ISSN 2219-9365
DOI: 10.31891/2219-9365

Міжнародний науково-технічний журнал

ВИМІРЮВАЛЬНА ТА ОБЧИСЛЮВАЛЬНА ТЕХНІКА В ТЕХНОЛОГІЧНИХ ПРОЦЕСАХ

2021, № 2

International scientific-technical journal

MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES

2021, Issue 2

Хмельницький 2021
Khmelnytskyi 2021

МІЖНАРОДНИЙ НАУКОВО-ТЕХНІЧНИЙ ЖУРНАЛ
ВИМІРЮВАЛЬНА ТА ОБЧИСЛЮВАЛЬНА ТЕХНІКА В ТЕХНОЛОГІЧНИХ ПРОЦЕСАХ

Затверджений як фахове видання (перереєстрація), група «Б»
Наказ МОН 28.12.2019 №1643

Засновано в травні 1997 р. ***Виходить 2 рази на рік***

Хмельницький, 2021, № 2 (68)

Засновник і видавець: **Хмельницький національний університет (до 2005 р. — Технологічний університет Поділля, м. Хмельницький)**

Наукова бібліотека України ім. В.І. Вернадського http://nbuv.gov.ua/j-tit/votte

Журнал включено до наукометричних баз:

Index Copernicus http://jml2012.indexcopernicus.com/,p24781565,3.html h-індекс 54,02
Google Schoolar http://scholar.google.com.ua/citations?user=nwN_nusAAAAJ&hl=uk - індекс 10
CrossRef http://doi.org/10.31891/2219-9365

Національна бібліотека України ім. В.І. Вернадського http://nbuv.gov.ua/j-tit/votte

Рекомендовано до друку рішенням Вченої ради Хмельницького національного університету, протокол № 10 від 02.12.2021

Адреса редакції: **Україна, 29016, м. Хмельницький, вул. Інститутська, 11, Хмельницький національний університет редакція журналу "Вимірювальна та обчислювальна техніка в технологічних процесах"**

☎ **067-347-74-57**

e-mail: **mscientificjournal@gmail.com**

web: **http://journals.khnu.km.ua/index.php/MeasComp**

Зареєстровано Міністерством України у справах преси та інформації.
Свідоцтво про державну реєстрацію друкованого засобу масової інформації
Серія КВ № 23279-13119ПР від 24 травня 2018 року (перереєстрація)

ISSN 2219-9365

ЗМІСТ

ISSN 2219-9365

УДК 004.056.53
DOI: 10.31891/2219-9365-2021-68-2-5

КАТАЄВ В. С., СІНЮГІН В. В.,
ГРИЦАК А. В., ПАВЛОВСЬКИЙ П. В.
Вінницький національний технічний університет

МОБІЛЬНИЙ ЗАСІБ БЛОКУВАННЯ ВИТОКУ ІНФОРМАЦІЇ АКУСТИЧНИМИ КАНАЛАМИ

У статті запропоновано пристрій для забезпечення захисту акустичної (мовної) інформації від несанкціонованого перехоплення на основі ефекту маскування звуку. Пристрій дозволяє блокувати витік мовної інформації шляхом створення шумової завади. Розроблений пристрій складається блоку телефонії та блоку відтворення шумових сигналів. Телефонія реалізується за допомогою мікрофонних підсилювачів до яких підключається гарнітури для спілкування двох абонентів та вихідного підсилювача виходи якого підключаються до головних телефонів абонентів. Блок відтворення складається з двоканального підсилювача потужності зі змінним коефіцієнтом підсилення та можливістю регулювання гучності шумової завади, вихід підсилювача підключається до вбудованого динаміка. Особливістю пристрою є те, що у якості джерела шумових сигналів являється не вбудований шумогенератор, а зовнішній мультимедійний пристрій, через який відтворюється попередньо записаний аудіофайл, який містить у собі шум. Такий підхід дозволяє забезпечити гнучкість вихідних аудіозавад, включаючи різні види шумів та фальшиві розмови. Можливість модульної побудови пристрою дозволяє забезпечити, окрім очевидного спрощення та зниження вартості виготовлення, також і відносну універсальність, а переваги зовнішнього джерела сигналів - широкий спектр способів застосування на реальних об'єктах інформаційної діяльності. Розроблений пристрій було промодельовано у програмному середовищі для автоматизованого проектування, в результаті чого підтверджено його функціональність і здатність виконувати заявлені задачі та в результаті складено дослідний зразок, який продемонстрував роботоспроможність у реальних умовах використання. Реалізація елементів даного пристрою за допомогою засобів електронно-обчислювальної техніки, зокрема мультимедійних пристроїв та загальнодоступних компонентів робить його доступним, а також ефективним засобом для вирішення завдань технічного захисту інформації. Окрім цього пристрій максимально простий у налаштуванні і використанні для користувачів, що дає змогу використовувати його не тільки для захисту інформації, а й в освітньому та науковому процесах.

