УДК 621.397

О. М. РОЇК, Ю. В. МІРОНОВА, О. П. ВОЛКОТРУБ

Вінницький національний тенічний університет, м. Вінниця

ЗАХИСТ ІНФОРМАЦІЇ ВІД ВИТОКУ АКУСТИЧНИМИ КАНАЛАМИ

Анотація. Дана стаття присвячена розробленню мікроконтролерного пристрою захисту інформації. Пропонується підхід до створення додаткової перешкоди всередині приміщень за допомогою генератора білого шуму. Як наслідок, підвищення відношення акустична перешкода/мовний сигнал дозволяє маскувати голос людини в приміщенні і є ефективним в захисті інформації від витоку акустичним каналом.

Ключові слова: генератор шуму, підсилювач потужності, акустичний випромінювач.

Аннотация. Данная статья посвящена разработке микроконтроллерного устройства защиты информации. Предлагается подход к созданию дополнительной преграды внутри помещений с помощью генератора белого шума. Как следствие, повышение отношения акустическая помеха / речевой сигнал позволяет маскировать голос человека в помещении и является эффективным в защите информации от утечки по акустическому каналу.

Ключевые слова: генератор шума, усилитель мощности, акустический излучатель.

The abstract. This article focuses on the development of microcontroller device information security. An approach to the creation of additional barriers indoors using a white noise generator. As a consequence, increase the ratio of acoustic interference / speech signal can mask a man's voice in the room and is effective in protecting information from leaking via the acoustic channel.

Key words: noise generator, power amplifier, the acoustic source.

Вступ

Захист мовної інформації є одним із найважливіших у загальному комплексі заходів технічного захисту інформації (ТЗІ). Несанкціоноване ознайомлення із мовною інформацією з метою її подальшого використання є можливим шляхом перехоплення її зловмисниками. Для цього зловмисник може використовувати широкий арсенал портативних засобів акустичної мовної розвідки, які дають змогу перехоплювати мовну інформацію акустичним, віброакустичним, електроакустичним та оптикоакустичним каналами [1].

Для захисту мовної інформації використовують різні сучасні засоби захисту акустичних каналів витоку інформації, які дозволені державною службою спеціального зв’язку та захисту інформації України, а саме [2]:

Генератор шуму акустичний "Топаз ГША-4".

Призначення приладу - генерація шумових сигналів при використанні у складі технічних засобів активного захисту мовної інформації від витоку акустичним і віброакустичним каналами. Комплект складається з генератора віброакустичного захисту "Топаз ГША-4"(1), вібровипромінювачі «Топаз ВВ-1» , колонка акустична , виносні акустичні електронні реле.

Генератор " Топаз ГША -4 " - це цифровий двоканальний генератор, який має смуговий фільтр на діапазон робочих частот і в кожному каналі еквалайзер нижніх і верхніх частот.

Генератор комплектується віброакустичними випромінювачами «Топаз ВИ-1», а також до нього можуть бути підключені інші випромінювачі, що мають індуктивний або ємнісний характер навантаження з робочою напругою 2 - 8 В. За узгодженням із замовником надаються всі види кріплень віброакустичних випромінювачів: на бетон, метал, металопластик, пластик, дерево, труби.

Генератор шумових сигналів "МАРС-ТЗО-4-2".

Призначення приладу - генерація шумових сигналів при використанні у складі технічних засобів активного захисту мовної інформації від витоку акустичним і віброакустичним каналами. Відповідає вимогам ТУ, зазначеним у сертифікаті відповідності № UA1.105.0095414-09. Виробник - АТВТ "МАРС", м. Київ.

У виробі застосований цифровий метод формування шумового сигналу псевдовипадковою послідовністю. Генератор псевдовипадкової послідовності виконаний на мікроконтролері PIC12C508. На контролері реалізований 33- розрядний регістр зі зворотним зв’язком, що забезпечує період повторення генерованих послідовностей не менше 24 ч. Цифрова псевдовипадкова послідовність надходить на ФНЧ з частотою зрізу 6 кГц.

Після корегування АЧХ шумовий сигнал надходить на підсилювач потужності і вихідний роз'єм.

