https://doi.org/10.31649/1997-9266-2023-167-2-89-96

УДК 004.056.53.

В. В. Карпінець[1]
В. С. Катаєв[1]
П. В. Павловський[1]
Д. Ю. Гереш[1]

ЗАСІБ ЗАХИСТУ АНАЛОГОВОГО ТЕЛЕФОННОГО ЗВ'ЯЗКУ НА ОСНОВІ СКРЕМБЛЕРА ЗІ ЗМІНОЮ КОЕФІЦІЄНТІВ ВЕЙВЛЕТ-ПЕРЕТВОРЕННЯ

[1]Вінницький національний технічний університет

Запропоновано пристрій для забезпечення захисту мовної інформації, яка передається через лінії аналогового телефонного зв'язку від несанкціонованого перехоплення на основі скремблера зі зміною коефіцієнтів вейвлет-перетворень відповідно до латинського квадрату. Реалізовано пристрій, який складається з апаратної та програмної частин, апаратна частина реалізована на мікроконтролерній платформі плат сімейства Arduino, програмну частину пристрою реалізовано за допомогою програмного середовища Proteus. Оскільки основну частину функцій пристрою виконує мікроконтролер, то в загальному структура пристрою складається з мікрофону, джерела живлення та плати Arduino. Враховуючи результати досліджень, запропоновано модернізацію алгоритму скремблювання за рахунок виконання операцій перестановок, XOR відповідності до ключа скремблера, який є латинським квадратом. Здійснено статистичний та спектральний аналіз вдосконаленого методу та виконано порівняння швидкості виконання алгоритмів скремблювання. Для підвищення захищеності запропоновано здійснювати декілька етапів перестановок отриманих коефіцієнтів вейвлет-перетворень. Збільшення варіативності перестановок коефіцієнтів вейвлет-перетворень дозволило збільшити витрати часу зловмиснику на перебір усіх можливих комбінацій. А враховуючи, що перестановка відбувається не однієї частини сигналу, а набору n частин, це, і собі, додатково ускладнює процедуру перебору усіх можливих варіантів. Реалізація елементів цього пристрою за допомогою засобів електронно-обчислювальної техніки та загальнодоступних компонентів робить його доступним, а також ефективним засобом для вирішення завдань технічного захисту інформації, що може забезпечити покращення систем захисту інформації різних суб'єктів господарювання.

Ключові слова: технічний захист інформації, системи передавання інформації, скремблер, акустика, акустична інформація.

Вступ

На сьогодні майже неможливо уявити собі світ без щоденного застосування різноманітних засобів зв'язку або переоцінити їхній вплив на будь-яку сферу людської діяльності. Зокрема, телефонний зв'язок став невід'ємною частиною нашого повсякденного життя, особливо з розвитком мобільної телефонії. Значна частина несанкціонованого перехоплення інформації припадає саме на телефонні розмови, адже зазвичай телефонні мережі не мають достатнього рівня захисту. Метою несанкціонованого доступу до інформації є здебільшого політичний чи комерційний інтереси. Наприклад, бізнесмену потрібна інформація про конкурентів та інформація самих конкурентів про нього. Підсумовано, що втрата банком 20…25 % конфіденційної інформації призводить до його банкрутства. Знання конфіденційної інформації допомагає швидше й ефективніше вирішувати політичні, фінансові, бізнесові проблеми. Встановлено, що 47 % закритих відомостей здобувають за допомогою технічних засобів через технічні канали витоку інформації. Тому актуальною є проблема технічного захисту інформації і особливої уваги потребує на сьогодні питання захисту акустичної (мовної) інформації, що циркулює на об'єктах інформаційної діяльності [1].

Протягом останніх років спостерігається тенденція до переходу від аналогових телефонних систем до цифрових, але й досі в широкому використанні знаходяться аналогові пристрої, особливо в

державних структурах і великих підприємствах, в яких присутній внутрішній телефонний зв'язок. Головною проблемою аналогового зв'язку є те що, сигнали, які передаються лініями, ніяк не кодуються, що робить таке передавання критично вразливим до прямого перехоплення зловмисником.

Аналіз проблеми та постановка задачі

Наявність значної кількості елементів у телефонній мережі дозволяє зловмиснику здійснювати перехоплення інформації за допомогою широкого спектру засобів та методів у різних точках мережі. Більше того, зловмисник може використовувати телефонну мережу не тільки для прослуховування самих телефонних розмов, але й для прослуховування переговорів, що ведуться у приміщенні, в якому знаходиться телефонний апарат [2].

