УДК 004.415.056:658.115

А. О. Азарова
В. О. Гудзь
В. О. Блонський

УДОСКОНАЛЕННЯ ПІДХОДУ ДО ВИЯВЛЕННЯ РАДІОЗАКЛАДНИХ ПРИСТРОЇВ ЗА РАХУНОК ОДНОЧАСНОГО ПОЄДНАННЯ МЕТОДІВ ЛОКАЛІЗАЦІЇ ЗА РІВНЕМ ПОЛЯ ТА АКУСТИЧНОГО ЗВ`ЯЗУВАННЯ

Вінницький національний технічний університет

Анотація

У статті проаналізовано існуючі методи захисту інформації від витоку акустичним каналом, а також методи та засоби захисту від закладних пристроїв. Доведено доцільність інтегрування методів локалізації за рівнем поля та акустичного зв'язування з метою мінімізації часових витрат на виявлення радіозакладних пристроїв. Обґрунтовано необхідність розроблення пристрою, який буде виконувати функції кількох пристроїв водночас, що визначає не лише його функціональну, але й економічну доцільність.

Ключові слова: витік інформації, закладні пристрої, технічний захист інформації

Abstract

The article analyzes the existing methods of information security of leakage by the acoustic channel as well as security methods and means of against embedded devices. The expediency of integrating field-level localization and acoustic communication methods in order to minimize the time spent on detecting radio embedded devices has been proved. The necessity of developing a device that will perform the functions of several devices at the same time is substantiated. It determines not only its functional but also economic feasibility.

Keywords: information leakage, embedded devices, technical protection of informationю

Інформація – це будь-які відомості та (або) дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [1]. Інформація, втрата якої може спричинити шкоду особі, суспільству чи національним інтересам держави в будь-якій сфері повинна захищатися від несанкціонованого доступу до неї, тобто інформація повинна бути об'єктом захисту [2].

Захист інформації – комплекс правових, організаційних і технічних заходів і дій щодо запобігання загроз інформаційної безпеки та усунення їх наслідків в процесі збору, зберігання, обробки і передачі інформації в інформаційних системах.

Захист інформації місить в собі такі заходи:

– забезпечення фізичної цілісності інформації, виключення спотворень або знищення елементів інформації;

– недопущення підміни елементів інформації при збереженні її цілісності;

– відмова в несанкціонованому доступі до інформації особам або процесам, які не мають на це відповідних повноважень;

– придбання впевненості в тому, що передаються власником інформаційні ресурси будуть застосовуватися тільки відповідно до обговорених сторонами умовами.

Захищеність інформації – стан інформації, при якому забезпечена відповідність показників захищеності інформації нормам та вимогам захищеності інформації.

Технічний захист інформації (ТЗІ) – діяльність, спрямована на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації. Мета ТЗІ – запобігання витоку та (або) порушенню цілісності та доступності інформації, що підлягає захисту [3].

Об'єктом технічного захисту є інформація, що становить державну або іншу передбачену законодавством України таємницю, ІзОД, що є державною власністю чи передана державі у володіння, користування, розпорядження.

Інформація з обмеженим доступом в процесі інформаційної діяльності, основними видами якої є одержання, використання, поширення та зберігання ІзОД, може зазнавати впливу загроз її безпеці, у результаті чого може відбутися її витік або порушення цілісності інформації [3].

Найпоширеніший метод витоку інформації – через технічні канали витоку інформації (ТКВІ). Технічний канал витоку інформації (ТКВІ) – сукупність джерела небезпечного сигналу, середовища його поширення та засобу технічної розвідки. Тобто, технічним каналом витоку інформації є фізичний шлях носія інформації від його джерела до противника [4].

Одним із найбільш поширених ТКВІ є акустичний. Акустичні канали утворюються шляхом перехоплення мовних сигналів з ОІД акустичними мікрофонами направленої дії або акустичними антенами засобів технічної розвідки (ЗТР), які встановлюються за межами контрольованої зони (рис.1) [5].