Виріб має два незалежних канали. У кожному каналі забезпечується регулювання вихідного рівня і корегування АЧХ в області нижніх і верхніх частот. У виробі забезпечується індикація вихідного рівня по кожному каналу та індикація контролю зашумлення при підключенні датчика - акселерометр МВИР.46728.002 -01 [4].

Система акустичного і віброакустичного зашумлення на базі генератора «DNG-2300».

Система «DNG-2300» призначена для захисту конфіденційної інформації від витоку через закладні пристрої, які неможливо визначити традиційними пошуковими приладами; захисту від пристроїв - провідних мікрофонів, контактних мікрофонів, передавачів, що використовують для передачі інформації

мережу 220В і так називаємих віконних систем, принцип дії яких заснований на відображенні лазерних / інфрачервоних / мікрохвильових променів.

DNG-2300 містить 3 незалежних цифрових канали генератора «білого» шуму. «Білий» тому, що містить всі частотні гармоніки, присутні у спектрі людського голосу. Наявність всіх складових гармонік людської мови дозволяє ефективно боротися з різноманітними методами очищення мовної інформації.

DNG-2300 працює в діапазоні 250-5000 Гц, що є оптимальним для придушення найбільш поширених типів підслуховуючих пристроїв.

Система складається з наступних елементів: генератор шуму DNG-2300 , спеціальний мікрофон DNG-MIC для каналу зворотнього зв’язку , вібровипромінювач TRN-2000 , акустичний випромінювач OMS2000 [5].

Вібровипромінювач TRN - 2000 призначений для захисту стін, вікон, стелі, підлоги і труб. Один вібровипромінювач захищає цегляну стіну 3х3 м, одне скло або одну трубу водопроводу або опалення. Для інших поверхонь кількість випромінювачів може відрізнятися [6].

Акустичний випромінювач OMS2000 призначений для захисту простору підвісних стель, ніш, шаф, вентиляційних коробів. Акустичні випромінювачі ставляться за підвісними стелями, в прилеглих кімнатах-сховищах, вентиляціях та інших порожнинах [7].

Порівняльна характеристика генераторів шуму наведена у таблиці 1.

Таблиця 1 – Порівняльна характеристика генераторів шуму

№ п/п	Найменування технічних характеристик	Топаз ГША-4	МАРС-ТЗО-4-2	DNG-2300
1	Діапазон частот вихідного сигналу, Гц	170 – 5700	180 - 5600	250-6500
2	Макс. вихідна потужність акустичного випромінювача	2*4	2*10	2*8
3	Період повторення ПВП, год	24	16	20
4	Електроживлення, В	220 ± 22	100-240 ± 22	220
5	Габарити основного блоку, мм	180*160*70	225*142*48	175*254*60
6	Вага основного блоку, кг	1,5	1,5	2,2

Ретельно ознайомившись з характеристиками сучасних генераторів, не складно помітити, що діапазон випромінюваних частот у середньому складає 175 – 5900 Гц. Самий широкий діапазон у DNG-2300, однак нижня границя на 70 - 80 Гц вища. В генератора МАРС-ТЗО-4-2 період повторення псевдовипадкової послідовності менший, що відкидає його на гіршу позицію. Однак потужність вихідного сигналу у нього більша ніж в інших та можливість працювати при напрузі живлення від 100 В.

Згідно аналізу, вибраним аналогом розроблюваного мікроконтролерного пристрою захисту інформації є генератор шуму Топаз ГША-4. Але є деякі відмінні риси, які відрізнятимуть аналог від розроблюваного приладу. Першою з них є те, що розроблюваний генератор генеруватиме шум в діапазоні від 20 до 20000 Гц, таким чином, зашумлюючи любий чутний для людини звук, а не лише мовний діапазон. Наступна відмінність - це збільшення вихідної потужності сигналу. Однак, негативною відмінністю є те, що регулювання сигналу буде можливе лише за рахунок зміни керуючої програми мікроконтролера [8].

Актуальність

Витік інформації в загальному плані можна розглядати як неправомірний вихід конфіденційних відомостей за межі організації або кола осіб, котрим ці відомості були довірені.