За роки використання аналогових телефонних систем з'явилось декілька способів підключення до телефонної лінії, за допомогою яких здійснюється несанкціоноване перехоплення інформації. Найпростішим у реалізації способом несанкціонованого підключення є просте контактне підключення до лінії зв'язку з подальшим виведенням на паралельний телефонний апарат, записуючий пристрій або передавач. Але такий тип підключення дуже просто виявити, оскільки за такого виду підключення в мережі дуже падає напруга, що можна виявити найпростішими пристроями контролю параметрів лінії. У зв'язку з чим, для маскування факту несанкціонованого підключення зловмисником можуть використовуватись спеціальні узгоджувальні пристрої, які компенсують зміни параметрів телефонної лінії. Такий спосіб ускладнює, але не уможливлює виявлення факту підключення, оскільки компенсувальний пристрій часто не враховує індуктивні параметри лінії, які також змінюються у разі несанкціонованого підключення. Таким чином, методи безпосереднього підключення мають значний недолік — порушення цілісності лінії і зміну її електричних параметрів.

Іншим варіантом знімання інформації з провідних телефонних ліній є підключення індуктивного струмознімача. Ці пристрої неможливо виявити шляхом вимірювання електричних параметрів каналу зв'язку, оскільки вони знімають сигнали з лінії за рахунок котушки індуктивності, яка розташовується навколо лінії без безпосереднього підключення до неї. Таким чином відбувається зняття електромагнітних коливань, які згодом перетворюються в електричні коливання, після цього отриманий сигнал підсилюється та передається або записується на диктофон. Єдиними недоліком такого методу є висока чутливість до електромагнітних завад і, як наслідок, зниження якості перехопленої інформації.

Таким чином, існує низка загроз витоку інформації, через телефонну лінію, при чому методи захисту від одного виду загроз не завжди допоможуть захиститись від іншого. Так, наведений вище контроль параметрів лінії з допомогою спеціальних аналізаторів ніяк не допоможе зафіксувати підключення індуктивного знімача, а використання лінійного зашумлення допоможе від прослуховування тільки у момент, коли телефон знаходиться у режимі очікування. Відповідно постає питання вибору методу захисту, який би дозволив перекрити максимальну кількість загроз, забезпечував достатній рівень захищеності і при цьому би не заважав нормальному функціонуванню телефонної лінії. За наявності великої кількості потенційних загроз, оптимальним рішенням буде не блокування кожної можливої точки витоку сигналу, а перетворення небезпечного сигналу у форму, яку зловмисник не зможе прослухати навіть у випадку, якщо йому вдасться перехопити цей сигнал, тобто використовуючи шифрування.

Для захисту мовної інформації використовують так звані спеціалізовані засоби шифрування звукового сигналу — скремблери. Також, аналогові скремблеми можуть перетворювати сигнал за трьома параметрами: амплітудою, частотою та часом, але на практиці використання амплітудного перетворення сигналу не використовується, оскільки відтворення амплітуди на іншій стороні лінії зв'язку є досить неточним, це пов'язано з високим рівнем шумів і завад у телефонній мережі, які постійно змінюють відношення «сигнал/шум», що і впливає на амплітуду [3].

Додатково аналогові скремблери поділяють відповідно до режиму роботи на два таких типи:

– статичні системи, в яких схема кодування не змінюється протягом усього процесу перетворення мовного сигналу;

– динамічні системи, ключі яких динамічно, у деяких випадках декілька разів, генеруються в ході процесу передавання мовної інформації.

Порівнюючи ці два типи, очевидним стає факт, що скремблери з динамічними системами здатні забезпечити значно вищу ступінь захищеності, ніж системи зі статичним ключем. Однак склад-

ність таких систем зазвичай призводить до того, що динамічні системи набагато дорожчі у реалізації. Також, використання динамічних систем в деяких випадках призводить до створення значних затримок у процесі зв'язку [4]. Особливо цей факт актуальний у методах часового скремблювання.

