УДК 004.942:534.231:621.391.825
DOI: 10.15587/2312-8372.2019.85133

РОЗРОБКА МАТЕМАТИЧНОЇ МОДЕЛІ ГЕНЕРАТОРА МОВОПОДІБНОГО СИГНАЛУ ЗАВАДИ СКРЕМБЛЕРНОГО ТИПУ ДЛЯ СИСТЕМ ПРОТИДІЇ ВИТОКУ МОВНОЇ ІНФОРМАЦІЇ АКУСТИЧНИМИ ТА ВІБРАЦІЙНИМИ КАНАЛАМИ

Блінцов В. С., Нужний С. М., Касьянов Ю. І., Корицький В. І.

РАЗРАБОТКА МАТЕМАТИЧЕСКОЙ МОДЕЛИ ГЕНЕРАТОРА РЕЧЕПОДОБНОГО СИГНАЛА ПОМЕХИ СКРЕМБЛЕРНОГО ТИПА ДЛЯ СИСТЕМ ПРОТИВОДЕЙСТВИЯ УТЕЧКИ РЕЧЕВОЙ ИНФОРМАЦИИ АКУСТИЧЕСКИМИ И ВИБРАЦИОННЫМИ КАНАЛАМИ

Блинцов В. С., Нужный С. Н., Касьянов Ю. И., Корицкий В. И.

DEVELOPMENT OF A MATHEMATICAL MODEL OF SCRAMBLER-TYPE SPEECH-LIKE INTERFERENCE GENERATOR FOR SYSTEM OF PREVENT SPEECH INFORMATION FROM LEAKING VIA ACOUSTIC AND VIBRATION CHANNELS

Blintsov V., Nuzhniy S., Kasianov Yu., Korytskyi V.

Захист мовної інформації відноситься до основних задач інформаційної безпеки і є ознакою відповідального відношення організації (фірми) як до своїх інформаційних ресурсів, так і поваги до партнерів. Об'єктом дослідження є процеси захисту мовної інформації від витоку акустичними та вібраційними технічними каналами на об'єктах інформаційної діяльності. Виключною рисою таких об'єктів є циркуляція, обробка та обговорення питань, що містять інформацію обмеженого доступу, в тому числі й державну таємницю. Особливістю України є вимога про застосування на таких об'єктах виключно технічних засобів, що пройшли відповідну сертифікацію.

Основою системи постановки активної шумової завади є генератор шуму. При цьому, одним з найбільш проблемних питань є те, що в Україні дозволені до використання тільки генератори шумової завади типу «білий» шум та його клони. Системи мають ряд значних недоліків – низький рівень захищеності перехоплених мовних сигналів від фільтрації шуму (завади), значний рівень шуму в приміщеннях, які підлягають захисту, та інші.

Запропоновано структурну схему генератора завади. А також розроблено та досліджено в середовищі Matlab її математичну модель. В ході дослідження проведено порівняльний аналіз вхідних та синтезованих генератором сигналів, досліджені їх тимчасові та спектральні характеристики. Отримані результати свідчать про високу ефективність запропонованого методу захисту мовної інформації. Це пов'язано з тим, що метод формування мовоподібної завади має ряд

особливостей, які забезпечують значний деструктивний вплив на мовну інформацію, а саме використання моделі комбінованого скремблера з тимчасовими та частотними перетвореннями. Метод враховує використання динамічних ключів, для систем кодування, та підключення сторонніх джерел мовних сигналів, а також закільцьовування (змішування вхідного та вихідного сигналів) на вході блоку скремблювання. Таке рішення унеможливлює ре-інжиніринг.

Отримані результати підтверджені дослідженням експериментального зразка. Проведено порівняння деструктивного впливу типових шумових завад («білий» шум та його клони) і шумової завади, створеної запропонованим методом, за критерієм залишкова словесна розбірливість мови диктора. Дослідження показали, що, за умови забезпечення не більше 10 % рівня залишкової розбірливості, рівень гучності вихідного сигналу генератора шумової завади можна знизити майже на 6 дБА.

Ключові слова: *генератор мовоподібної завади скремблерного типу, захист мовної інформації, інформаційна безпека.*

Защита речевой информации относится к основным задачам информационной безопасности и является признаком ответственного отношения организации (фирмы) как к своим информационным ресурсам, так и уважения к партнерам. Объектом исследования являются процессы защиты речевой информации от утечки акустическими и вибрационными техническими каналами на объектах информационной деятельности. Исключительной чертой таких объектов является циркуляция, обработка и обсуждение вопросов, содержащих информацию ограниченного доступа, в том числе и государственную тайну. Особенностью Украины является требование о применении на таких объектах исключительно технических средств, прошедших соответствующую сертификацию.

Основой системы постановки активной шумовой помехи является генератор шума. При этом, одним из самых проблемных вопросов является то, что в Украине разрешены к использованию только генераторы шумовой помехи типа «белый» шум и его клоны. Системы имеют ряд значительных недостатков – низкий уровень защищенности перехваченных речевых сигналов от фильтрации шума (помехи), значительный уровень шума в помещениях, подлежащих защите, и другие.

Предложена структурная схема генератора помехи. А также разработана и исследована в среде Matlab ее математическая модель. В ходе исследования проведен сравнительный анализ входящих и синтезированных генератором сигналов, исследованы их временные и спектральные характеристики. Полученные результаты свидетельствуют о высокой эффективности предложенного метода защиты речевой информации. Это связано с тем, что метод формирования речеподобной помехи имеет ряд особенностей, которые обеспечивают значительное деструктивное влияние на речевую информацию, а именно использование модели комбинированного скремблера с временными и частотными преобразованиями. Метод учитывает использование динамических ключей, для систем кодирования, и

подключение сторонних источников речевых сигналов, а также закольцовывание (смешивание входного и выходного сигналов) на входе блока скремблирования. Такое решение исключает ре-инжиниринг.

Полученные результаты подтверждены исследованиями экспериментального образца. Проведено сравнение деструктивного влияния типовых шумовых помех («белый» шум и его клоны) и шумовой помехи, созданной по предложенному методу, по критерию остаточной словесной разборчивости речи диктора. Исследования показали, что, при условии обеспечения не более 10 % уровня остаточной разборчивости, уровень громкости выходного сигнала генератора шумовой помехи можно снизить почти на 6 дБА.

Ключевые слова: *генератор речеподобной помехи скремблерного типа, защита речевой информации, информационная безопасность.*

1. Вступ

Захист мовної інформації від витоку акустичними та вібраційними каналами в Україні відбувається в відповідності до законодавчих [1–3] та нормативних документів і включає в себе три групи заходів:

– організаційні;

– організаційно-технічні;

– технічні.

Аналіз вимог [4–6] показує, що найкращі показники захищеності мовної інформації мають комплексні системи захисту інформації (КСЗІ), які побудовані на основі систем постановки активних вібраційних та акустичних завад (СПАВАЗ). Згідно з [7, 8], в Україні пройшли сертифікацію та дозволені для використання на об’єктах інформаційної діяльності (ОІД) окремо та в складі КСЗІ сім типів систем СПАВАЗ:

1) комплекс технічного захисту об'єкта «МАРС-ТЗО» (генератори шумових сигналів «МАРС-ТЗО-4-2» виробництва України);

2) комплекс віброакустичного захисту інформації «СКЕЛЯ-2» виробництва України;

3) комплекс активного захисту інформації «РІАС-АЗ» (прилади «РІАС-2С», «РІАС-2М» виробництва України);

4) комплекс активного захисту інформації «Топаз-4» (генератор шуму акустичний «Топаз ГША-4» виробництва України);

5) комплекс активного захисту інформації «Базальт-4» (пристрій захисту «Базальт-4ГА» виробництва України);

6) система захисту аудіоінформації «Druid» (цифровий генератор шуму «DNG-2300» виробництва Німеччини);

7) прилад віброакустичного захисту інформації «ОЦЗІ-ВА» виробництва України.