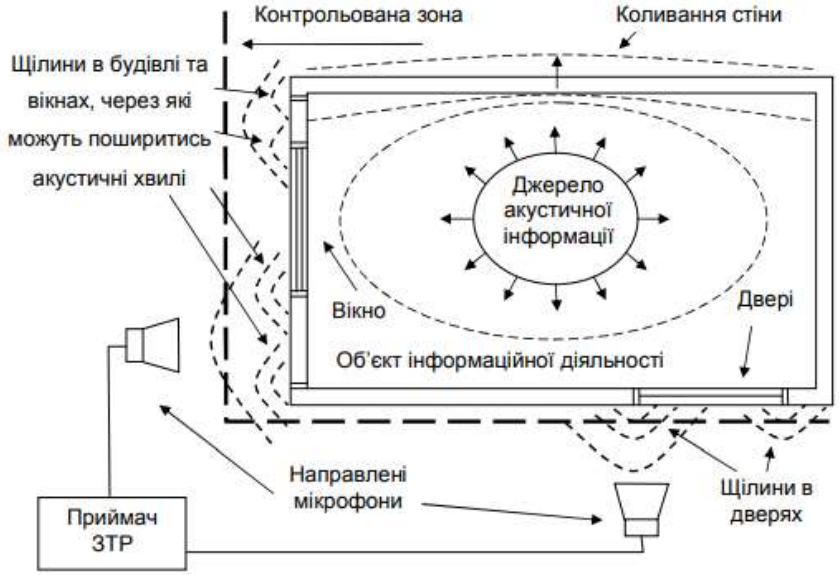

Рисунок 1 – Акустичні канали витоку інформації

Такий тип ТКВІ є найбільш «простим», саме тому він дуже часто використовується. Тому актуальним є розроблення пристрою, який буде здійснювати захист від витоку інформації таким каналом. Один із таких засобів є пристрій, що здійснює пошук радіозакладних пристроїв. Принцип його роботи базується на пошуку радіовипромінювань та реагуванню на них. Таких пристроїв на сьогоднішній день є дуже багато, саме тому пропонується поєднати функції кількох пристроїв у один, що буде зручніше та набагато здешевить його вартість.

Автори пропонують покращити можливості виявлення радіозакладних пристроїв шляхом поєднання трьох пристроїв у один, що, в свою чергу, дозволяє не лише більш точно локалізувати несанкціонований пристрій але й отримати певну інформацію про нього. Для досягнення цієї мети пропонується поєднати в один пристрій індикатор поля, частотомір та демодулятор.

Частотомір – це електровимірювальний прилад, що призначений для вимірювання частот різних періодичних коливань, електричних або механічних. Такі пристрої поділяються на вібраційні, електромеханічні, резонансні та цифрові [6].

Принцип дії цифрових частотомірів полягає в підрахунку числа періодів вимірюваних коливань за певний проміжок часу. Цифровий частотомір складається з формуючого пристрою, що перетворює синусоїдальну напругу вимірюваної частоти в послідовність однополярних імпульсів, тимчасового селектора імпульсів, що відкривається на певний проміжок часу (переважно від 10^{-4} до 10 с), електронного лічильника, який відраховує число імпульсів на виході селектора, та цифрового індикатора.

Демодуляція (детектування) сигналу – процес, виділення інформаційного (модулюючого) сигналу з модульованого коливання високої (несучої) частоти.

Демодулятор – пристрій, що здійснює розподіл сигналу на інформаційний та несучий (які утворюються в процесі модуляції сигналів). Це дає змогу відкинути несучий сигнал і працювати лише з інформаційним, тобто процес демодуляції сигналу, який передає закладний пристрій дозволить отримати детальну інформацію про закладний пристрій, та яку інформацію він передає.

Автори пропонують комбінувати ці всі пристрої у одне технічне рішення. Таке поєднання дозволяє мінімізувати час, оскільки для пошуку закладних пристроїв потрібно буде використовувати лише один пристрій, який виконуватиме функції трьох пристроїв. Запропонований пристрій дозволяє здійснити пошук закладних пристроїв, частотомір відобразити користувачеві частоту, на якій працює даний «шпигунський» пристрій, а демодулятор зчитати та відфільтрувати інформацію, що випромінює закладний пристрій. Такий підхід уможливлює не лише отримання синергічного ефекту [7-14] від застосування такого комплексного пристрою, а також знизити його собівартість порівняно з ринкової вартістю трьох окремих його складових-пристроїв.