Також слід зазначити, що з розвитком інформаційно-телекомунікаційних систем широкого застосування набули методи скремблювання з перетворення аналогового сигналу в цифровий. Ці методи забезпечують значно вищий рівень захищеності мовної інформації в процесі шифрування [5]. На сьогодні на ринку наявні в основному цифрові скремблери, але різноманітність існуючих зразків відносно невелика. У більшості випадків наявні скремблери дозволяють захистити інформацію на достатньому рівні, особливо це характерно для пристроїв захисту стільникових телефонних мереж. Гірша ситуація спостерігається з аналоговими системами передавання даних, в яких значна кількість скремблерів використовує прості методи захисту, які не здатні забезпечити високий рівень.

Для підвищення захищеності необхідно застосовувати ще й деякі додаткові методи скремблювання. Тому пропонується для підвищення захищеності процедури скремблювання застосовувати вейвлет-перетворення — інтегральні перетворення, які є поєднанням вейвлет-функції з сигналом [6]. Вейвлет-перетворення переводить сигнал з часового представлення у частотно-часове, що дає змогу стиснути вихідний набір даних. Додатково за допомогою вейвлет-перетворень можна усунути недолік частотних скремблерів, що мають рівномірне розбиття частотної смуги сигналу на підсмуги. У такому випадку перетворення мають діадне розбиття частотної смуги і постійне відносне розширення у всьому діапазоні частот сигналу. Це дозволяє зменшити ширину підсмуг у низькочастотній області та отримати рівномірний сигнал, тому використання цього перетворення у скремблюванні є перспективним. Таким чином вдосконалення існуючих методів скремблювання доцільно робити якраз на основі вейвлет-перетворень, насамперед за рахунок збільшення кількості можливих перестановок, що дозволить значно збільшити необхідний час на отримання зловмисником оригінального повідомлення.

Розробка алгоритму скремблювання на основі перестановок коефіцієнтів вейвлет-перетворень

Як зазначалось раніше, захищеність аналогового сигналу в скремблерах визначається часом, який зловмисник витратить на несанкціоноване отримання доступу до інформації. Тому у цій статті пропонується поліпшити захищеність за рахунок виконання двох етапів обробки коефіцієнтів вейвлет-перетворень. На першому етапі пропонується виконувати операцію перестановки відповідно до ключа, а на другому — виконання операції XOR отриманих коефіцієнтів з певним сеансовим ключем. Як секретний ключ пропонується використовувати значення латинських квадратів. Латинський квадрат — це таблиця, розміром $n \times n$ заповнена n різними елементами так, що в кожному стовпці і кожному рядку всі елементи зустрічаються по одному разу та кожний з них належить певній множині чисел $M = \{1, 2, 3\ldots, n\}$.

Одним із методів вейвлет-перетворення, що найкраще підходить для застосування у засобах зв'язку є дискретне вейвлет-перетворення. За своїми властивостями воно є альтернативою швидкому перетворенню Фур'є. Дискретне вейвлет-перетворення використовує для визначення вейвлет-коефіцієнтів фільтри низьких і високих частот. Таким чином увесь сигнал поділяється на області високих та низьких частот, при чому дані області є однаковими.

Важливою характеристикою цього перетворення є те, що низькочастотна область є важливішою, і тому за більшого масштабування сигналу відбувається поділ саме низьких частот. Максимальний рівень розкладання сигналу залежить від дискретизації сигналу (кількості значень сигналу N) та визначається за формулою

$$J = \log_2 N. \tag{1}$$

Здійснивши необхідний рівень масштабування шляхом поділу на високі та низькі частоти, отримуємо вектор з коефіцієнтами. Низькочастотні через свою більшу значущість називаються «апроксимуючими», а високочастотні виконують функцію доповнення низькочастотних і називаються «деталізуючими». Кожний вектор вейвлету буде мати однакову довжину та буде складатися з суми апроксимуючих та деталізуючих коефіцієнтів. Кількість коефіцієнтів залежить від максимального можливого рівня деталізації та вибраного. Розрахунок відбувається за формулою

$$K = 2^{J-l}, \tag{2}$$

де J — максимальний рівень розкладання сигналу, l — вибраний рівень.

Кожний такий вектор визначається за формулою

$$i(t) = \sum_{k=0}^{k} i_{j,k}^{A} \varphi_{j,k}(t) + \sum_{j=0}^{j} \sum_{k=0}^{k} i_{j,k}^{D} \varphi_{j,k}(t), \tag{3}$$

де $\varphi_{j,k} = a_0^{\frac{-j}{2}} \varphi\left(\frac{t - kb_0}{a_0^j}\right)$ — вейвлет, що аналізується від базисного вейвлета φ.