А також спеціалізована мобільна споруда – Кабіна переговорна мобільна «КПМ-01» виробництва України.

До головних технічних характеристик таких систем належать кількість вихідних каналів (зазвичай 1 або 2) та вихідна електрична потужність або

допустима кількість типових випромінювачів на канал (від 8 до 24 шт.). В якості генератора шуму в усіх системах використовуються генератори «білого» шуму (або його клони).

Однак, як показує аналіз [9–11], використання «білого» шуму та його клонів має значний недолік – використання сучасних систем цифрової обробки фонограм дозволяє суттєво понизити рівень шумової завади в фонограмі. А в [12–14] наведені методи цифрової обробки цифрових фонограм, в тому числі вейвлет-перетворення та кореляційного аналізу. Відновленню інформаційного складу перехопленого повідомлення суттєво допомагає використання зловмисником мультиточкового «зняття» інформації з конструкційних елементів [15, 16] – це є можливим, так як в СПАВАЗ використовуються підключені до одного каналу декілька випромінювачів. Такий стан дискредитує КСЗІ, однак на даний час в Україні відсутні методи та технології, які б задовольняли сучасним вимогам по захищеності мовної інформації. Обов'язковою вимогою до СПАВАЗ є їх стійкість до сучасних та перспективних методів цифрової обробки фонограм з метою фільтрації та відновлення перехоплених мовних повідомлень.

Таким чином, виникла нагальна потреба в розробці вдосконаленого методу формування сигналу шуму завади для СПАВАЗ. Метод повинен інтегруватись в структуру та принципи роботи існуючих КСЗІ та бути спроможним врахувати сучасні та перспективні методи цифрової обробки фонограм.

Таким чином, актуальним є розробка методу формування акустичної та вібраційної завади, яка створює значний деструктивний вплив на мовний сигнал та є стійкою до фільтрації сучасними методами та засобами цифрової обробки фонограм.

2. Об'єкт дослідження та його технологічний аудит

Об'єктом дослідження є процеси захисту мовної інформації від витоку акустичними та вібраційними технічними каналами на об'єктах інформаційної діяльності. Особливістю таких об'єктів є циркуляція, обробка та обговорення питань, що містять інформацію обмеженого доступу, в тому числі й державну таємницю.

На сьогоднішній день створені методи та технічні засоби, які призначені для забезпечення безпеки мовної інформації в спеціально виділених приміщеннях – кімнатах переговорів, кабінетах відповідальних співробітників, керівників середньої і вищої ланки та інше.

В Україні та світі використовується технології, в яких захист мовної інформації забезпечується пасивними засобами (звукоізоляція, звукопоглинання та інше) та системами постановки активної шумової завади. При цьому, для об'єктів, що обробляють інформацію, яка містить державну таємницю, використання систем активного захисту мовної інформації є обов'язковим. Особливістю України є вимога про застосування на таких об'єктах виключно технічних засобів, що пройшли відповідну сертифікацію.

Основою системи постановки активної шумової завади є генератор шуму. Одним з найбільш проблемних місць є те, що в Україні дозволені до використання тільки генератори шумової завади типу «білий» шум та його клони. *Системи мають ряд значних недоліків* – низький рівень захищеності

перехоплених мовних сигналів від фільтрації шуму (завади), значний рівень шуму в приміщеннях, які підлягають захисту та інші.

На даний час розроблені методи та технології захисту, основані на використанні мовоподібних шумів, створених з мови дикторів та/або маніпуляціями з нею. Найбільшого поширення набули методи «мовний хор» («гомін натовпу») та частотні-тимчасові перетворення (частотна та тимчасова реверберація). Такі методи мають значно вищій рівень деструктивних впливів на сигнал, що підлягає захисту. Однак, *одним з найбільш проблемних місць* є методозалежність (цифрова обробка фонограми перехопленого сигналу дозволяє відновити (фільтрувати) небезпечний сигнал) та мала стійкість до ре-інжинірингу («розбиття» натовпу на окремих дикторів).

3. Мета та задачі дослідження

Метою даного дослідження є удосконалення методу формування сигналу шумової завади для систем постановки активних вібраційних та акустичних завад.

Для досягнення мети були поставлені такі завдання:

1. Розробити узагальнену схему генератора мовоподібного сигналу скремблерного типу.
2. Розробити та дослідити спрощену математичну модель генератора мовоподібного сигналу.
3. Провести процедуру верифікації результатів математичного моделювання спрощеної математичної моделі генератора мовоподібного сигналу.

4. Дослідження існуючих рішень проблеми

Головними перевагами «білого» шуму та його клонів над іншими видами шумів є їх спектральна щільність та простота реалізації. Це зумовило їх широке застосування в усіх системах постановки активних завад. Однак, розробка методів фільтрації та відновлення інформаційних повідомлень призвели, спочатку в радіо-телекомунікаційних системах, а згодом і в інших сферах, пов’язаних з передачею інформаційних повідомлень, до відмови «білого» шуму.

Іншими типами шумів, які на разі розглядаються як заміна для «білого» шуму та його клонів є мовоподібні шуми:

– створені на основі мови диктора, що знаходиться в даний час в контрольованій зоні;

– створені на незалежних від диктора, що знаходиться в даний час в контрольованій зоні, мовних сигналах.

Використання мовоподібних шумів в якості основи для створення систем захисту мовної інформації базується на роботах, які проводились в середині XX століття. Так, в роботі [17] була обґрунтована можливість використання спеціалізованих акустичних сигналів для захисту інформаційних повідомлень в лініях передачі та на межах контрольованої зони.

Використання акустичної завади у вигляді періодичних та неперіодичних меандрів в системах протидії перехопленню інформаційних повідомлень в відкритих телекомунікаційних лініях розглянуто в [18]. В роботі проведено

аналіз впливу таких завад на розбірливість мовного сигналу для різних співвідношень сигнал/завада.

В [19] розглянуто вплив частоти переключання акустичного сигналу та шумової завади. Проводились дослідження комбінованих сигналів з різною інтенсивністю, тимчасовими та спектральними складами. Корисний сигнал та сигнал завади (шуму) подавались в різних комбінаціях та з різними співвідношеннями сигнал/завада.

Результати досліджень, які проводились компанією Beranek & Newman з 1948 по 1953 рр., були опубліковані в [20]. Їх головним здобутком стала ідея використання спеціалізованих акустичних шумів та систем (пристроїв) для захисту мовної інформації в телекомунікаційних мережах та на виділених об'єктах. Був сформований напрям «Системи контролю акустичної завади».

Подальші дослідження впливу різних типів шумів на рівень захищеності мовної інформації на межі контрольованої зони, розділились на декілька напрямів, які досліджували окремі параметри впливу. До таких напрямків слід віднести:

– дослідження псевдовипадкових послідовностей з заданими параметрами стійкості до ре-інжинірингу для генераторів «білого» шуму;

– дослідження впливу частотної реверберації на можливість відновлення мовної інформації [21–23];

– дослідження можливості виділення «конкретного» диктора з розмови, при одночасній мові двох і більше дикторів [24, 25];

– розробка методів виявлення ознак мовного сигналу в складнозашумлених фонограмах [26, 27].