Ключові слова: технічний захист інформації, генератор шуму, активні засоби захисту, акустична інформація.

V. KATAEV, V. SINIUHIN,
A. HRYTSAK, P. PAVLOVSKIY
Vinnytsia National Technical University

RECOVERY OF THE INFORMATION SECURITY INCIDENT RESPONSE TEAM IN THE CONTEXT OF INCREASING CYBER ATTACKS

The article develops a device for protecting acoustic (speech) information from unauthorized access is proposed, the device is based on the effect of sound masking. The device allows to block the leakage of speech information by creating noise. The developed device consists of a telephony and a noise player blocks. Telephony is realized by means of a set of microphone amplifiers for communication of two subscribers and the output amplifier which outputs are connected to the head telephones of subscribers. The playback block consists of a two-channel power amplifier with a variable gain and has the ability to adjust the volume of noise, the output of the amplifier is connected to the built-in speaker. A feature of the device is that the source of noise signals is an external multimedia device, which plays a pre-recorded audio file that contains noise, rather than the built-in noise generator. This approach allows for the flexibility of output audio interference, including various types of noise and fake conversations. The possibility of modular construction of the device allows to provide, in addition to the obvious simplification and reduction of manufacturing costs, also relative versatility, and the advantages of an external signal source - a wide range of applications on real objects of information activities. The developed device was modeled in a CAD software, which confirmed its functionality and ability to perform the stated tasks, and as a result, a prototype was developed, which demonstrated performance in real conditions of use. The implementation of the elements of this device with the help of computer technology, in particular multimedia devices and available components makes it an affordable and effective means of solving problems of technical protection of information. In addition, the device is easy to set up and comprehensible for users, which allows you to use it not only to protect information, but also in educational and scientific processes.

Keywords: technical protection of information, information protection systems, noise generator, active protection means, acoustic information.

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями

Загроза витоку інформації через акустичні канали є загальновідомою, суть її полягає у тому, що акустична (мовна) інформація, яка озвучується у приміщенні, поширюється у вигляді акустичних хвиль і може поширюватись за межі самого приміщення, через недостатні звукоізоляційні властивості елементів та конструкцій приміщення, в результаті чого дані коливання можуть перехоплюватись засобами технічної розвідки (ЗТР). Також, велику частину загроз становлять закладні пристрої (ЗП) або апаратні закладки. Вони являють собою мініатюрні передавачі або записуючі пристрої, що встановляються безпосередньо у

приміщенні де циркулює інформація з обмеженим доступом, а сигнали від них модулюються інформаційними сигналами. Проблема полягає у тому, що ЗП для знімання інформації можуть використовувати більшість існуючих каналів. Однак, найчастіше закладки слугують для перехоплення мовної та видової інформації. Важливість проблеми захисту такої інформації характеризується постійним розширенням арсеналу засобів та пристроїв негласного отримування і перехоплення мовних сигналів, технічні характеристики та способи застосування яких неухильно удосконалюються. Також, питання безпеки мовної інформації особливо гостро стає при проведенні різноманітних зустрічей, конференційних нарад і т.д у не підготовлених приміщеннях. У зв`язку з цим особливий інтерес представляють дослідження, що спрямовані на розроблення нових або удосконалення існуючих методів та засобів захисту інформації, які дозволяли б істотно ускладнити процес негласного отримання мовної інформації. Особливо у випадках коли організаційні заходи не в змозі забезпечити достатніх результатів щодо захисту.

Існує велика кількість спеціальних засобів, призначених для несанкціонованого отримання мовної інформації. Це, у першу чергу, акустичні та радіоакустичні закладні пристрої, портативні та стаціонарні диктофони, GPS трекекери, направлені мікрофони, електронні стетоскопи та лазерні мікрофони. Крім цього, функцією звукозапису володіє велика кількість побутових пристроїв, починаючи с персонального комп`ютера та закінчуючи стільниковими телефонами.

Для вирішення проблеми захисту інформації від такого типу загроз застосовують різні методи та засоби, при чому захист часто може відрізнятись в залежності від конкретних умов та можливостей потенційного зловмисника. Так, можна виділити два загальних підходи до організації захисту інформації. У випадку захисту від можливого використання спеціалізованих ЗТР використовують методи та засоби направлені на блокування технічних каналів витоку, а при захисті від ЗП, здебільшого, застосовують пошукові роботи з виявлення та знешкодження, таких підслуховуючи пристроїв.