Перед початком скремблювання, необхідно отримані коефіцієнти об'єднати в одну матрицю $I_{x,y}$. Розмірність такої матриці залежить від кількості коефіцієнтів в одному сегменті сигналу, яка залежить від процедури дискретизації, що також залежить від апаратних можливостей вибраного мікроконтролера та рівня вейвлет-перетворення.

$$I_{x,y} = \begin{bmatrix} I_{1.1} & \cdots & I_{1.y} \\ \vdots & \ddots & \vdots \\ I_{x.1} & \cdots & I_{x.y} \end{bmatrix},$$

де $I_1 - \{I_{1.1}, I_{1.2} ... I_{1.y}\}$ — набір коефіцієнтів першого сегменту, $I_n - \{I_{x.1}, I_{x.2} ... I_{x.y}\}$ — набір коефіцієнтів другого сегменту.

Запропоноване вдосконалення алгоритму використовує два набори ключів, представлених у вигляді латинських квадратів. Розмірність таких квадратів має дорівнювати розмірності матриці $I_{x,y}$.

$$K_i = \begin{bmatrix} k_{1.1} & \cdots & k_{1.y} \\ \vdots & \ddots & \vdots \\ k_{x.1} & \cdots & k_{x.y} \end{bmatrix}.$$

На першому етапі скремблювання буде виконуватись операція перестановки значень коефіцієнтів $I_{x,y}$ по рядках та стовпцях. Для перестановки рядків буде використовуватись набір ключів вигляду $k_1 - \{k_{1.1}, k_{1.2}..., k_{1.y}\}$, для перестановки стовпців — $k_1 - \{k_{1.1}, k_{2.1}..., k_{x.1}\}$.

В загальному, даний етап можна представити схемою, яка показана на рис. 1.

Рис. 1. Перший етап перестановок

Перестановки на першому етапі алгоритму з ключем K_1 виконуються за такою формулою:

$$I'_{x,y} = I_{x,K_{(x,y)}}. \tag{4}$$

Аналогічним шляхом необхідно виконати відповідні перестановки, застосувавши ключ K_2 іншого учасника сеансу.

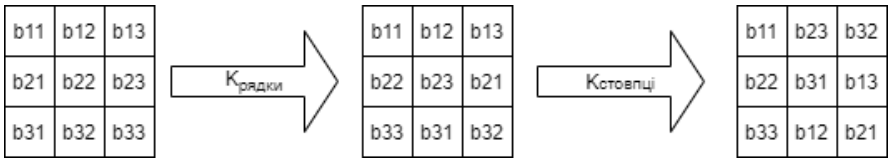

Рис. 2. Другий етап перестановок

Перестановки з ключем K_2 виконуються за такою формулою:

$$I''_{x,y} = I'_{K_{(y,x)},y}. \tag{5}$$

Як зазначалось вище, другим етапом алгоритму пропонується виконувати операцію XOR після кожного етапу перестановки. Операцію XOR слід виконувати відповідно таким чином:

$$B_{j,k} = \left(A_{j,k} \oplus K_{j,k} \right) \bmod n . \quad (6)$$

Після першого етапу перестановок з використанням першого ключа (отримання матриці значень $I''_{x,y}$) для операції XOR використовується ключ іншого учасника. Після другого етапу перестановок за ключем K_2, необхідно використати ключ K_1 для операції XOR. В загальному вигляді операція XOR коефіцієнтів з ключем показана на рис. 3.

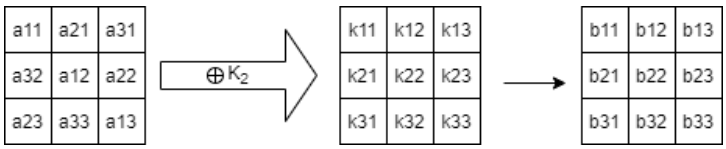

Рис. 3. Операція XOR коефіцієнтів з ключем

Отримавши таким чином набір коефіцієнтів, необхідно перетворити в аудіосигнал за допомогою зворотного дискретного вейвлет-перетворення за формулою

$$x(t) = K_{\varphi} \sum_{j,k=-\infty}^{\infty} \left(f, \varphi_{j,k} \right) \varphi^{j,k}(t). \quad (7)$$

Таким чином отримана матриця значень не може бути відтворена до початкового стану шляхом перебору усіх можливих значень. Відповідно застосування цієї операції буде ефективно впливати на захищеність запропонованого алгоритму. Більше того, запропоновані зміни дозволяють усунути такі недоліки стандартних скремблерів, як значні затримки під час передавання сигналу, зменшення якості сигналу та варіативності ключів. Блок-схема вдосконаленого алгоритму скремблювання у вигляді послідовності окремих ключових операцій показана на рис. 4.