Базою для запропонованого пристрою автори пропонують мікроконтролер Arduino UNO, оскільки дана платформа є найбільш гнучкою, зручною у використанні та має невелику вартість.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Закон України «Про інформацію». URL : https://zakon.rada.gov.ua/laws/show/2657-12
2. Іванченко С. О., Гавриленко О. В., Липський О. А., Шевцов А. С. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації. Навчальний посібник. К. : ІСЗЗІ НТУУ «КПІ», 2016. 104 с.
3. Зайцев А. П., Шелупанов А. А, Мещеряков Р. В., Скрыль С. В., Голубятников И. В. Технические средства и методы защити информации. М. : «Машиностроение». 2009. 508 с
4. Хорев А. А. Защита информации от утечки по техническим каналам. М. : НПЦ «Аналитика», 2008 р. С. 436–440.
5. Богуш В. М., Юдин О. К. Інформаційна безпека держави. К. : «МК-Прес», 2005. 432 с.
6. Куренков Е. В., Лысов А. В., Остапенко А. Н. Энциклопедия промышленного шпионажа / под общ. ред. Куренкова Е. В. С.-Петербург : ООО «Издательство Полигон», 1999, 512 с.
7. Азарова А. О., Погребняк О. В., Азарова Л. Є., Міронова Ю. В., Ляхович Л. М. Комп'ютерна програма «Автентифікація користувача на основі клавіатурного почерку в режимі реального часу». Свідоцтво про реєстрацію авторського права на твір № 98144. Дата реєстрації 16.06.2020 р. Заявка № 99489 від 15.06.2020 р.
8. Азарова А. О., Азарова Л. Є., Міронова Ю. В., Бойчук Ю. В., Пазюк О. С. Комп'ютерна програма «Захист потокового відео засобів масової інформації з використанням підпису векторів руху». Свідоцтво про реєстрацію авторського права на твір № 98401. Дата реєстрації 06.07.2020 р. Заявка №99598 від 18.06.2020 р.
9. Азарова А. О., Азарова Л. Є., Міронова Ю. В., Пазюк О. С., Бойчук Ю. В. Комп'ютерна програма «Автентифікація аудіо-сигналів у судовій системі на основі крихких водяних знаків». Свідоцтво про реєстрацію авторського права на твір № 99597. Дата реєстрації 18.06.2020 р. Заявка №99597 від 18.06.2020 р.
10. Азарова А. О., Азарова Л. Є., Білий Р. О., Міронова Ю. В. Комп'ютерна програма «Захищений засобами двофакторної авторизації месенджер для організації комінікаційних процесів на підприємстві». Свідоцтво про реєстрацію авторського права на твір №97856. Дата реєстрації 05.06.2020 р. Заявка № 99244 від 02.06.2020 р.
11. Свідоцтво № 90163 про реєстрацію авторського права на твір "Комп'ютерна програма «Модуль захисту програмного забезпечення від несанкціонованого копіювання у процесах публічного управління»" / Азарова А. О., Азарова Л. Є., Ткачук Л. М., Шиян А. А., Нікіфорова Л. О., Кудлик А. В. Дата реєстрації 25.06.2019 р.
12. Свідоцтво про реєстрацію авторського права на твір №79708. Комп'ютерна програма „Захист інформації від несанкціонованого копіювання шляхом прив'язки до унікальних параметрів вінчестера і використання ключа активації" / Азарова А. О., Азарова Л. Є., Каплун І. С., Щербатюк А. В. Заявка від 05.06.2018 р. №80958. Дата реєстрації 11.06.2018 р.
13. Свідоцтво про реєстрацію авторського права на твір №79708. Комп'ютерна програма „Програмний модуль ідентифікації користувача за відбитками пальців через смартфон з подальшою авторизацією" / Азарова А. О., Азарова Л. Є., Мисько Ю. О., Колган В. А. Заявка від 05.06.2018 р. №80951. Дата реєстрації 11.06.2018 р.
14. Свідоцтво про реєстрацію авторського права на твір №80464. Комп'ютерна програма „Мобільний додаток для захищеного передавання конфіденційних даних у смартфонах" / Азарова А. О., Азарова Л. Є., Бадя Ю. В. Заявка від 12.06.2018 р. №81238. Дата реєстрації 24.07.2018 р.

Азарова Анжеліка Олексіївна, кандидат технічних наук, професор, заступник декана Факультету менеджменту та інформаційної безпеки з наукової роботи та міжнародного співробітництва.

Блонський Владислав Олександрович, Вінницький національний технічний університет**,** м. Вінниця, факультет менеджменту та інформаційної безпеки, УБ-19м, vlados,blonskiy@gmail.com.

Гудзь Віталій Олександрович, Вінницький національний технічний університет**,** м. Вінниця, факультет менеджменту та інформаційної безпеки, УБ-19м, vitalik1211@ukr.net.

Anzhelika Azarova, PhD in technique, Professor, Deputy dean of the Faculty of management and information security by scientific work and international cooperation Vinnytsia National Technical University, Vinnytsia.

Vladyslav Blonskyi, Vinnytsia National Technical University, Vinnytsia, Department of Management and Security of Information Systems, vlados.blonskiy@gmail.com.

Vitalii Hudz, Vinnytsia National Technical University, Vinnytsia, Department of Management and Security of Information Systems, vitalik1211@ukr.net.