Аналіз досліджень та публікацій

Методи та засоби захисту від ЗТР, у загальному можна розділити на дві категорії — це активні та пасивні. Основна ідея пасивних засобів захисту — це зниження співвідношення сигнал/шум у можливих місцях перехоплення інформації за рахунок зниження інформативного сигналу. Робиться це за рахунок використання різноманітних огороджувальних конструкцій, які виготовлені зі звуко- або вібропоглинаючих матеріалів. Однак, пасивні методи не завжди можуть забезпечити достатні показники захищеності, а також часто призводять до значних фінансових витрат при закупівлі спеціальних матеріалів та проведенні відповідних будівельних робіт. В таких випадках використовуються засоби активного захисту. Переважно це технічні пристрої, які створюють штучні завади, на фоні яких буде неможливо виявити інформативні сигнали. Для захисту мовної інформації у виділених приміщеннях використовуються генератори «білого шуму», вони генерують електричний сигнал даного типу у мовному частотному діапазоні, і далі цей сигнал за допомогою акустичних колонок перетворюється у акустичний шум або за допомогою віброперетворювачів — у вібраційний. Після чого колонки та віброперетворювачі встановлюються у точках, з яких можливе перехоплення інформації (двері, вікна, батареї опалення тощо) [1]. Проблема активного захисту полягає у тому, що у деяких випадках кількість проблемних точок у приміщені може сягати великої кількості і, при встановлені на кожній із них активного захисту, загальний рівень акустичних завад буде на стільки високий, що це буде заважати розмовам.

Захист інформації від витоку через ЗП базується на локалізації та знешкодженні даних пристроїв. А у випадках коли локалізація неможлива, створюються такі умови при яких нормальна робота цих пристроїв буде ускладнена. Виявлення ЗП може здійснюватись двома способами: організаційним та технічним. Перший – це аналітична робота з визначення можливих місць встановлення ЗП із врахуванням особливостей їх роботи і візуальний огляд приміщення та пошук певних демаскуючих ознак в місцях можливого знаходження даних пристроїв. Другий – це локалізація апаратних закладок з допомогою спеціальної пошукової апаратури. Причому цей спосіб повинен враховувати всі технічні характеристики та особливості роботи ЗП, адже від принципу роботи закладки буде залежати і метод, яким можна буде цю закладку виявити. Наприклад, радіозакладки під час своєї роботи випромінюють електромагнітний сигнал, і відповідно пошуковий пристрій повинен вміти цей сигнал виявити з поміж інших та обробити його і т.д. Тому заходи технічного способу виявлення можуть включати: контроль сигналів у лініях зв’язку та електроживлення; контроль радіовипромінювань у області об’єкту; контроль інфрачервоних випромінювань; використання приладів нелінійної локації, металодетекції, тепловізійних систем та ін. Тобто технічний спосіб вимагає великої бази різних пошукових пристроїв, при чому, в деяких випадках, конкретний пристрій може використовуватись для виявлення ЗП, які мають лише конкретні складові або характеристики [2].

Як можна побачити, наведені методи захисту мають певні недоліки, і хоча більшість із них можна вирішити, наприклад використанням комбінованого захисту, все ж існує проблема, яку вирішити не так просто. Усі заходи, що передбачають дані методи вимагають часу, у випадку монтажних робіт по звукоізоляції - це дні або навіть тижні в залежності від площі та складності приміщення, у випадку монтажу системи активного захисту - це як мінімум один день робіт, без урахування попередніх обстежень та

закупівлі обладнання, а у випадку пошукових робіт – це декілька годин. У ситуації коли конфіденційну розмову або нараду потрібно провести тут і зараз у попередньо не підготовленому приміщенні, всі згадані вище методи та засоби ніяк не допоможуть. В такому випадку єдиним способом унеможливити витік мовної інформації є лише один - це оперативно створити у приміщенні певні умови при яких нормальне функціонування ЗТР або ЗП буду не можливим або значно ускладненим. Аналіз багатьох робіт та досліджень з питань захисту акустичної інформації [3-6] дає право стверджувати, що дієвим способом в даному випадку, є використання звукового маскування з допомогою портативного засобу, який не вимагає попереднього монтажу та розгортання. Принцип роботи подібних пристроїв для забезпечення конфіденційних переговорів полягає в тому, що співрозмовники спілкуються між собою за допомогою блоку телефонії, а в цей час вбудований генератор шуму та підключені до нього випромінювачі створюють у приміщенні акустичний шум на фоні якого маскується сама розмова, при цьому спеціальна гарнітура, яку використовують абоненти зменшує вплив шуму для них самих, тим самим сильно не погіршуючи комфортність розмови.

Проблемою являється те, що такі переговорні пристрої хоч і давно відомі все ж, на відміну від інших видів засобів технічного захисту інформації, не так широко представлені ринку України. Для купівлі у вільному доступі можливо знайти лиже декілька моделей, які при цьому мають високу вартість та певні обмеження по технічних характеристиках, зокрема неможливість вибору типу завади.