Акустичний канал витоку інформації реалізується в наступному:

- Підслуховування розмов на відкритій місцевості й у приміщеннях, перебуваючи поруч або використовуючи спрямовані мікрофони (бувають параболічні, трубчасті або плоскі). Спрямованість 2-5 градусів, середня дальність дії найбільш поширених - трубчастих становить близько 100 метрів. При хороших кліматичних умовах на відкритій місцевості параболічний спрямований мікрофон може працювати на відстань до 1 км.

- Негласна запис розмов на диктофон або магнітофон (в т.ч. цифрові диктофони, що активізуються голосом).

- Підслуховування розмов з використанням виносних мікрофонів (дальність дії радіомікрофонів 50-200 метрів без ретрансляторів).

Тому, розробка мікроконтролерного пристрою захисту інформації полягає в можливості легко та просто захистити конфіденційну інформацію під час переговорів від витоку акустичними каналами.

Мета дослідження

Метою даного дослідження є розробка мікроконтролерного пристрою генерації білого шуму для захисту інформації від витоку акустичними каналами, який буде реалізовано на основі математичного методу отримання цифрового білого шуму.

Постановка задач

Для досягнення мети, а саме створення мікроконтролерного пристрою захисту інформації від витоку акустичними каналами, необхідно розв'язати такі задачі:

1) проаналізувати основні вимоги до розроблюваного пристрою:
   - великий період повторення псевдовипадкової послідовності;
   - широкий діапазон частот ;
   - широкий діапазон регулювання рівня вихідного сигналу;
   - достатній рівень гучності;
2) провести вибір мікроконтролера;
3) розробити алгоритм генерування псевдовипадкових чисел;
4) провести аналіз та обрати метод перетворення цифрового сигналу у аналоговий.

Розв'язання задач

Згідно проведених досліджень, мікроконтролер повинен відповідати усім вимогам, щоб унеможливити несанкціоноване зняття інформації із захищеного приміщення.

Отже, після визначення методу захисту та винесення вимог, можна розробляти мікроконтролерний пристрій захисту інформації від витоку акустичними каналами.

При розробці пристрою виникає необхідність у виборі мікроконтролера, що задовольняє вимогам по продуктивності, надійності, умовам застосування і т.д. Вибір мікроконтролера є одним з найбільш важливих рішень, від яких залежить успіх або провал усього проекту. При виборі мікроконтролера існують численні критерії.

Основна мета – обрати мікроконтролер з мінімальною ціною (щоб знизити загальну вартість системи), але в той же час задовольняє системну специфікацію, тобто вимоги по продуктивності, надійності, умовам застосування і т.д.

Другий крок - пошук мікроконтролерів, які задовольняють всім системним вимогам. Він звичайно включає підбір літератури, технічних описів і технічних комерційних журналів, а також демонстраційні консультації.

Остання стадія вибору складається з кількох етапів, мета яких – звузити список прийнятних мікроконтролерів до одного. Ці етапи включають в себе аналіз ціни, доступності, засобів розробки, підтримки виробника, стабільності та наявності інших виробників [9].

Згідно до вимог роботи, необхідно обрати такий мікроконтролер, який би мав достатню для генерування псевдовипадкових чисел тактову частоту – не менше 8 МГц, мав простий та зручний інтерфейс для програмування та засоби моделювання його роботи у віртуальному середовищі, та невелику вартість.

Проаналізувавши вимоги, було прийняте рішення використати високопродуктивні 8-розрядні RISC-мікроконтролери сімейства AVR. Термін RISC (Reduced Instruction Set Computer – обчислювач з скороченим набором команд) означає, що процесорне ядро оперує з мінімізованим набором машинних команд, і, отже, кількість різних машинних циклів невелика. Це дозволяє в значній мірі скоротити час виконання машинного циклу, і команди відповідно. Таким чином, відношення тривалості машинного циклу до тривалості такту зменшується – від 12 у класичних контролерів сімейства MCS-51 до 1-4 у контролерів сімейства AVR. Таким чином, при однаковому значенні тактової частоти продуктивність зростає в кілька разів.

Оскільки мікроконтролер буде виконувати лише генерацію чисел та їх вивід, було прийняте рішення обрати мікроконтролер Tiny AVR, а саме ATTiny2313. Оскільки даний контролер працює на частоті 8 МГц, його набір периферії цілком задовольняє усі вимоги, легко програмується та дешево коштує.