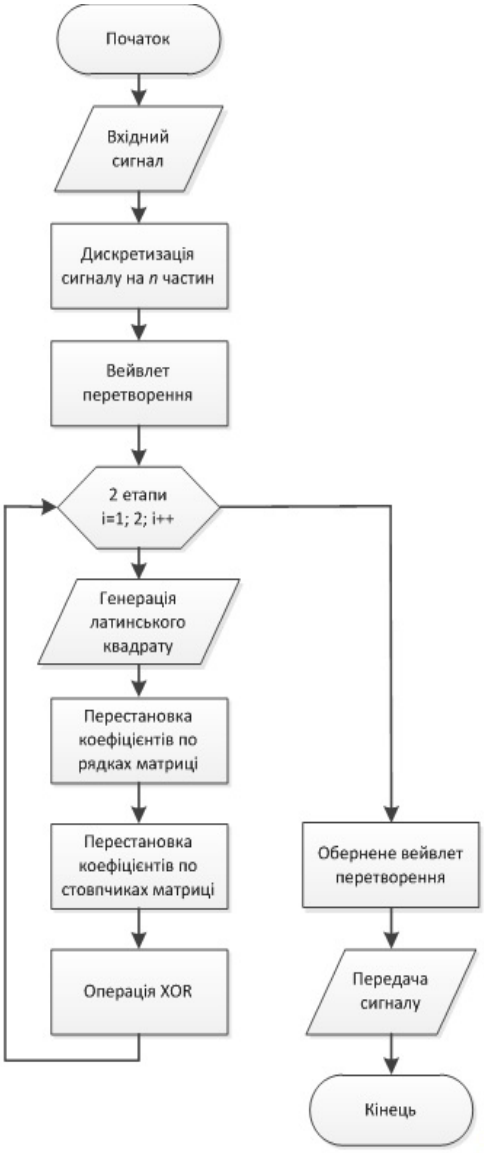

Рис. 4. Блок-схема алгоритму скремблювання

Розробка апаратної частини засобу захисту на основі запропонованого скремблера

Розроблений пристрій вирішено підключати до пристрою зв'язку після мікрофону та динаміка, тобто у випадку звичайного стаціонарного телефонного апарату скремблер буде включатись між слухавкою та розмовною схемою апарату. Таким чином, на вхід розробленого пристрою буде надходити інформаційний сигнал з лінії зв'язку, а на виході отримаємо скрембльований/дескрембльований сигнал. Спрощено структурну схему можна показати на рис. 5.

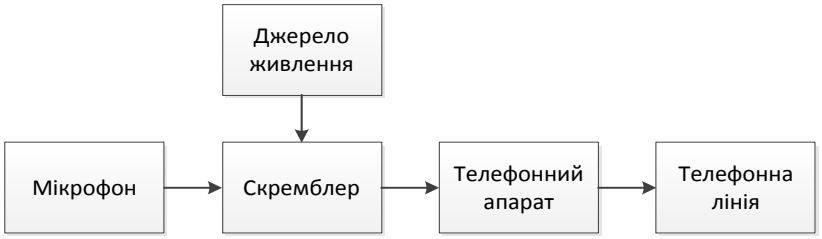

Рис. 5. Структурна схема розробленого пристрою

Також для перевірки працездатності пристрою замість телефонної слухавки використано модульний мікрофон MAX9814, який спеціально спроектований для використання з мікроконтролерами Arduino, що дозволило не ускладнювати схему дослідного зразка додатковими АЦП тощо.

Проектування та перевірка працездатності проводилась у САПР Proteus, будова електричного кола та взаємозв'язки усіх складових компонентів показана на рис. 6.