Одним з провідних досліджень нашого часу є розробка методів відновлення мовної інформації в умовах наявності шумів. Найбільшого поширення отримав метод на основі *MFCC*-коефіцієнтів (*Mel-frequency cepstral coefficients*). Його використовують і як інструмент досліджень і в якості базового методу для верифікації запропонованих методів та отриманих результатів. Так, в [21] розглянуто вплив реверберації та шуму в умовах «тісного» приміщення. Показано, що за певних умов (взаєморозміщення джерела сигналу та джерела завади, співвідношення сигналів та інше) запропонована в [21] бінауральна система показала значно кращі результати по відношенню до звичайної системи розпізнавання на основі *MFCC*-коефіцієнтів (*Mel-frequency cepstral coefficients*). В роботі показано, що основним інтервалом використання запропонованої авторами бінауральної системи і *MFCC*-коефіцієнтів є співвідношення сигнал/завада з *SNR*>0 дБА. Таким чином, для відновлення сигналів, що зазнали деструктивного впливу акустичної завади з використанням вказаних методів, є малоймовірним.

Подальший розвиток дослідження можливості відновлення мовної інформації отримали в [22]. В роботі запропоновано використання методу зважування коефіцієнту *TFR* (*Term Frequency representation*) мови з використанням слухової схильності для шумозахисного *ASR* (*Automatic Speech Recognition*). Запропоноване в роботі поєднання багатопотокової системи за допомогою використаного методу та однопотокової системи з залученням технології спектрального маскування *EBM* (*Estimated Binary Mask*) ще більше

знизило *WER* (*Word Error Rate*). Однак, система залишилась вразливою до шумової завади з *SNR*<0 дБА.

В [23] розглядаються особливості використання синтезованих шумів для формування сигналу завади. Запропонований в роботі метод частотної реверберації показує досить непогані результати по рівню деструктивного впливу на тест-сигнал. Однак, приведена в роботі спектрограма (рис. 6 в [23]) досить наглядно демонструє недоліки даного методу – наявність повторюваності сигналу (реверберація) в частотному діапазоні. Ускладнення алгоритму формування завади за вказаною методикою досить легко нівелюється використанням нейронної мережі в системі фільтрації.

Представниками наступного напрямку робіт є [24, 25].

В [24] пропонується за допомогою ймовірнісного методу відстежувати сприйнятий крок для потенційно аперіодичних звуків, а також відстежувати висоти тону з декількох одночасних джерел. При цьому використання інваріантного зсуву представлення в області постійного *Q* дозволяє моделювати прийняті зміни кроку як вертикальні зрушення спектрів. Це дозволяє відстежувати ці зміни звуків з довільним спектральним профілем.

Однак, запропонований в [24] метод не дозволяє розпізнавати реверберaційні сигнали, які можуть стати джерелом значної шумової завади.

В [25] представлені результати досліджень лабораторії корпорації Google по розпізнаванню диктора (або динаміка) на фоні розмови інших людей чи значних шумових завадах, створених системою озвучення приміщення. Запропонована в [25] методика відокремлює голос диктора від сигналів декількох динаміків, використовуючи опорний сигнал з голосу диктора. Це досягається шляхом навчання двох окремих нейронних мереж:

– 1-га мережа – розпізнавання диктора, формує мовно-дискримінаційні вектори представлення слів;

– 2-га мережа – маскування спектрограм, створює маску на основі прийнятого сигналу мови диктора та шумової завади.

Такий підхід дозволив підвищити рівень виділення мови диктора – коефіцієнт WER зменшується з 55,9 % до 23,4 % для випадків з двома дикторами (диктор та динамік акустичної системи).

До недоліків вказаного методу необхідно віднести досить складний алгоритм навчання нейронних мереж, який вимагає наявності «чистої» мови диктора на початковому етапі. Також в роботі не вказано на співвідношення сигнал/завада, при яких отримані результати.

Для розпізнавання мовного сигналу на фоні акустичного шуму використовують методи енергетичного контролю та на основі ентропії спектру сигналу [26]. Дослідження проводились для різних сигналів та завади (сигнали вибирались з бази *TIDigits*, а шуми – *Noisex*) та при значних рівнях шумової завади (–10 дБА<*SNR*<10 дБА). В роботі показано, що використання ентропії спектру сигналу для виявлення ознак мовного сигналу є більш ефективним. Одночасно з цим, необхідно відмітити, що до використаної бази шумових сигналів *Noisex* не входять мовоподібні сигнали на базі мови диктора, в тому числі й з бази *TIDigits*. А аналіз математичних залежностей, використаних в [26], показує неможливість

розпізнавання мовного сигналу вказаними методами – енергетичного контролю та на основі ентропії спектру сигналу.

В [27] наведені результати досліджень можливості виявлення ознак мовного сигналу при використанні методів *ZCR* (*Zero Crossing Rate*) та *STE* (*Short Time Energy*). Результати показали, що обидва методи забезпечують достатню точності виявлення мовного сигналу при *SNR*>0 дБА. Однак при SNR≤0 дБА обидва методи втрачають свою ефективність.

Таким чином, результати аналізу дозволяють зробити висновок про те, що сучасні методи цифрової обробки фонограм здатні відфільтрувати та відновити мовний сигнал, шо зазнав деструктивного впливу. Використання нейронних мереж дозволяє виявляти ознаки мовного сигналу в складнозашумлених фонограмах. Це дає змогу фільтрувати «білий» шум і його клонів, видаляти завади реверберaційного типу та, навіть, виділити диктора з розмови, в якій приймають участь двоє і більше людей.

5. Методи дослідження

5.1. Узагальнена схема генератора мовоподібного сигналу

Головною ідеєю генератора є використання комбінованого методу формування сигналу завади. Для збільшення його складності в процесі формування використовуються додатково два типи зовнішніх сигналів – фонограми дикторських текстів, які знаходяться в додатковій пам’яті пристрою, та сигнали з багатоканального ресивера, вбудованого в генератор. Узагальнена схема пристрою наведена на рис. 1.

В загальному випадку, метод формування сигналу завади в блоці «Змішування» описується виразом:

$$S_i(t) = A_i(t) + SS_{i-1}(t) + \sum_{j=1}^{k_{in}} M_j(t) + \sum_{z=1}^{k_{of}} R_z(t), \qquad (1)$$

де $A_i(t)$ – мовний сигнал, озвучений диктором;

$S_{i-1}(t)$ – сигнал завади попереднього циклу;

$M_j(t)$ – *j*-ий елемент масиву, який є випадковою послідовністю з $k_{in}=u+rnd(w)$ елементів (номерів фонограм);

$R_z(t)$ – z-ий елемент масиву, який є випадковою послідовністю з $k_{of} = p + rnd(t)$ елементів (номерів ресиверів);

u та *w* – мінімальна кількість фонограм, які повинні бути підключеними до тракту формування сигналу завади та загальна кількість фонограм в блоці пам’яті генератора;

p та *r* – мінімальна кількість каналів ресивера, які повинні бути підключеними до тракту формування сигналу завади та загальна кількість каналів ресивера вистроєного в генератор.