Формулювання цілей статті

Аналіз представлених на вітчизняному ринку пристроїв блокування витоку інформації акустичним каналом, показав те, що нині ці пристрої мають високу вартість, що при врахуванні доступності компонентів, які входять до складу цих пристроїв не є виправданим. Слід виділити ще те, що доступні пристрої мають обмежений функціонал і, як правило, в їх арсеналі присутній один тип шумового сигналу [7,8]. Також в ході аналізу було встановлено, що дані пристрої потребують оновлення принципів побудови, що дозволить підвищити їх універсальність, зможе значно їх здешевити та зробити доступнішими для використання в сфері технічного захисту інформації, як для проведення досліджень, так і для прямого застосування. Одним із напрямків вирішення зазначених проблем може бути використання популярних і при цьому не дороговартісних компонентів, а також використання мультимедійних пристроїв в якості бази для виконання деяких апаратних вузлів у віртуальному вигляді [9].

Таким чином, метою статті є розробка портативного модульного переговорного пристрою із використанням віртуального генератора шуму для блокування витоку інформації акустичним каналом, який би використовував сучасну елементну базу та нові принципи побудови таких пристроїв, був зручним у обслуговувані та налаштуванні.

Розробка структурної схеми переговорного пристрою. Головною відмінністю запропонованого рішення є те що у якості джерела шумових сигналів виступає не вбудований шумогенератор, а зовнішній мультимедійний пристрій, через який відтворюється попередньо записаний аудіофайл, який містить у собі шум. Такий підхід має ряд переваг. По перше, в якості мультимедійного пристрою може виступати будь-який пристрій, що має можливість відтворення аудіо сигналів, через роз'єм типу «mini- Jack 3,5мм», а це практично усі сучасні мобільні телефони, mp3 плеєри, комп'ютери і т.д., які завжди є під рукою. По друге, забезпечується гнучкість вихідних аудіо завад, включаючи різні види шумів та фальшиві розмови. Представлений пристрій розроблений для можливості спілкування двох людей, але універсальність структури дозволить легко збільшити кількість абонентів простим додаванням до схеми додаткових підсилювачів. На рис.1 показано узагальнену структурну схему переговорного пристрою.

Пристрій умовно можна поділити на 2 основні частити. Перша – це блок відтворення та підсилення акустичних сигналів. Друга – блок телефонії. Обидва блоки мають спільну схему живлення від інтерфейсу USB, однак включаються окремо. Акустичні сигнали на перший блок подаються через AUX кабель. В загальному з пристроєм розроблено mp3 файл, який містить білий шум, хоча подавати на підсилювач можливо будь-який аудіосигнал. Підсилювач в даному блоці має схему регулювання підсилювання, що дозволяє змінювати гучність шуму. Як зазначалось раніше, однією з цілей розробки є здешевлення пристрою, тому в якості вихідного підсилювача було обрано схему з не великою потужністю, але якої буде достатньо для захисту розмов у невеликих приміщеннях або автомобілях. Для вирішення проблеми захисту у великих приміщення, в даному блоці пристрою було передбачено паралельний аудіо вихід, що дозволяє підключати до нього зовнішні акустичні системи з власними вбудованими підсилювачами, що дозволяє забезпечити будь-яку необхідну вихідну потужність системи в загальному.

Другий блок має дві паралельних схеми телефонії, сигнали на які подаються з підключених до входів мікрофонів, а вихідні сигнали подаються через відповідні виходи на навушники. Доцільним в даному випадку є використання комп'ютерних гарнітур в яких мікрофон та головні навушники об'єднані разом. Підключення відбувається через роз'єми типу «mini Jack 3,5мм». В даному блоці немає окремої схеми регулювання підсилення, тому гучність розмови регулюється з допомогою атенюаторів на самій гарнітурі.

Вхідний роз'єм типу «mini-jack 3.5», дозволяє подавати шумові сигнали з будь-якого

мультимедійного пристрою. Такий варіант надає гнучкість з точки зору можливого шумового сигналу, у більшості існуючих аналогів шум є вбудованим, зокрема часто використовується вбудований генератор «білого шуму», відповідно пристрій може генерувати лише визначений тип шуму. В нашому випадку, ми можемо подавати будь-який сигнал у вигляді MP3 файлу, відповідно можемо генерувати, як білий шум, так і будь-який інший, наприклад фальшиву розмову.