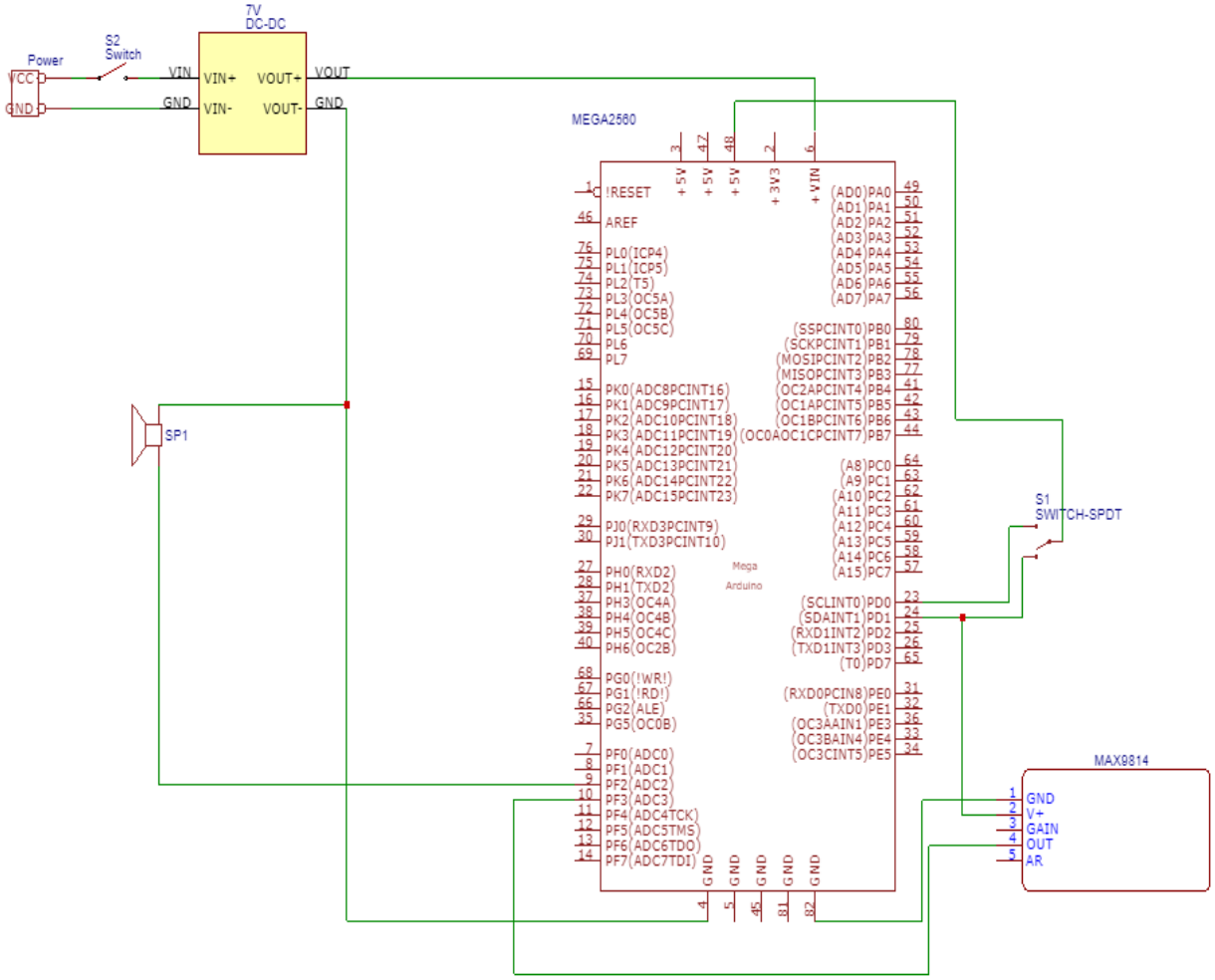

Рис. 6. Електрична схема розробленого пристрою

Насамперед для перевірки коректності роботи пристрою проаналізовано спектри оригінального інформаційного та отриманого скрембльованого сигналів. У випадку правильної роботи програмного коду, отриманий сигнал має бути змінений у частотно-часовій області, а отже його спектр має містити значні відмінності саме у частотно-часових характеристиках. Отриманні спектри оригінального та скрембльованого сигналів показані на рис. 7, з якого видно, що процес скремблювання відбувається коректно. У разі подачі отриманого сигналу на динамік підтверджується його нерозбірливість, що унеможливлює для несанкціонованого користувача розуміння якоїсь частини сигналу.