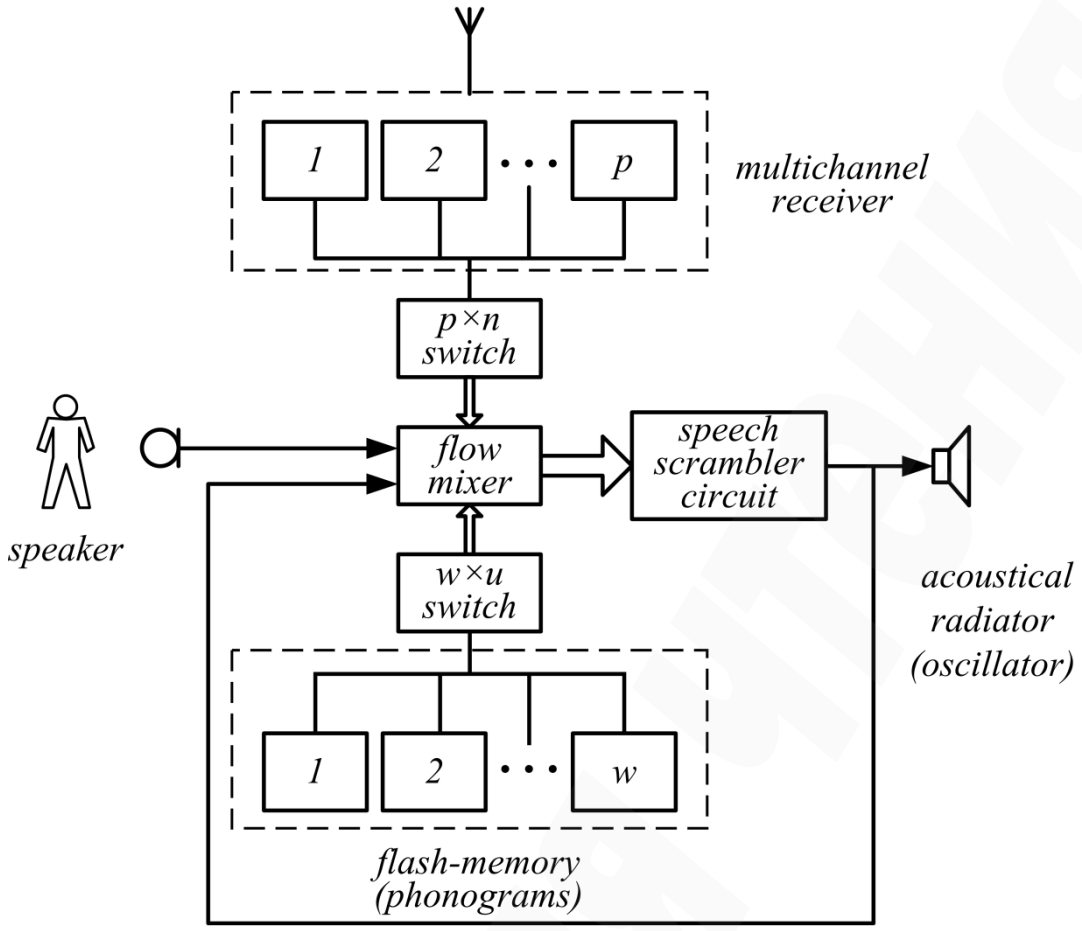


Рис. 1. Узагальнена структурна схема генератору мовоподібного сигналу завади скремблерного типу для систем протидії витоку мовної інформації акустичними та вібраційними каналами

В блоці «Скремблювання» сигнал завади кодується на основі комплексного сигналу $S_i(t)$, до складу якого входить мовний сигнал диктора (який і підлягає захисту). Для зменшення ефективності методів ре-інжинірингу в блоці «Скремблювання» використано динамічну зміну коефіцієнтів кодування.

Процедура синтезу включає два незалежних перетворення – по частоті та часу:

$$SS(f,t)=\begin{cases}\sum\limits_{j=1}^{n}\sum\limits_{i=1}^{m}A\left(f_{b_j+(-1)^{a_j}\cdot i+m\cdot a_j}\right);\\ \sum\limits_{y=1}^{k_t}\sum\limits_{x=1}^{h_t}A\left(t_{d_y+(-1)^{c_y}\cdot x+h_t\cdot c_y}\right);\end{cases} \quad (2)$$

де j та n – номер та кількість ⅓-октавних смуг (за звичаєм n=18…21);

i та m – номер та кількість тонових частот в ⅓-октавних смугах (визначається рівнянням ШПФ (швидкого перетворення Фур'є));

a_j – j-ий елемент бітового масиву $a=rnd(0,1)\big|_n$, який є випадковою бітовою послідовністю з n елементів (забезпечується кодування прямого/інверсного переміщення смуг);

b_j – j-ий елемент масиву $\dot{b} = rnd(0...1)$, який є випадковою послідовністю з n елементів;

y та k_t – номер та кількість тимчасових блоків, на які розділено вікно періоду обробки сигналу (визначається як випадкове число $k_t = 8 + rnd(8)$;

x та h_t – номер та кількість часових смуг, на які розділено тимчасовий блок обробки сигналу (визначається як випадкове число $h_t = 3 + rnd(8)$);

c_y – y-ий елемент бітового масиву $\dot{c} = rnd(0,1)\big|_{k_t}$, який є випадковою бітовою послідовністю з k_t елементів (забезпечується кодування прямого/інверсного переміщення тимчасових смуг);

d_{t_y} – y-ий елемент масиву $\dot{d}_t = rnd(1...k_t)$, який є випадковою послідовністю з k_t елементів.

При проведенні кодування завадового сигналу період його обробки T визначається з залежності $T = k_t \cdot h_t \cdot \left[0,05 + 0,01 \cdot rnd(10)\right] = var$.

5.2. Модель генератора мовоподібного сигналу

Моделювання генератора виконана в середовищі *Matlab 15 R2015a/Simulink*. При моделюванні використана спрощена структура пристрою – не використовуються зовнішні джерела мовних сигналів (багатоканальний ресивер та флеш пам'ять). Це дозволяє дослідити можливості блоку «Скремблювання» на мінімальних режимах стійкості до ре-інжинірингу.

На рис. 2 наведено математичну модель генератора.