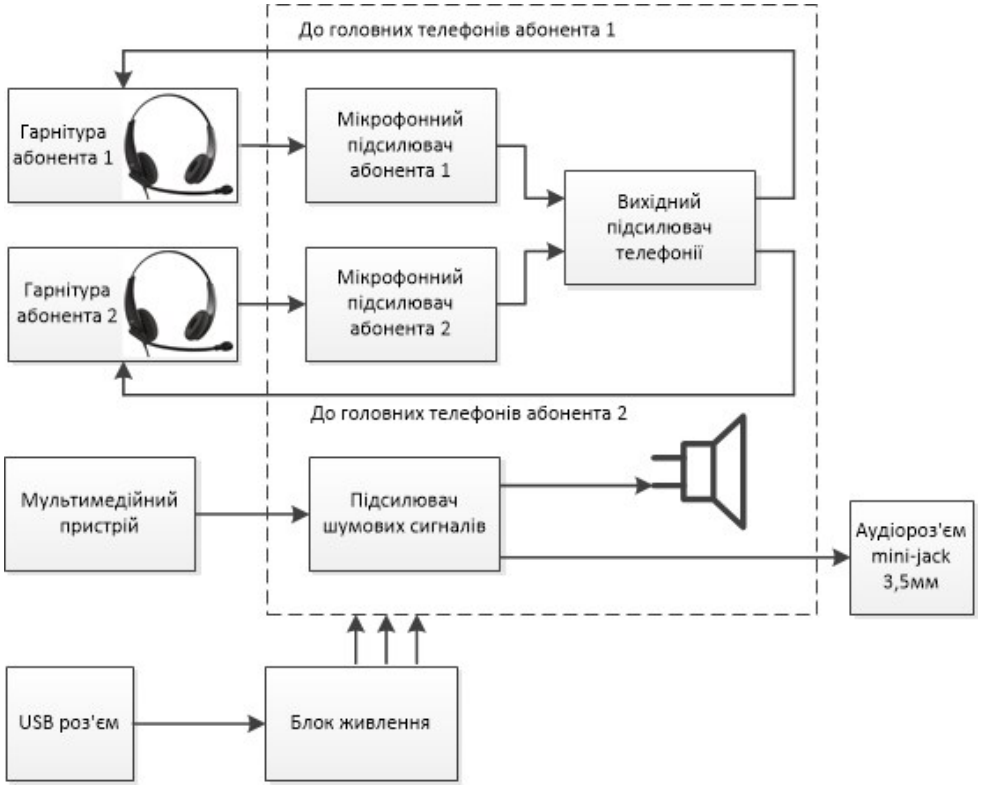

Рис.1. Узагальнена структурна переговорного пристрою

Більше того, на сьогоднішній день можливості ЕОМ та програмного забезпечення пішли сильно вперед і дають змогу будувати складні системи, зокрема і генератори шумів різних типів або навіть реверберaційних завад. Відповідно використання такої системи у комплексі з запропонованим переговорним пристроєм, ще більше розширить його функціональні можливості та дасть змогу не тільки забезпечити необхідний рівень захисту від витоку акустичної інформації, а й проводити дослідження шумових характеристик у навчальному та науковому процесах. Тому, поряд із розробкою структурної схеми, також важливим питанням є розробка віртуального генератора шуму.

Програмна реалізація віртуального генератора шуму. Віртуальний генератор шуму, що розробляється включатиме в собі блоки генерування різних типів шумів. Для програмної розробки і дослідження роботи була обрана програма LabVIEW - це кроссплатформенне графічне середовище розробки додатків. Завдання розробки віртуального генератора полягає у проектуванні такого генератора шуму в якому можна було б обирати, в залежності від ситуації і задач, різні типи шумів, при цьому, структура програми була побудована так, щоб її можна було розширювати додаючи в неї інші види шумових сигналів, модулі відображення параметрів цих сигналів, модулі аналізу параметрів шумових сигналів тощо.

Всі програмні коди для систем і приладів, які розробляються в середовищі LabVIEW пишуться графічно. У LabVIEW розроблювані програмні частини називаються «Virtual Instruments» (Віртуальні Інструменти) або VI. VI - це частини, з яких складається LabVIEW - програма. Будь-яка LabVIEW програма містить як мінімум один VI. Само собою зрозуміло, один VI може бути викликаний з іншого VI. В принципі кожен VI складається з двох частин - блок-діаграма (Block Diagram) і передня панель (Front Panel). Блок-діаграма - це візуальне графічне представлення коду, а передня панель - це інтерфейс. На рис.2 зображено вікно з блок-діаграмою візуального графічного представлення коду розроблюваного пристрою з віртуальним генератором шуму.

В сірій рамці (область циклу while) заключені блоки і взаємозв'язки між ними, що реалізують основний цикл програми. Поза основним циклом, по аналогії з іншими мовами програмування, знаходяться блоки і взаємозв'язки, що відповідають за встановлення початкових параметрів та параметрів, які встановлюються після завершення циклу основної програми віртуального пристрою.