Характеристики ATTiny2313:

- 2 КБ програмованої в системі Flash пам'яті програми;
- 128 байтна EEPROM пам'ять даних;
- 128 байтнее SRAM (статичне ОЗУ);
- 18 ліній введення - виведення загального застосування;
- 32 робочих регістра загального призначення;
- однопровідний інтерфейс для вбудованого відладчика;
- два гнучких таймера / лічильника зі схемами порівняння;
- внутрішні і зовнішні джерела переривання;

- послідовний програмований USART;
- універсальний послідовний інтерфейс з детектором стартової умови;
- програмуємий сторожовий таймер з вбудованим генератором;
- три програмно ініціалізуємих режими пониженого споживання.

Білим шумом можна вважати будь-який шум, спектральна щільність якого однакова (або майже однакова) у певному діапазоні частот. Відомі два основні методи отримання цифрового білого шуму: фізичний – генерування випадкових двійкових чисел за допомогою спеціальних пристроїв – генераторів випадкових чисел; математичний – формування псевдовипадкових числових послідовностей спеціальними програмами або з використанням генераторів псевдовипадкових чисел [10].

Тому, важливо вибрати вірний алгоритм, який забезпечував би великий період повторення та був простий для швидкого його виконання на мікроконтролері. Оскільки, сьогодні найдоступнішими і найефективнішими є конгруентні генератори псевдовипадкових чисел. Для цього класу генераторів зроблені математично строгі висновки, якими властивостями володіють вихідні сигнали цих генераторів з погляду періодичності та випадковості. Тому, було прийнято рішення використати лінійний конгруентний алгоритм.

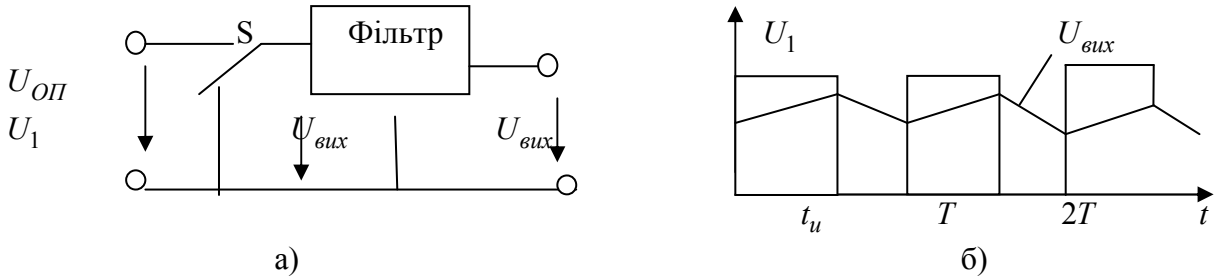
Даний алгоритм був вперше запропонований Д. Х. Лемером в 1948 р. Він генерує послідовності псевдовипадкових чисел X_n, які описують формулою :

$$X_{n+1} = \left(AX_n + C \right) mod\, M \,.$$

де, A і C – константи, X_n – вихідна величина, вибрана в якості числа, що породжує. Очевидно, що ці три величини й утворюють ключ.

Такий генератор генерує псевдовипадкові числа з визначеним періодом повторення, який залежить від вибраних значень А і C. Як показано Д. Кнутом, лінійний конгруентний генератор псевдовипадкових чисел має максимальну довжину періоду повторення тоді і тільки тоді , коли A – непарне, і C mod 4=1.

Для перетворення цифрового сигналу у аналоговий використовуються цифро-аналогові перетворювачі. Дуже часто цифро-аналоговий перетворювач входить у склад мікропроцесорних систем. В такому випадку, цифро-аналогове перетворення може бути дуже просто здійснене за допомогою широтно-імпульсної модуляції (ШІМ), що й було обрано для даного пристрою.



а) б)

Рисунок 1 - а) схема послідовного ЦАП; б) діаграма напруг

Вихід ШІМ-модулятора керує роботою ключа S (в нашому випадку дану функцію буде виконувати мікроконтролер). В залежності від коду формується імпульс ШІМ, тривалість якого прямо пропорційна значенню цифрового коду.