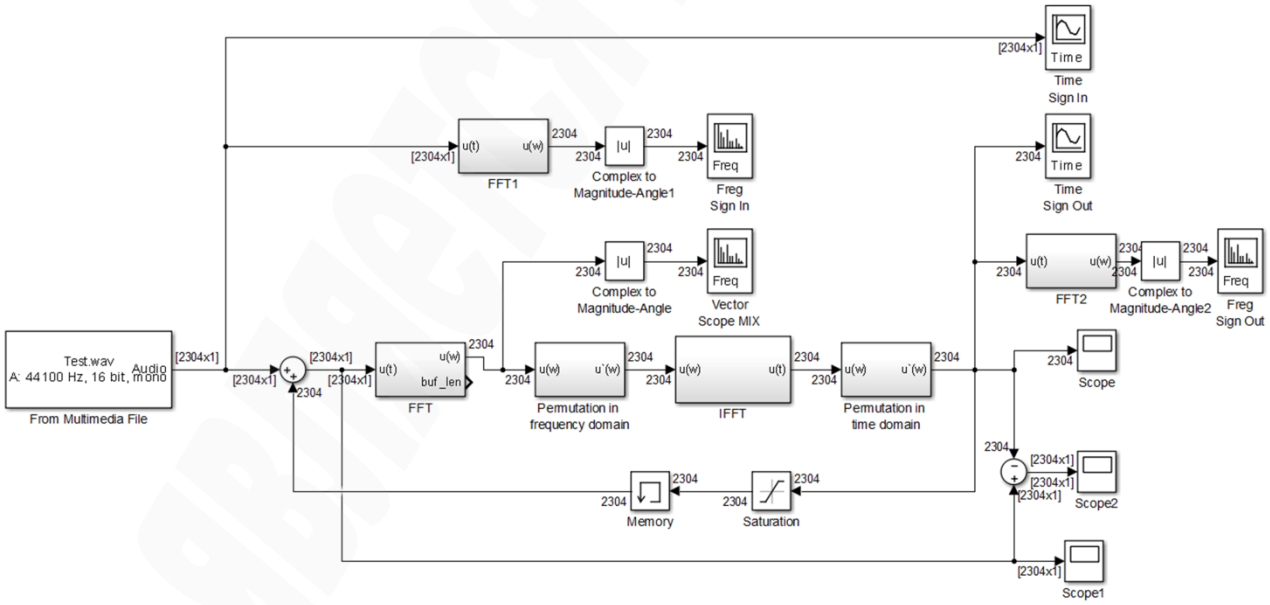
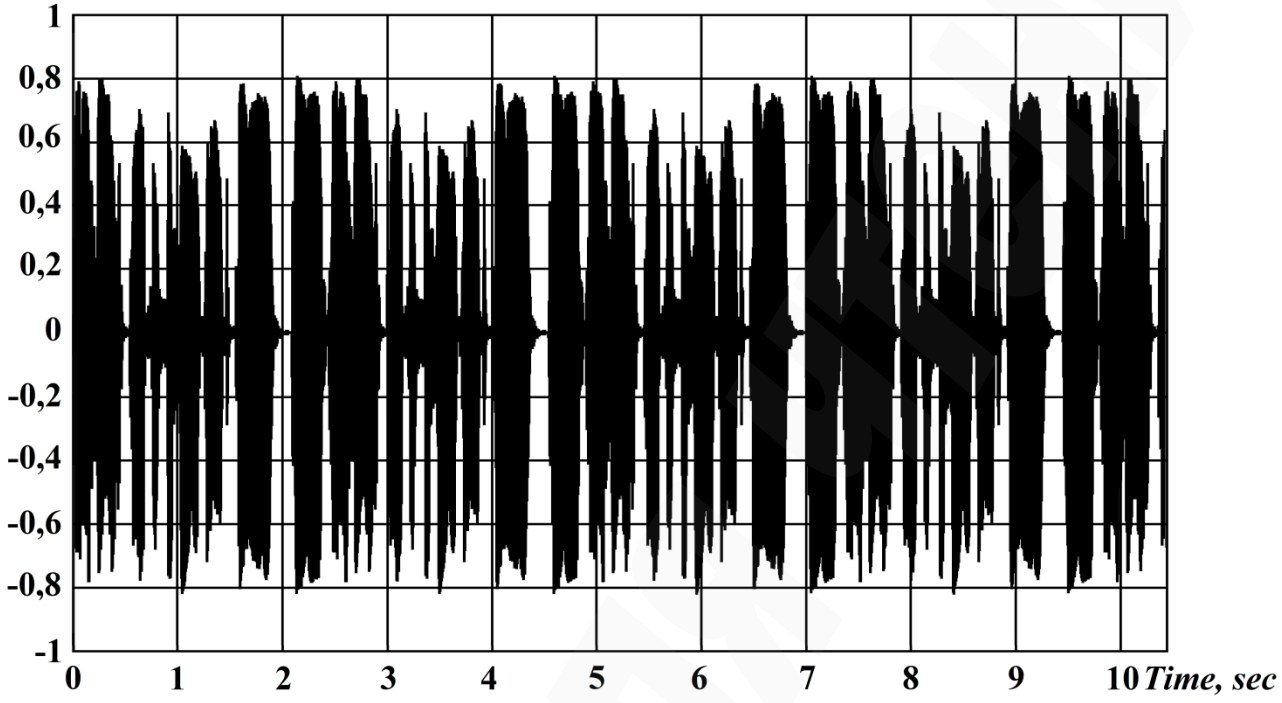


Рис. 2. Модель генератору мовоподібного сигналу завади скремблерного типу

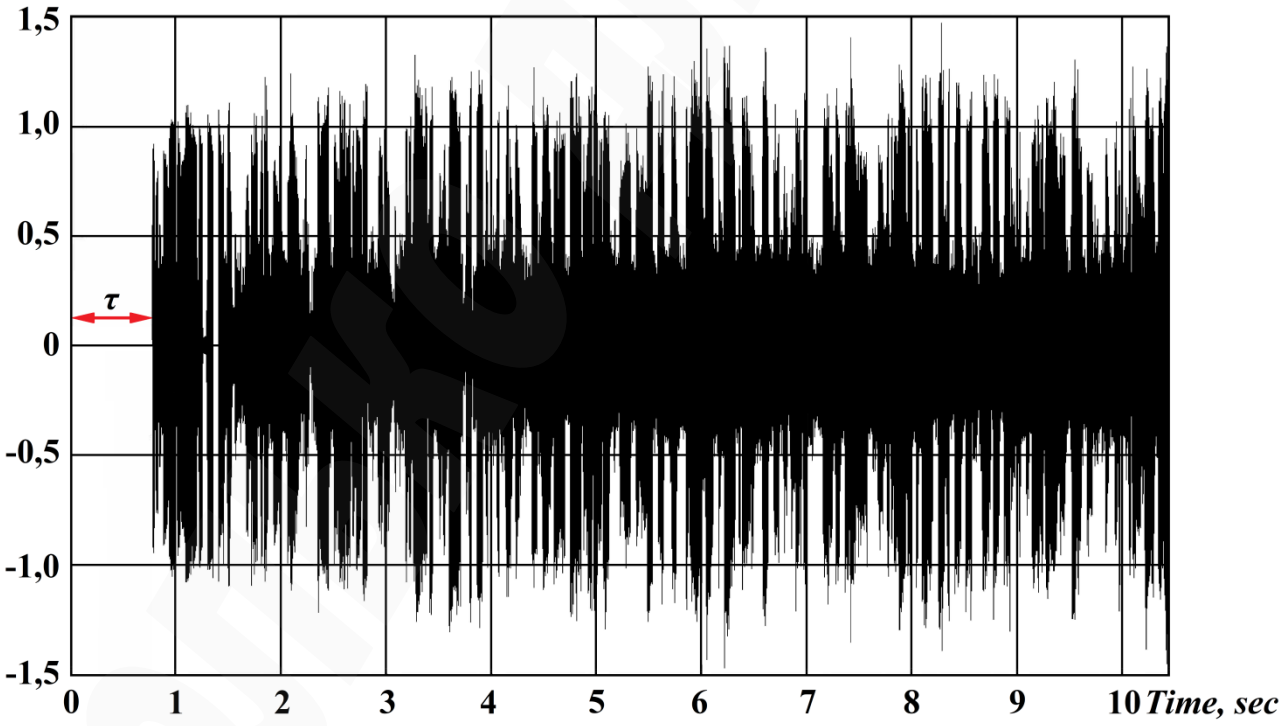
Для тест-сигналу використана коротка фраза «Вивів корабель на посадкову траєкторію». Для отримання неперервного сигналу фонограма зациклена на відтворення.

На рис. 3 наведені тимчасові, а на рис. 4 – частотні осцилограми.

Основними параметрами блоку скремблювання, прийнятими незмінними для спрощення аналізу результатів моделювання, є розмір вікна тимчасових перестановок – 0,52 мс, та кількість смуг при частотному скремблюванні – 16.



а



б

Рис. 3. Тимчасова діаграма:
а – вхідний тест-сигнал (Time Sign In); *б* – вихідний сигнал (Time Sign Out)