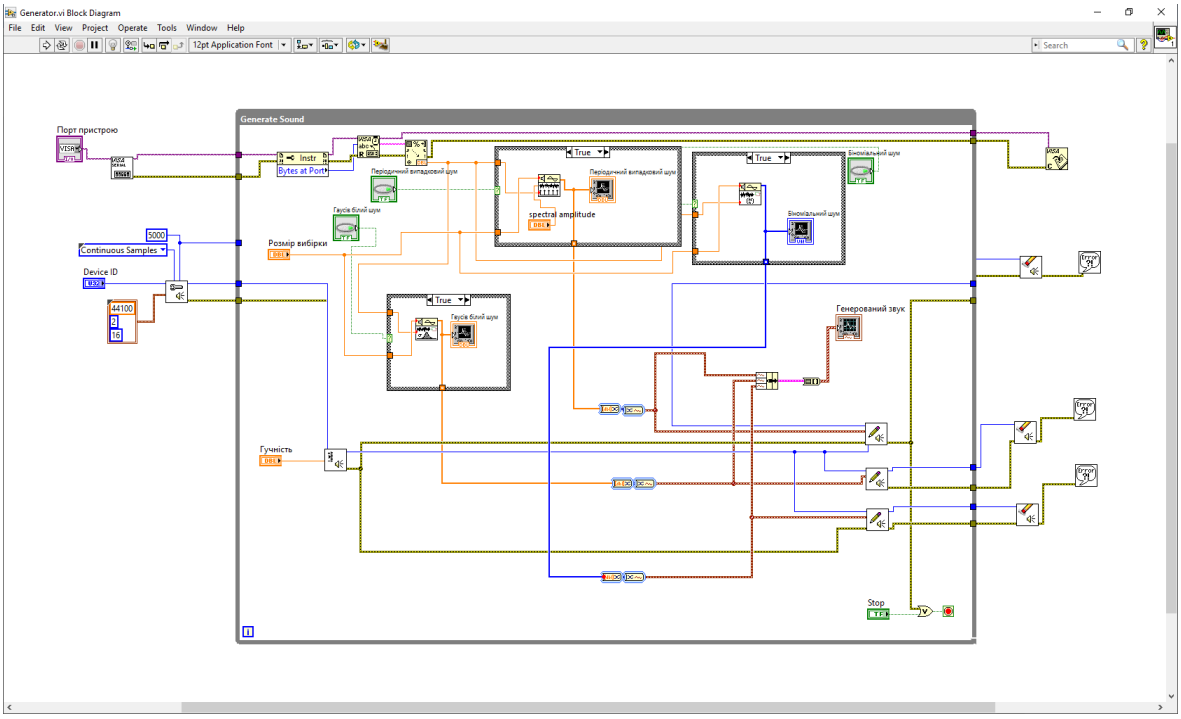

Рис.2. Блок-діаграма візуального графічного представлення коду розроблюваного пристрою

Принцип роботи програмного коду віртуального генератора шуму наступний. Перед початком запуску віртуального генератора ініціалізується послідовний порт, по якому дані з апаратної платформи надходять до віртуального генератора. На мікроконтролерній платі реалізовано програмний код генератора псевдовипадкових чисел. Генеровані платформою числа виступають у ролі початкових значень для обраних вбудованих в LabVIEW блоків генераторів. Перед запуском основного циклу програми потрібно конфігурувати і ініціалізувати виходи ЕОМ, які відповідають за виведення сигналів звуку, так як генерований в основному циклі шум має бути відтворений підключеним переговорним пристроєм. Для реалізації генератора псевдовипадкових чисел було обрано плату Arduino Pro Mini. Для запису програмного коду і суміщення плати з ЕОМ пропонується використати перехідник USB – TTL. Таким чином, плата Arduino Mini разом з перехідником при під'єднані до ЕОМ буде розмірами з стандартний флеш-накопичувач.

Апаратно випадкові числа можна брати через виводи (pin). Якщо пін нікуди не під'єднано, то на нього наводяться зовнішні електромагнітні наведення із оточуючого середовища. Шуми мають природу близьку до випадкової і цим фактором можна скористатися для формування випадкових подій. Виконавши всі необхідні налаштування, під'єднавши до послідовного порту апаратну платформу, робота програми переходить в основний цикл. В основному циклі для приймання генерованих випадкових чисел необхідно правильно зчитувати їх з послідовного порту так, щоб програмне середовище LabVIEW сприймало їх однозначно, відповідно до значень передбачених генератором випадкових чисел. Значення, які надходять з послідовного порту, одночасно передаються на всі типи генераторів шуму в якості базису для генерування шуму по законам, передбаченими тими чи іншими блоками.