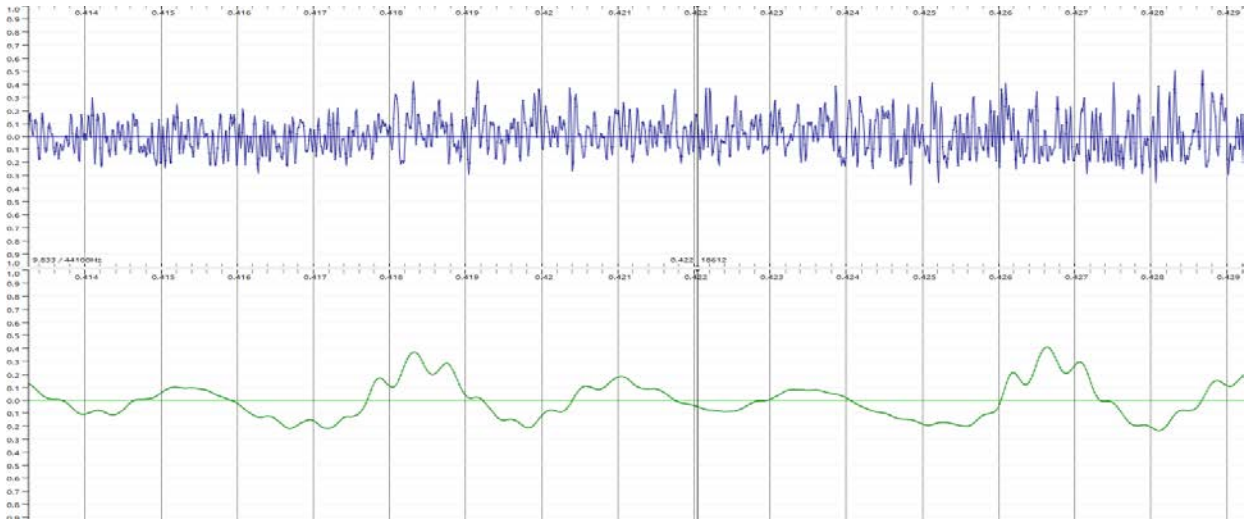

Рис. 7. Порівняння спектрів сигналів

Також перевірено режим роботи пристрою, коли обидва учасника розмови є санкціонованими. Порівнявши спектри сигналів санкціонованих користувачів, підсумовано про їх ідентичність, а подача сигналу на динамік підтвердила цей висновок. Отже, отриманий сигнал може бути повністю відтворений до початкового стану санкціонованим користувачем системи зв'язку. Таким чином ефективність скремблювання перевірена як звучанням отриманого сигналу, так і проведеним спектральним аналізом.

До того ж, проведено порівняння затримки роботи у разі використання методів-аналогів із розробленим. У результаті чого можна підсумовано, що, незважаючи на використання латинських квадратів та поєднання операцій перестановки і XOR, розроблений алгоритм не вносить значних затримок у канал зв'язку.

Висновки

Запропоновано пристрій для забезпечення захисту мовної інформації, яка передається через лінії аналогового телефонного зв'язку від несанкціонованого перехоплення на основі скремблера зі змінною коефіцієнтів вейвлет-перетворень відповідно до латинського квадрату.

Розроблено апаратний скремблер, який є основою для програмно реалізованого алгоритму скремблювання на основі велет-перетворень, що дозволяє підвищити захищеність за рахунок виконання двох етапів обробки коефіцієнтів вейвлет-перетворень. На першому етапі виконується операція перестановки відповідно до ключа на основі латинських квадратів, а на другому — виконується операція XOR отриманих коефіцієнтів з визначеним сеансовим ключем. Цей метод дозволяє усунути недоліки стандартних скремблерів такі як: значні затримки в процесі передавання сигналу, зменшення якості сигналу та варіативності ключів. Реалізація на платформі Arduino Pro Mini дала можливість зменшити габаритні розміри пристрою.

Відповідно до отриманих результатів перевірки функціонування розробленого пристрою, підтверджено коректність роботи апаратної і програмної частини розробки. Отриманий сигнал після скремблювання перевірено спектральними та статистичними тестами. Визначені коефіцієнти кореляції підтверджують ефективність розробленого пристрою. Виконавши порівняння швидкості роботи цього пристрою з аналогами, встановлено відсутність у каналі зв'язку значних затримок. Таким чином, розроблений засіб дозволяє підвищити захищеність сигналу в процесі передавання аналоговою системою зв'язку, не створюючи при цьому значних затримок у каналі зв'язку.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] В. О. Хорошко, В. С. Чередниченко, і М. Є. Шелест, *Основи інформаційної безпеки*, В. О. Хорошко, Ред. Київ, Україна: ДУІКТ, 2008,186 с.

