні пристрої бездротового типу можуть передавати інформацію як по відомим стандартам стільникового зв'язку і бездротового доступу, так і за власними технологіями. Частота, на якій працює закладний пристрій залежить від безлічі факторів. Наприклад, використання низьких частот неможливо зважаючи на сильну зашумленості цієї смуги частот і необхідності мати антенні пристрої великого розміру і потужності. Використання ж високих частот обмежена, тому що зменшується дальність поширення радіохвиль.

За призначенням індикатори поля діляться на пошукові, сторожові (порогові) і комбіновані: пошукові детектори призначені для пошуку і локалізації закладних пристроїв, сторожові індикатори призначені для контролю рівня електромагнітного поля.

До основних параметрів і характеристик, що визначає ефективність індикаторів поля при пошуку закладних пристроїв, відносять: частотний діапазон, чутливість індикатора, динамічний діапазон вимірювання рівню вхідного сигналу, діапазон регулювання відносного нульового рівню сигналу, чутливість частотоміру, діапазон регулювання чутливості індикатора.

Частотний діапазон є однією з основних характеристик індикатора поля, що визначають його можливості з пошуку закладних пристроїв. Чутливість індикатора поля визначає граничні можливості по виявленню сигналів, тобто максимальну дальність виявлення закладного пристрою. Інтегральна чутливість сучасних індикаторів поля становить 0.6 - 5 мВ. Спектральна чутливість індикатора поля багато в чому залежить від характеристик антени і вхідного каскаду.

Висновки

Таким чином, на сьогодні, індикатори електромагнітного випромінювання є найбільш поширеними засобами для пошуку та виявлення електронних закладних пристроїв. Індикатори є дуже простими в використанні та експлуатації, мають компактні розміри та здатні виявляти майже будь-які типи закладних пристроїв. Також, в порівнянні з іншими засобами інформаційної безпеки, такі пристрої мають низьку ціну, що є значним фактором для деяких організацій.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Методичні вказівки до проведення практичних занять та до виконання самостійної й індивідуальної роботи з дисципліни „Основи науково-дослідної роботи / Укладачі: А. О. Азарова, В. В. Карпінець. – Вінниця: ВНТУ, 2013. – 44 с.
2. Лужецький В. А. Основи інформаційної безпеки [Текст] : навчальний посібник / В. А. Лужецький, А. Д. Кожухівський, О. П. Войтович. – Вінниця : ВНТУ, 2013. – 221 с.
3. Андрианов В.И. Шпионские штучки и устройства для защиты объектов информации, ISBN 5 - 86617 - 044 - 2; Санкт - Петербург, Лань, 1996г.
4. Хорев А.А. Техническая защита информации: учеб. пособие:В 3 - хт.Т. 1 : Технические каналы утечки информации / А.А.Хорев. - М. : НПЦ"Аналитика", 2008. - 436 с.
5. Каторин Ю.Ф., Куренков Е.В., Лысов А.В., Остапенко А.Н. Большая энциклопедия промышленного шпионажа, ISBN 5 - 8689173 - 106 - 1, Санкт - Петербург, ПОЛИГОН, 2000 г.

Клешня Борис Михайлович — студент групи 1БС-19м, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: 1bs15bklesnya@gmail.com

Войтович Олеся Петрівна — кандидат технічних наук, доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, email: voytovych.op@gmail.com

Kleshnya Boris M. — Student of 1BS-19m, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: 1bs15bklesnya@gmail.com

Voitoyich Olesya P. — Candidate of Technical Sciences, Docent of the Information Security department, Vinnytsia National Technical University, Vinnytsia, email: voytovych.op@gmail.com