В якості генераторів шуму, що представляються на вибір користувачу обрано генератор періодичного випадкового шуму, генератор Гауссового білого шуму та генератор біноміального шуму. Кількість і тип генераторів можна змінювати, LabVIEW має у бібліотеці широкий вибір таких блоків. Кожен з представлених генераторів вмикається в потрібний момент за допомогою клавіш на передній панелі віртуального пристрою. Разом з тим на відповідних графіках відображується осцилограма відповідного шумового сигналу. Підключення окремо кожного з генераторів відбувається за допомогою реалізації в case-структурі. Обирати генератори можна, як і на початку роботи основного циклу, так і під час виконання основного циклу. Таким чином, маємо сформований алгоритм роботи віртуального генератора шуму.

На рис.3 зображено передню панель віртуального генератора шуму. Як видно, на передній панелі розміщено елементи вибору параметрів генератора, елемент вибору порту зовнішніх пристроїв, елементи вибору між генераторами різних типів шумів та їхніми осцилограмами та осцилограму рівня звуку шумового генератора. Використання даного віртуального генератора шуму у тандемі із розробленим вище пристроєм для переговорів, значно розширює можливості останнього.

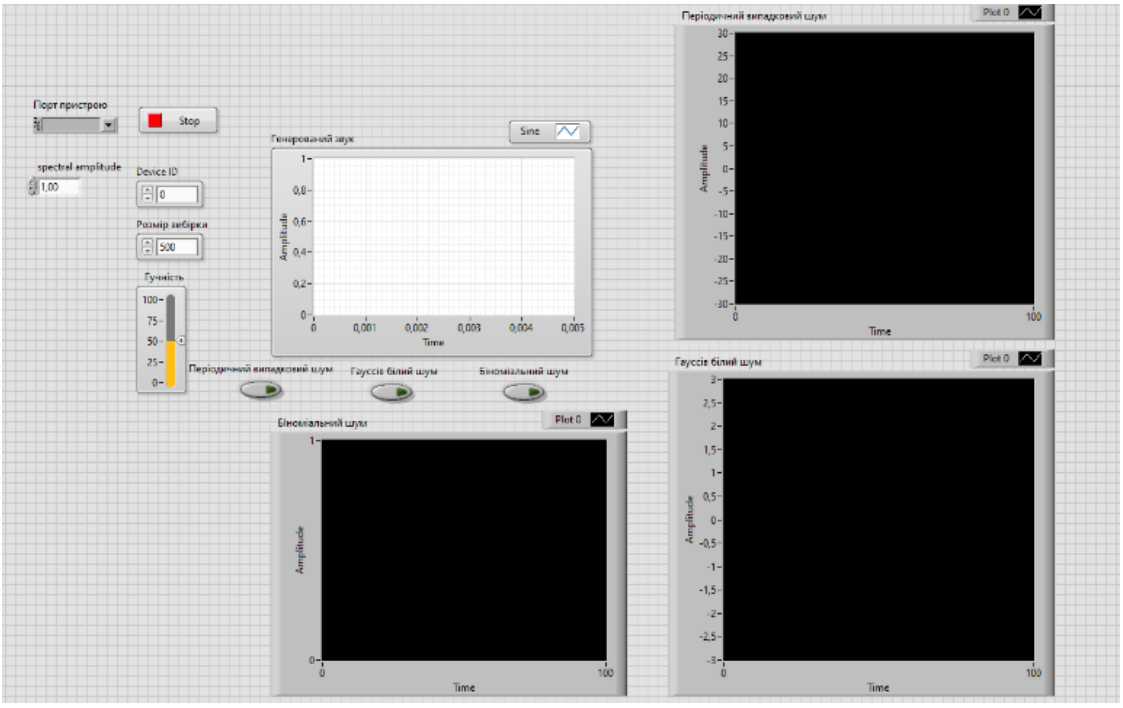

Рис.3. Передня панель віртуального генератора шуму

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі

Запропоновано мобільний засіб блокування витоку інформації акустичними каналами із використанням віртуального генератора шуму, що перешкоджає перехопленню мовної інформації під час ведення переговорів на об'єктах інформаційної діяльності. Представлена структура пристрою має ряд переваг. Компактність – пристрій реалізований за блоковою структурою, що дозволяє компактно розміщувати внутрішні елементи у невеликому корпусі, зокрема розроблений прототип розміщений у корпусі від звичайної акустичної колонки. Універсальність живлення – живлення пристрою реалізується від USB роз'єму, що відкриває широкий спектр джерел живлення: звичайний БЖ від мобільного телефону, power банк, USB перехідник в автомобілі тощо. Регулярність структури – телефонія в пристрої реалізована на базі простих мікрофонних підсилювачів, що дозволяє легко збільшувати кількість абонентів простим додаванням до схеми додаткових підсилювачів. Також, мультимедійний пристрій у якості джерела шумових сигналів забезпечує гнучкість з точки зору шумових завад, зокрема використання розробленого віртуального генератора шумів дозволило об єднати одразу декілька типів шумів.