В якості фільтра для розроблюваного пристрою було прийнято рішення використати фільтр Чебишева другого порядку, налаштованого на частоту зрізу 20000 Гц.

Фільтр Чебишева – один з типових лінійних аналогових або цифрових фільтрів, відмінною особливістю якого є більш крутий спад амплітудно-частотної характеристики (АЧХ) та суттєві пульсації АЧХ на частотах смуг пропускання (фільтр Чебишева I роду) і придушення (фільтр Чебишева II роду), ніж у фільтрів інших типів . Фільтр отримав назву на честь відомого російського математика XIX століття Пафнутія Львовича Чебишева, так як характеристики цього фільтра ґрунтуються на многочленах Чебишева [11].

Амплітудно-частотна характеристика такого фільтра n-го порядку задається наступним виразом:

$$G_n(w)=\frac{1}{\sqrt{1+\varepsilon^2 T_n^2(\frac{w}{w_0})}},$$

де, ε - показник пульсацій, w_0 – частота зрізу, T_n – многочлен Чебишева n-го порядку.

У смузі пропускання такого фільтра видно пульсації, амплітуда яких визначається показником пульсації ε. На частоті зрізу w_0 - коефіцієнт підсилення G має значення:

$$G=\frac{1}{\sqrt{1+\varepsilon^2}}$$

Схема електрична принципова фільтра та АЧХ зображені на рис. 2 та 3.

Сигнал, який ми отримаємо після цифро-аналогового перетворення, буде дуже слабким для виведення на акустичні випромінювачі, тому його необхідно підсилити.

При розробці було вирішено використати підсилювач потужності TDA1558Q від компанії Phillips. Оскільки – це високоякісний підсилювач потужності звукової частоти, який має можливість включення на 4 канали та на 2 (мостове з'єднання). Відповідно максимальна вихідна потужність відповідає: 4 канали по 11 Вт або два канали по 22 Вт (мостове з'єднання).

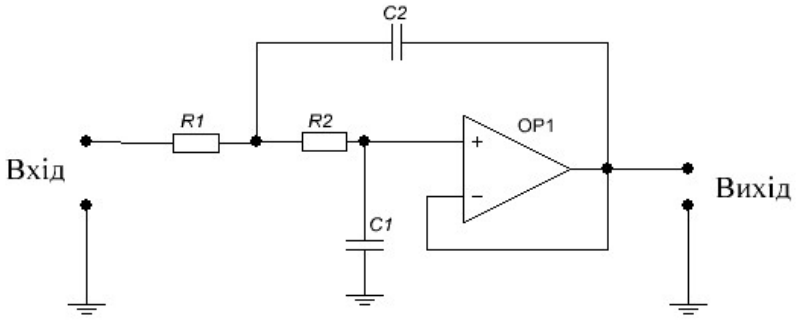


Рисунок 2 – Схема електрична принципова фільтра Чебишева другого порядку

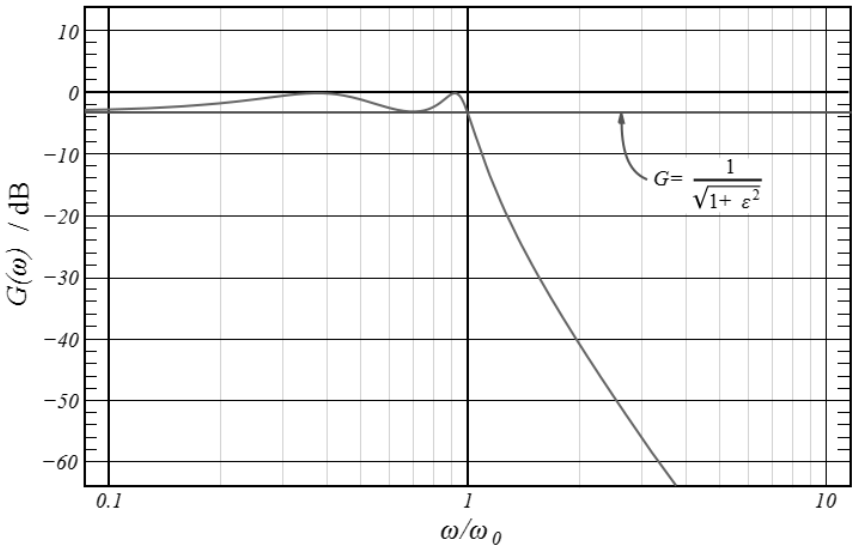


Рисунок 3 – АЧХ фільтра Чебишева

Типова схема включення TDA1558 (мостове з'єднання, 2 канали по 22 Вт) зображено на рис.4.