[2] С. О. Іванченко, та ін., *Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації*, навч. посіб. Київ, Україна: НТУУ «КПІ», 2016, 104 с. [Електронний ресурс] Режим доступу: https://ela.kpi.ua/handle/1234_5б789/15155 .

[3] С. Е. Остапов, С. П. Евсеев, і О. Г. Король, *Технології захисту інформації*, навч. посіб. Харків, Україна: вид-во ХНЕУ, 2013, 476 с.

[4] Г. Ф. Конахович, В. П. Климчук, С. М. Паук, В. Г. Потапов, і О. О. Горбунов, *Захист інформації в телекомунікаційних системах*, навч. посіб. Київ, Україна.: НАУ, 2009, 380 с.

[5] О. В. Рибальський, В. Г. Хахановський, і В. А. Кудінов, *Основи інформаційної безпеки та технічного захисту інформації*, посіб. для курсантів ВНЗ МВС України. Київ, Україна: вид-во Національної академії внутрішн. справ, 2012, 104 с.

[6] М. М. Проценко, «Методика вибору вейвлет-функції для обробки цифрових сигналів,» *Вісник ЖДТУ*, № 49, с. 97-100, 2009.

Рекомендована кафедрою менеджменту та безпеки інформаційних систем ВНТУ

Стаття надійшла до редакції 17.04.2023

Карпінець Василь Васильович — канд. техн. наук, доцент, завідувач кафедри менеджменту та безпеки інформаційних систем, e-mail: karpinets@gmail.com ;

Катаєв Віталій Сергійович — асистент кафедри менеджменту та безпеки інформаційних систем, інженер Центру інформаційних технологій і захисту інформації, e-mail: kataev@vntu.net ;

Павловський Павло Валерійович — асистент кафедри менеджменту та безпеки інформаційних систем, інженер Центру інформаційних технологій і захисту інформації, e-mail: prepod@vntu.net ;

Гереш Денис Юрійович — студент факультету менеджменту та інформаційної безпеки.

Вінницький національний технічний університет, Вінниця

V. V. Karpinets[1]
V. S. Kataiev[1]
P. V. Pavlovskii[1]
D. Yu. Geresh[1]

Device of Protection of Analog Telephone Communication Based on Scrambler with Change of Wavelet Conversion Coefficients

[1]Vinnitsa National Technical University

The paper proposes a device for providing protection of speech information transmitted over an analog telephone line against unauthorized interception based on a scrambler with modified Latin square wavelet transform coefficients. The developed device consists of hardware and software parts, the hardware part is implemented on the microcontroller platform of the Arduino family, the software part of the device is implemented using the Proteus software environment. As the main part of the functions of the device is performed by a microcontroller, the general structure of the device comprises a microphone, a power supply and an Arduino board. Taking into account the results of the research, it is proposed to modernize the scrambling algorithm by performing permutation operations, matching XOR to the scrambler key, which displays the Latin square itself. A statistical and spectral analysis of the improved method was carried out and a comparison of the execution speed of scrambling algorithms was performed. To improve the security, it was proposed to carry out several stages of permutations of the received coefficients of wavelet transformations. Increasing the variability of the permutations of the wavelet transformation coefficients made it possible to increase the time spent by the attacker on going through all possible combinations. And taking into account that the permutation does not take place in one part of the signal, but in a set of n parts, this in its turn further complicates the procedure of sorting through all possible options. The implementation of the elements of this device with the help of electronic computing equipment and available components makes it an accessible, as well as an effective tool for solving technical information protection tasks, which can ensure the improvement of information protection systems at various business entities.

Keywords: technical information protection, information transmission systems, scrambler, acoustics, acoustic information.

Karpinets Vasyl V. — Cand. Sc. (Eng.), Associated Professor, Head of the Chair of Management and Security of Information Systems, e-mail: karpinets@gmail.com ;

Kataiev Vitalii S. — Assistant of the Chair of Management and Security of Information Systems, engineer of the Center of Information Technologies and Information Security, e-mail: kataev@vntu.net ;

Pavlovskii Pavlo V. — Assistant of the Chair of Management and Security of Information Systems, engineer of the Center of Information Technologies and Information Security, e-mail: prepod@vntu.net ;

Geresh Denys Yu. — Student of the Department of Management and Information Security