Література

1. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації [Електронний ресурс] : навчальний посібник / С. О. Іванченко, О. В. Гавриленко, О. А. Липський [та ін.] ; - Київ : НТУУ «КПІ», 2016. - 104 с. Режим доступу: https://ela.kpi.ua/handle/1234_5б789/15155.

2. Остапов С.Е. Технології захисту інформації : навчальний посібник / С.Е. Остапов, С. П. Евсеев, О.Г. Король. -Х.: Вид. ХНЕУ, 2013. -476с.

3. Яремчук Ю.Е. Метод активного захисту інформації від зняття лазерними системами акустичної розвідки / Катаев В.С., Яремчук Ю.Е. // Захист інформації. - Т. 21, №1, 2019. - С. 34-39.

4. Яремчук Ю.Е. Дослідження характеристик різних типів шумів для захисту інформації від витоку лазерним каналом. / Катаев В.С., Яремчук Ю.Е.,Сінюгін В.В. // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. - Випуск 2(32), 2016. - С. 21-27.

5. Проблеми активного захисту інформації від витоку через віброакустичні канали / В.С. Катаев, А.В. Грицак, В.О. Леонтьев, Н.В. Ляховченко // Реєстрація, зберігання і обробка даних. - Т. 18, N23, 2016. - С. 54- 58.

6. Яремчук Ю.Е. Можливості практичного застосування тепловізорів у питаннях захисту інформації / Ю.Е. Яремчук, В.С. Катаев, М.Ю. Гижко, С.М. Скуратов // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. - Випуск 1(31), 2016. - С. 99-105.

7. Пристрій забезпечення конфіденційних переговорів DRUID D-06 [Електронний ресурс]. – Режим доступу : https://one-click.com.ua/uk/ustroystvo-obespecheniya-konfidencialnyh-peregovorov-druid-d-06.html

8. Мобильный генератор шума MNG-300 Rabbler [Електронний ресурс]. – Режим доступу: https://www.forter.com.ua/poiskovaya-tehnika/mng-300-rabbler/

9. Хилобокий С.М. «Розробка мобільного засобу блокування інформації від витоку прямим акустичним каналом для проведення конфіденційних розмов у незахищеному середовищі»: Дипл. робота., фак-т менедж. та інф. безпеки, ВНТУ, Вінниця, 2021.

References

1. Technical channels of information leakage. The order of creation of complexes of technical protection of information: textbook / S. Ivanchenko, O. Gavrilenko, O. Lipsky [etc.]; - Kyiv: NTUU "KPI", 2016. - 104 p. URL: https://ela.kpi.ua/handle/1234_56789/15155.

2. S. Ostapov Technologies of information protection: textbook / S. Ostapov, S. Evseev, O. Korol. -H.: Pub. KhNEU, 2013. -476p.

3. Y. Yaremchuk The method of active protection of information from the laser acoustic intelligence systems / V. Kataiev, Y. Yaremchuk // Information protection. - Vol. 21, №1, 2019. - P. 34-39.

4. Y. Yaremchuk Investigation of the characteristics of different types of noise to protect information from leakage by the laser channel. / V. Kataiev, Y. Yaremchuk, V. Sinyuhin // Legal, regulatory and metrological support of information security system in Ukraine. - Issue 2(32), 2016. - P. 21-27.

5. Problems of active protection of information from leakage through vibroacoustic channels / V. Kataiev , A. Gritsak, V. Leontiev, N. Lyakhovchenko // Реєстрація, зберігання і обробка даних. - Т. 18, N23, 2016. - С. 54- 58.

6. Y. Yaremchuk The practical application of thermal imager for the protection of information / Y. Yaremchuk, V. Kataiev, M. Guzhko, S. Skuratov // Legal, regulatory and metrological support of information security system in Ukraine. - Issue 1 (31), 2016. - P. 99-105.

7. Device for ensuring confidential conversations DRUID D-06 URL: https://one-click.com.ua/uk/ustroystvo-obespecheniya-konfidencialnyh-peregovorov-druid-d-06.html

8. Mobile noise generator MNG-300 Rabbler URL: https://www.forter.com.ua/poiskovaya-tehnika/mng-300-rabbler/

9. S. Hilobokiy "Development of a mobile means of blocking information from leakage through a direct acoustic channel for confidential conversations in an unprotected environment": Diploma. work., Faculty of Management. and inf. of Security, VNTU, Vinnytsia, 2021.