Розглянувши та продумавши всі ключові елементи, було складено загальну структурну схему пристрою (рис. 5)

В процесі своєї роботи, мікроконтролер генерує псевдовипадкову послідовність чисел, яка передається на фільтр Чебишева другого порядку, в результаті відбувається широко імпульсна модуляція та обрізання частот вище 20000 Гц, тобто перетворення цифрового сигналу в аналоговий та фільтрування. Після чого, вже аналоговий сигнал потрапляє на підсилювач потужності та на акустичний випромінювач.

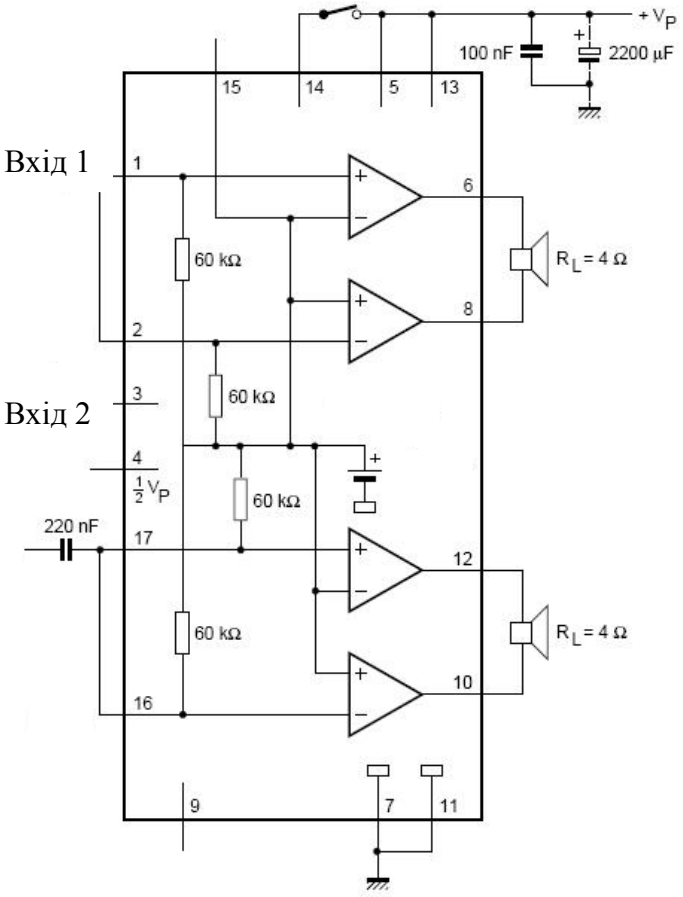


Рисунок 4 – Типова схема включення TDA1558

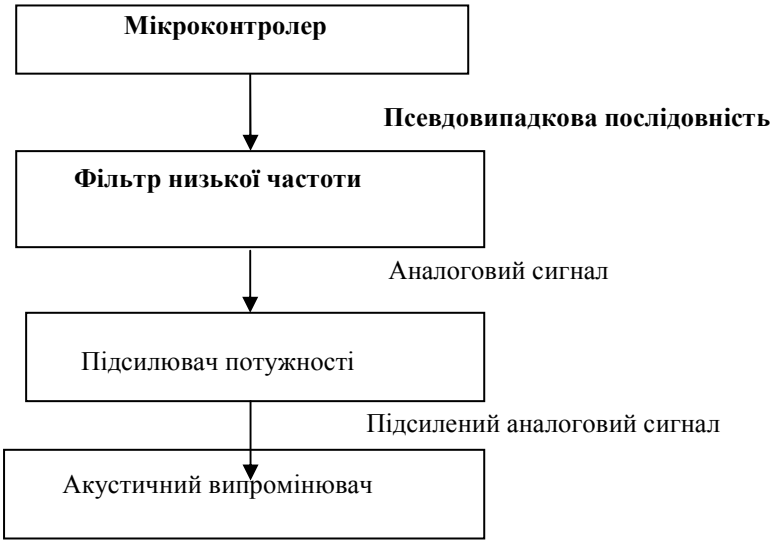


Рисунок 5 – Структурна схема пристрою

Висновки

Проаналізувавши існуючі методи захисту акустичних каналів витоку інформації, можна зробити висновки, що абсолютного захисту не існує. Але одним з найефективніших методів є **акустичне зашумлення приміщення, оскільки воно забезпечує ефективний захист інформації в ньому.** Саме тому, було вирішено розробити пристрій захисту інформації від витоку по акустичних каналах, який реалізує цей метод. А також розроблено алгоритм роботи мікроконтролера, розглянуто та визначено усі ключові елементи пристрою, а саме обрано оптимальний мікроконтролер, цифро-аналоговий перетворювач, фільтр та підсилювач потужності, складено структурну схему пристрою. Отже, все це є основою для створення мікроконтролерного пристрою для захисту інформації від витоку акустичними каналами.

Список літератури

1. Петраков А. В. Основы практической защиты информации / А.В. Петраков – М.: Радио и связь, 2001. – 368 с.

2. Диева С. А. Организация и современные методы защиты информации / С. А. Диева А. Г. Шаваева – М. : Коцерн "Банковский Деловой Центр", 2005. – 472 с.

3. Домнин Ф. А. Микропроцессоры и микропроцессорные системы. Кн.2: Программирование, разработка устройств и систем. Учебное пособие / Ф. А. Домнин И. С. Зыков, А. Н. Рысованый, В. В. Скороделов, В.А. Кравец – Харків : ХВУ, 2000. – 350 с.