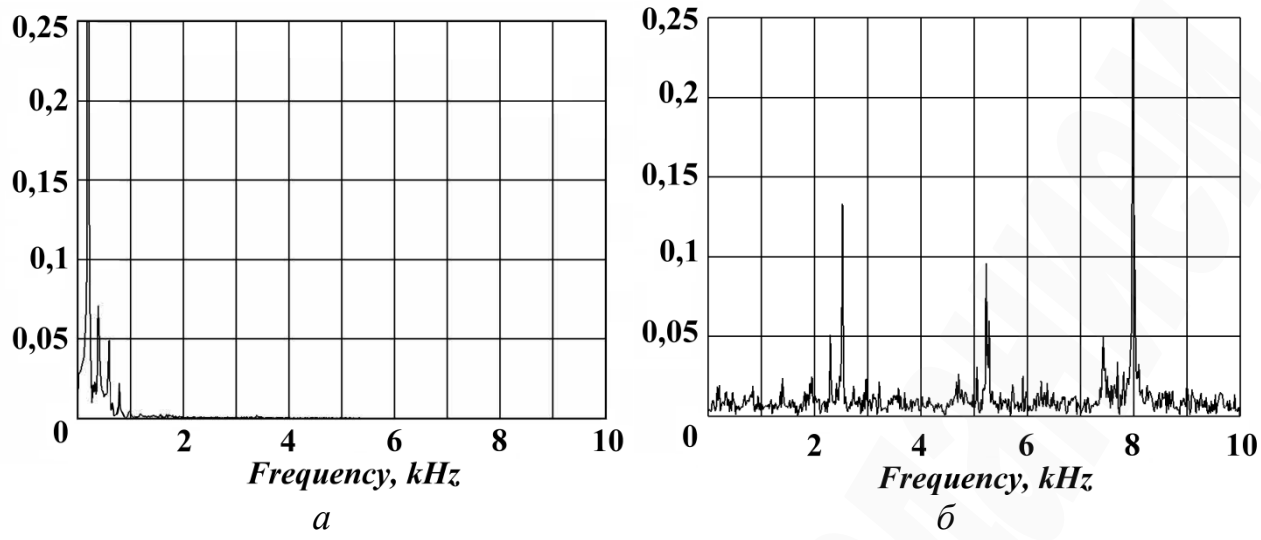


Рис. 4. Спектрограми:
а – вхідний тест-сигнал (*Time Sign In*); *б* – вихідний сигнал (*Time Sign Out*)

Аналіз наведених результатів показує, що:

1. Вхідний тест-сигнал відповідає вимогам простої неперервної мови:

– протяжність тест-сигналу становить, приблизно, 2 с (рис. 3, *а*);

– проміжок при повторенні тест-сигналу складає 0,2 с (рис. 3, *а*);

– кількість повторень тест-сигналу – більше 5 разів (рис. 3, *а*);

– основні лінгвістичні параметри фонем (частота основного тону *F*0 та основні форманти *F*1, *F*2 та *F*3) є чітко визначеними (рис. 4, *а*) та знаходяться в проміжку від 200 Гц до 1000 Гц;

– частотний діапазон, який займає сигнал (від 20 Гц до 5600 Гц) є типовим для фонограм, що обробляються на персональному комп'ютері, без використання в його складі додаткових апаратно-програмних пристроїв.

2. Вихідний сигнал зміщений по відношенню до вхідного на 0,75 с, що зумовлене особливостями роботи блоку «*Permutation in time domain*» (рис. 2), та прийнятими для моделювання розмірами вікна тимчасових перестановок.

3. «Вихід» пристрою на робочий режим, згідно рис. 3, *б*, складає 4 с – в вихідному сигналі не можливо виділити окремі слова та фонеми.

4. Аналіз спектрограми вихідного сигналу (рис. 4, *б*) показує:

– неможливість виділення основних лінгвістичних параметрів фонем;

– діапазон частотного спектру сигналу розширився до 10 кГц;

– в спектрі вихідного сигналу присутні три групи максимумів, розміщених через інтервал, приблизно 2,5…2,6 кГц, однак, ні набором частотних складових, ні характерними ознаками вони не корелюються між собою та спектром тест-сигналу.

6. Результати дослідження

6.1. Верифікація результатів дослідження математичної моделі генератора мовоподібного сигналу завади скремблерного типу

Для підтвердження результатів дослідження математичної моделі генератора мовотодібного сигналу розроблено дослідний зразок пристрою – генератор реальної мовоподібної завади ОССА-1, розробленого в лабораторії

систем технічного захисту інформації Національного університету кораблебудування (м. Миколаїв, Україна) [28]. Результати досліджень, з урахуванням вимог до рівня захищеності мовної інформації в залежності від категорії зони, наведені на рис. 5.

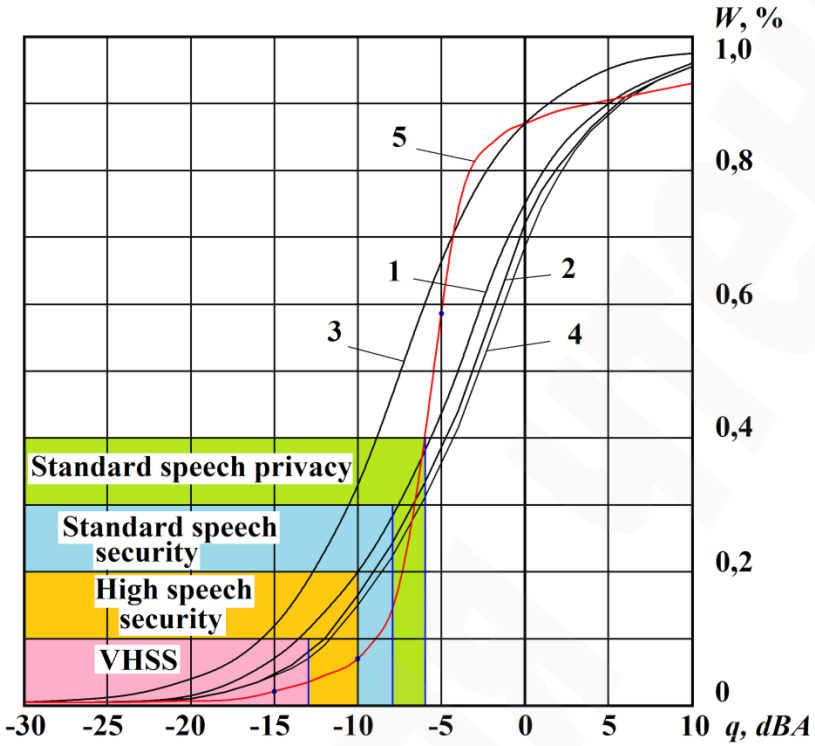


Рис. 5. Залежність словесної розбірливості *W* від інтегрального відношення сигнал/завада *q*: 1 – «білий» шум; 2 – «рожевий» шум; 3 – «коричневий» шум; 4 – «мовоподібний» шум; 5 – реальна мовоподібна завада, сформована генератором ОССА-1; *VHSS – Very high speech security*

При вказані зон захищеності на рис. 5 за основу взято «білий» шум (лінія 1). Графіки залежності словесної розбірливості *W* від інтегрального відношення сигнал/завада *q* для «білого», «рожевого», «коричневого» та «мовоподібного» шумів визначені експериментально та порівняні з [29] – відхилення отриманих значень склало менше 3 %. При проведенні досліджень використовувався артикуляційний метод. Більш докладно схема установки та методика проведення дослідження викладені в [28].

Дослідження показали більш високу ефективність завади, яку сформував генератор ОССА11, в порівнянні з типовими методами формування акустичної завади на основі «білого» шуму та його клонів [5]. Згідно рис. 5, генератор ОССА-1 синтезує шумову заваду (при $SNR \leq -8$ дБА), вплив якої достатній для виконання вимог по запобіганню витоку мовної інформації з зони категорії VHSS.

6.2. Обговорення результатів дослідження математичної моделі генератора мовоподібного сигналу завади скремблерного типу

В роботі запропоновано новий підхід до формування сигналу завади для систем постановки активних акустичних та вібраційних завад – використання

принципів скремблерування. Незважаючи на те, що самі пристрої (скремблери), свого часу, були досить розповсюдженими та широко використовувались в телекомунікаційних мережах, їх використання в якості генераторів завади в літературі не зафіксовано.

Запропонована схема та її математична модель дозволили визначити декілька особливо вагомих параметрів:

1. Час готовності системи до роботи, після включення або довгої паузи в розмові (в найпростішому варіанті, який був взято за основу при створенні моделі), складає 4 с. Таким чином, необхідно враховувати початковий етап виходу системи на робочий режим і обмежити тематику спілкування загальними темами.

2. Як видно з рис. 5, при використанні запропонованого методу для захисту мовної інформації в зоні з категорією «Standard speech private», її ефективність в порівнянні з типовими пристроями не значна. Суттєві переваги в рівні захищеності мовної інформації від витоку акустичними та вібраційними каналами запропонований метод синтезу завади надає при співвідношеннях $SNR \leq -8$ дБА. Це на 6…10 дБА менше, ніж рівень завади, який повинні створити генератори шуму, що використовують типові методи («білий» шум та його клони).

7. SWOT-аналіз результатів досліджень

Strengths. Проведені в середовищі Matlab 15 R2015a/Simulink дослідження математичної моделі та їх верифікація на дослідному зразку показали високий рівень деструктивного впливу запропонованого методу формування шумової завади. Використання генераторів такого типу на об’єктах інформаційної діяльності забезпечить:

– підвищення рівня захищеності мовної інформації від витоку акустичними та вібраційними каналами за рахунок підвищеної стійкості до сучасних методів фільтрації (вейвлет-перетворення, кореляційних та спектральних аналізів та ін.);

– зниження рівня акустичного та вібраційного шумового фону в контрольованому приміщенні, який створюється системою постановки активної завади, на 6…10 дБА, що суттєво покращує умови праці;

– зменшення демаскуючого рівня об’єкту за рахунок зниження рівня гучності шумової завади та використання методу «мовних хор» – для стороннього спостерігача перехоплений сигнал відповідає критеріям «відкритого» суспільного заходу;

– модернізація існуючих КСЗІ не потребує значних матеріальних витрат – необхідна заміна тільки генератора завади.

Weaknesses. Реалізація генератора мовоподібного сигналу завади скремблерного типу для систем протидії витоку мовної інформації акустичними та вібраційними каналами в відповідності до структури, яка зображена на рис. 1, потребує значних матеріальних витрат. Орієнтовно, вартість генератора буде на 30…40 % більша за типовий (за вказані в розділі 1). Однак, цей недолік в повній мірі компенсується підвищенням рівня безпеки.

Opportunities. Проблема забезпечення захисту мовної інформації від витоку технічними акустичними та вібраційними каналами та її несанкціоноване перехоплення зловмисником є перспективною для всіх країн світу. Таким чином, запропонована методика є предметом досліджень у всіх провідних країнах, а отримані результати відносяться до розряду «know how».

Threats. Можливими загрозами, яким через якийсь час доведеться протистояти розробникам виробів з запропонованим методом формування завади, є нові методи математичної обробки цифрових фонограм, що реалізовані на нейронних мережах (штучному інтелекту). Використання таких систем може призвести до небажаного виділення небезпечного сигналу (мови диктора) на фоні шумової завади.

Система спроможна протидіяти вказаній загрозі шляхом врахування принципів виділення мови окремого диктора з мовного хору – така модернізація передбачена в схемі пристрою.

8. Висновки

1. Запропоновано математичну модель генератора мовоподібного сигналу, в якій вперше використано комбінований метод аналогового кодування (скремблювання) мови диктора та сторонніх джерел мовних сигналів, для систем постановки активної віброакустичної завади. Це дало змогу уточнити узагальнену структурну схему генератору мовоподібного сигналу завади скремблерного типу та синтезувати аналітичні залежності для математичного апарату моделі.

В моделі використано принцип накопичувального закільцьовування сигнального потоку (змішування вхідного та вихідного сигналів) та використання частотно-смугових та тимчасово-смугових перестановок (скремблювання), що суттєво ускладнює ре-інжиніринг вихідного сигналу.

Запропоновані аналітичні залежності передбачають використання динамічних ключів для систем кодування в блоці скремблювання та підключення сторонніх джерел мовних сигналів. В якості сторонніх сигналів запропоновано використовувати набір фонограм (на змінних флеш-носіях) та он-лайн сигнали з радіоефіру. Це суттєво ускладнює процедуру ре-інжинірингу.

2. Розроблено та досліджено в середовищі *Matlab 15 R2015a/Simulink* спрощену математичну модель генератора мовоподібного сигналу. Дослідження показали високу ефективність запропонованого методу формування акустичної завади. Встановлено, що система має певну затримку при виході на «робочий режим». Затримка склала 4 с.

В спрощеній математичній моделі не включені сторонні джерела мовного сигналу та використано статичні ключі параметрів системи кодування. Це дозволило дослідити найбільш вразливий варіант реалізації пристрою. При цьому рівень деструктивного впливу згідно аналізу тимчасових та спектральних характеристик задовільнив вимогам.

3. Для перевірки достовірності результатів математичного моделювання проведені лабораторні дослідження дослідного зразка пристрою – генератор реальної мовоподібної завади ОССА-1, розробленого в лабораторії систем

технічного захисту інформації Національного університету кораблебудування (м. Миколаїв, Україна). Дослідження проводились артикуляційним методом. Встановлювалась залежність словесної розбірливості *W* від інтегрального відношення сигнал/завада *q*. Порівнювались результати впливу типових шумових завад («білий» шум та його клони) та шумової завади, створеної генератором. Результати досліджень показали, що для захисту мовної інформації в зоні з категорією «Standard speech private» її ефективність є не гіршою в порівнянні з типовими пристроями. Однак, для зони з категорією «High speech security» ефективність вже склала 6…10 дБА. Це забезпечує зниження рівня акустичного та вібраційного шумового фону в контрольованому приміщенні, який створюється системою постановки активної завади, до 10 дБА, що суттєво покращує умови праці.

Література

1. *On Protection of Information in Automated Systems. Law of Ukraine No. 80/94-BP*. 05.07.1994. Available at: https://zakon.rada.gov.ua/laws/main/80/94-%D0%B2%D1%80
2. *On State Secret. Law of Ukraine No. 3855-XII*. 21.01.1994. Available at: https://zakon.rada.gov.ua/laws/show/3855-12
3. *On Protection of Personal Data. Law of Ukraine No. 2297-VI*. 01.06.2010. Available at: https://zakon.rada.gov.ua/laws/main/2297-17
4. *Normatyvnyi dokument systemy tekhnichnoho zakhystu informatsii ND TZI 2.4-010-2015*. Available at: http://www.dsszzi.gov.ua/dsszzi/control/en/publish/article;jsessionid=D90D601C55F63184CFC22F8E76C42F44.app1?art_id=149166&cat_id=89991
5. *Normatyvnyi dokument systemy tekhnichnoho zakhystu informatsii ND TZI 2.3-019-2015*. Available at: http://www.dsszzi.gov.ua/dsszzi/control/en/publish/article;jsessionid=D90D601C55F63184CFC22F8E76C42F44.app1?art_id=149166&cat_id=89991
6. *Normatyvnyi dokument systemy tekhnichnoho zakhystu informatsii ND TZI 2.2-008-2015*. Available at: http://www.dsszzi.gov.ua/dsszzi/control/en/publish/article;jsessionid=D90D601C55F63184CFC22F8E76C42F44.app1?art_id=149166&cat_id=89991
7. Perelik zasobiv tekhnichnoho zakhystu informatsii, dozvolenykh dlia zabezpechennia tekhnichnoho zakhystu derzhavnykh informatsiinykh resursiv ta informatsii, vymoha shchodo zakhystu yakoi vstanovlena zakonom (stanom na 30 lypnia 2018). *DSSZZI Ukrainy*. Available at: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=284094&cat_id=39181
8. Vidomosti pro zasoby tekhnichnoho zakhystu informatsii, na yaki zakinchyvsia termin dii sertyfikativ vidpovidnosti ta ekspertnykh vysnovkiv (stanom na 1 sichnia 2017 roku). *DSSZZI Ukrainy*. Available at: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=234241&cat_id=39181
9. Grigorev, I. A., Kazanovskii, A. I. (2010). Metodicheskii podkhod k ocenke effektivnosti zaschity rechevoi informacii. *Vestnik Voronezhskogo gosudarstvennogo tekhnicheskogo universiteta, 5*, 133–136.
10. Nuzhnyi, S. M. (2018). Udoskonalena tekhnolohiia otsinky stupenia zakhystu movnoi informatsii. *Suchasnyi zakhyst informatsii, 1 (33)*, 66–73. Available at: http://journals.dut.edu.ua/index.php/dataprotect/article/view/179

11. Khorev, A. A. (2009). Ocenka vozmozhnostei sredstv akusticheskoi (rechevoi) razvedki. *Specialnaia tekhnika, 4*, 49–63.