4. Зиков І. С. Цифрові пристрої та мікропроцесори. Організація та функціонування : навчальний посібник / І. С. Зиков, О. М. Рисованний, В. В. Скородєлов, С. О. Соколов – Харків : ХВУ, 2002. – 328 с.

5. Главчев М. І. Цифрові пристрої та мікропроцесори. Організація та програмування : навчальний посібник. М. І. Главчев, А. М. Клименко, О. М. Рисованний, А. М. Філоненко – Харків: ХВУ, 2001. – 327с.

6. Домнин Ф. А. Микропроцессоры и микропроцессорные системы. Учебное пособие / Ф. А. Домнин, И. С. Зыков, А. Н. Рысованый, В. В. Скороделов – Харьков: ХГПУ – ХВУ, 2001. – 565 с.

7. Гребнев В. В. Микроконтроллеры симейства AVR фирмы Atmel / В. В. Гребнев. – М. : ИП Радиософт, 2002. – 176 с.

8. Кадино Э. Электронные системы охраны: Пер. с фр. / Э. Кадино. – М.: ДМК Пресс, 2001. – 256 с

9. Белов А. В. Конструирование устройств на микроконтроллерах / А. В. Белов. – СПб. : «Наука и Техника», 2005. – 256 с.

10. Хорошко В.А. Методи й засоби захисту інформації / В.А. Хорошко, А.А. Чекатков. – К. : ЮНІОР, 2003. – 501 с

11. Конахович Г.Ф. Захист інформації від витоку по технічних каналах / Г.Ф. Конахович, Є.Л. Назаренко, В.М. Свириденко // Наукоємні технології № 2. – 2009. – С. 90 – 93. [Електронний ресурс] – Режим доступу до статті: http://www.nbuv.gov.ua/portal/natural/Nt/2009_2/20.pdf

Стаття надійшла:03.02.2015.

Відомості про авторів

Роїк Олександр Митрофанович – д. т. н., професор, завідувач кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Хмельницьке шосе, 95, м. Вінниця, 21021 : тел. 598294.

Міронова Юлія Володимирівна – к. е. н., старший викладач кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Хмельницьке шосе, 95, м. Вінниця, 21021 : тел. 598294.

Волкотруб Оксана Петрівна – студентка четвертого курсу ІнМ, ВНТУ.