12. Blintsov, V., Nuzhniy, S., Parkhuts, L., Kasianov, Y. (2018). The objectified procedure and a technology for assessing the state of complex noise speech information protection. *Eastern-European Journal of Enterprise Technologies, 5 (9 (95))*, 26–34. doi: http://doi.org/10.15587/1729-4061.2018.144146

13. Rybalskii, O. V., Solovev, V. I., Zhuravel, V. V. (2017). Fraktalnii podkhod k vyiavleniiu sledov cifrovoi obrabotki v analogovykh fonogrammakh. *Suchasna specialna tekhnika*, *1*, 4–9. Available at: http://nbuv.gov.ua/UJRN/sstt_2017_1_4

14. Solovev, V. I., Rybalskii, O. V., Zhelezniak, V. K. (2014). Multifraktalnaia struktura shepota i raspoznavanie rechevykh struktur. Vestnik Polockogo gosudarstvennogo universiteta. *Seriia C, Fundamentalnye nauki, 12*, 16–20.Available at: http://elib.psu.by:8080/handle/123456789/11215

15. Bortnikov, A. N., Gubin, S. V., Lobov, V. A., Siromashenko, A. V., CHernyshov, P. V. (2007). Rezultaty eksperimentalnykh issledovanii ocenki vozmozhnostei perekhvata rechevoi informacii pri realizacii metodov dvukhkanalnogo sema. *Voprosy zaschity informacii*, *1*, 11–17

16. Lobov, V. A., Siromashenko, A. V., Chernyshov, P. V. (2007). Ocenka vozmozhnostei perekhvata rechevoi informacii pri realizacii metoda mnogokanalnogo sema. *Voprosy zaschity informacii*, *4*, 27–35.

17. Licklider, J. C. R. (1948). The Influence of Interaural Phase Relations upon the Masking of Speech by White Noise. *The Journal of the Acoustical Society of America*, *20 (2)*, 150–159. doi: http://doi.org/10.1121/1.1906358

18. Shannon, C. E. (1998). Communication In The Presence Of Noise. *Proceedings of the IEEE, 86 (2)*, 447–457. doi: http://doi.org/10.1109/jproc.1998.659497

19. Miller, G. A., Licklider, J. C. R. (1950). The Intelligibility of Interrupted Speech. *The Journal of the Acoustical Society of America*, *22 (2)*, 167–173. doi: http://doi.org/10.1121/1.1906584

20. Bolt, R. H., Beranek, L. L., Newman, R. B. (1952). *Handbook of acoustic noise control.* Volume I. Physical Acoustics. doi: http://doi.org/10.21236/ad0012015

21. Rosenblith, W. A., Stevens, K. N. (1953). *Handbook of acoustic noise control.* Volume II. Noise and man. doi: http://doi.org/10.21236/ad0018260

22. Palomäki, K. J., Brown, G. J., Wang, D. (2001). A binaural model for missing data speech recognition in noisy and reverberant conditions. *Consistent & Reliable Acoustic Cues for sound analysis*. Aalborg.

23. Do, C.-T., Stylianou, Y. (2018). Weighting Time-Frequency Representation of Speech Using Auditory Saliency for Automatic Speech Recognition. *Interspeech 2018*. doi: http://doi.org/10.21437/interspeech.2018-1721

24. Prodeus, A. M., Vityk, A. V., Didenko, D. Y. (2017). Subjective evaluation of quality and intelligibility of speech distorted by synthesized noise. *Microsystems, Electronics and Acoustics*, *22 (6)*, 56–63. doi: http://doi.org/10.20535/2523-4455.2017.22.6.101929

25. Smaragdis, P. (2009). Relative-pitch tracking of multiple arbitrary sounds. *The Journal of the Acoustical Society of America, 125 (5)*, 3406. doi: http://doi.org/10.1121/1.3106529

26. Wang, Q., Muckenhirn, H., Wilson, K., Sridhar, P., Wu, Z., Hershey, J. R. et. al. (2019). VoiceFilter: Targeted Voice Separation by Speaker-Conditioned Spectrogram Masking. *Interspeech 2019*. doi: http://doi.org/10.21437/interspeech.2019-1101

27. Renevey, P., Drygajlo, A. (2001). Entropy based voice activity detection in very noisy conditions. *EUROSPEECH-2001*, 1887–1890. URL: https://www.isca-speech.org/archive/eurospeech_2001/e01_1887.html

28. Özaydın, S. (2019). Examination of Energy Based Voice Activity Detection Algorithms for Noisy Speech Signals. *European Journal of Science and Technology*, 157–163. doi: http://doi.org/10.31590/ejosat.637741

29. Kasianov, Yu. I., Nuzhnyi, S. M. (2016) Otsiniuvannia efektyvnosti heneratora realnoi movopodibnoi zavady za kryteriiem rozbirlyvist movy. *Visnyk Natsionalnoho universytetu «Lvivska politekhnika». Seriia: Avtomatyka, vymiriuvannia ta keruvannia, 852*, 105–110. Available at: http://ena.lp.edu.ua:8080/handle/ntb/36473

30. Khorev, A. A., Makarov, Iu. K. (2001). Metody zaschity rechevoi informacii i ocenki ikh effektivnosti. *Specialnaia tekhnika, 4*, 22–33.

The protection of speech information is one of the main tasks of information protection and is a sign of a responsible attitude of an organization (company) both to its information resources and respect for partners. The object of research is the process of protecting speech information from leakage by acoustic and vibrational technical channels at the objects of information activity. An exceptional feature of such facilities is the circulation, processing and discussion of issues containing information of limited access, including state secrets. A peculiarity of Ukraine is the requirement to use exclusively technical means that have passed the relevant certification at such facilities.

The basis of the active noise jamming system is a noise generator. At the same time, one of the most problematic issues is that in Ukraine only noise interference generators of the «white» noise type and its clones are allowed to be used. The systems have a number of significant drawbacks – the low protection level of intercepted speech signals from noise filtering (interference), a significant noise level in the premises to be protected, and others.

A block diagram of an interference generator is proposed. And its mathematical model is also developed and researched in Matlab. In the course of the research, a comparative analysis of the signals input and synthesized by the generator was carried out, their temporal and spectral characteristics were investigated. The obtained results indicate the high efficiency of the proposed method of protecting speech information. This is due to the fact that the method of forming a speech-like interference has a number of features that provide a significant destructive effect on speech information, namely the use of a combined scrambler model with time and frequency transforms. The method takes into account the use of dynamic keys for coding systems, and the connection of third-party sources of speech signals, as well as ringing (mixing of the input and output signals) at the input of the scrambling unit. This decision excludes reengineering.

The results are confirmed by the research of an experimental sample. The destructive effect of typical noise interference («white» noise and its clones) and the

noise interference created by the proposed method are compared by the criterion of residual speech intelligibility of the speaker's speech. Studies have shown that, provided that no more than 10 % of the level of residual intelligibility is provided, the volume level of the output signal of the noise interference generator can be reduced by almost 6 dBA.

Keywords: *scrambler-type speech-like generator, protection of speech information, information protection.*