УДК 004.891

к.т.н., доц. **Муляр І.В.** (ХмНУ)
к.т.н. **Лєнков Є.С.** (ВІТІ)
Солодєєва Л.В. (ВІКНУ)

ШИФРУВАННЯ ЗВУКУ МЕТОДОМ ПРЕДСТАВЛЕННЯ ЙОГО У ВИГЛЯДІ СПЕКТРОГРАМИ

У статті представлений метод шифрування аудіо файлу у вигляді спектрограми. Це дозволить зберегти необхідні аудіо дані від зловмисників. Цей метод шифрування аудіофайлів дозволяє зашифровувати спектрограму самого звуку та передавати її по мережі з наступним відтворенням цього звуку Найкраще, цей метод шифрування, покаже себе при шифруванні розмов по ір-телефонії, між невеликою кількістю комп'ютерів, наприклад у невеликій корпоративній мережі.

Використовуючи бібліотеки для створення спектрограми та змінюючи їх під себе ми можемо отримати функції створення спектрограми такі як нам потрібно. Так як це окремі функції для створення та виведення інформації, їх легко можна використовувати в інших програмних продуктах.

Ключові слова: аудіофайл, спектрограма, звукова хвиля, віконні перетворення Фур'є.

Вступ. Задача шифрування файлів та наступне збереження їх чи передача по мережі, являється зараз важливою частиною існування комп'ютерної мережі. І не важливо чи ми просто зберігаємо наші дані на комп'ютері, чи хочемо безпечно їх передати комусь, потрібен хороший спосіб, що забезпечить достатній рівень безпеки для цих дій.

Системи зв'язку часто розглядаються як можливі проблемні засоби передачі даних, навіть якщо вони захищені певними системами захисту. Системи шифрування звуку, голосу, використовуються для забезпечення безпеки end-to-end. Тобто, для захисту в режимі реального часу в таких системах як GSM, VoIP та інші.

Принципи цифрового представлення звуку загалом досить прості:

- спочатку перетворюємо аналоговий сигнал в цифровий, це робить пристрій – аналогово-цифровий перетворювач (АЦП);
- зберігаємо отримані цифрові данні на носій;
- якщо нам потрібно відтворити отриманий файл, то для цього проводиться зворотне перетворення з цифрового в аналоговий звук за допомогою цифро-аналогового перетворювача (ЦАП).

Від того як часто програмно ми будемо зчитувати ці вибірки, так як ми їх будемо редагувати, залежить те на скільки якісний буде звук при оцифровуванні. Формат представлення звукових даних залежить від способу квантування АЦП, ну і формат самого файлу зі звуком залежить від структури та особливостей записаних аудіо даних. Виділяють загалом три групи аудіо форматів:

- аудіоформати без стиснення (WAV, AIFF)
- аудіоформати з стисненням без втрат (APE, FLAC)
- аудіоформати з стисненням з втратами (mp3)

Це є найпоширеніші аудіо формати.

В сучасному світі, аудіо файли використовуються у багатьох сферах діяльності людей. Це не лише записи пісень, а і записи телефонних розмов (при широкому поширенню IP-телефонії в наш час) чи особисті голосові записи. І за різних причин ми можемо не бажати щоб ці записи потрапили у чужі руки. Для цього можна проводити шифрування самих аудіо файлів.

По-перше нам потрібно знайти спосіб зашифрувати необхідні файли від зловмисників. Чи то при передачі цього файлу чи навіть просто при зберіганні.

По-друге, цей спосіб повинен бути зручним і надійним.

По-третє, використання цього способу не повинно нашкодити нашим даним.

На сьогодні існує три види шифраторів: апаратні, програмно-апаратні та програмні. Найдорожчі з них це апаратні, де для шифрування потоку аудіо нам потрібно додаткове

апаратне забезпечення, яке буде шифрувати аналогові хвилі і далі вже передавати це по мережі. Далі йдуть програмно-апаратні, і самі дешеві це програмні шифратори [1].

Постановка задачі. Загалом, основною метою є використання такого методу для шифрування, що може швидко працювати, достатньо якісно захищати звук від зловмисників, та не шкодити нашим даним. Використання апаратних шифраторів для «домашнього» використання, є дуже дорогим засобом. Використання їх для телефонії, також є дорогим та незручним методом. Тому розробляються нові програмні засоби, що вбудовуються в операційні системи, або використовуються як окремі програми.

На програмному рівні є варіанти шифрування даних під час передачі по мережі. Наприклад SRTP (Secure Real-Time Transport Protocol) – безпечний протокол передачі даних в реальному часі призначений для шифрування в однонаправлених та багатонаправлених передачах медіа та програм [2]. Це окремий протокол для мережі, шифрування в ньому проводиться за допомогою AES шифру що може працювати в двох режимах, що перетворюють початково блочний шифр AES в потоковий шифр. Недоліком цього методу є те, що працює він лише для передачі в реальному часі даних, немає можливості зберегти передані аудіо дані в зашифрованому вигляді якщо потрібно їх буде передати/перенести на інших носій.

Звісно завжди залишається варіант звичайного шифрування аудіофайлу, де ми поблоково можемо шифрувати частини даних будь-яким шифром що нам потрібно, але така методика також не допоможе зберегти проміжні результати шифрування для майбутнього їх відтворення з іншого носія або зручного перенесення.

Реалізувати зручний спосіб шифрування вхідного аудіопотоку, чи шифрування вже збереженого файлу можна за допомогою представлення цього звуку у вигляді зображення. Зображення і буде проміжним результатом при передачі від клієнта до клієнта, чи перенесенні з одного носія на інший. І навіть при зломі цього проміжного результату, буде важко відтворити аудіофайл без ключів.

Метою дослідження є створення методу шифрування аудіофайлів способом представлення їх у вигляді зображення спектрограми

Таким чином, актуальною є задача розробки нових ефективного методу та алгоритмів шифрування способом представлення аудіо в вигляді зображень, що дозволить швидко шифрувати аудіодані, на основі вже існуючих методів роботи зі звуком

Виклад основного матеріалу досліджень.

Основні методи шифрування аудіофайлу, мають на меті оперування з характеристиками звуку. Для того щоб оперувати з отриманим цифровим звуком необхідно знати як його можна зберігати та відтворювати. Існує велика кількість як методів збереження, так і методів стиснення і зберігання звуку. Так як від представлення даних залежать усі наступні операції з цими даними. Буде розглянуте представлення звуку у вигляді спектрограми. З якою і будуть проводитися всі дії в процесі шифрування.

При вирішенні задачі перетворення звуку а спектрограму, використовується віконне перетворення Фур'є. Спектрограма – це двовимірний графік, де на горизонтальній осі йде представлення часу, на вертикальній – частота. Третій вимір – амплітуда, представлена інтенсивністю або кольором кожної точки в зображенні [1]. Спектрограми зазвичай створюються одним з двох способів: апроксимуються, як набір фільтрів, отриманих з серії смугових фільтрів, або розраховуються по сигналу часу, використовуючи віконні перетворення Фур'є. Для цифрової обробки, зазвичай, використовуються саме віконні перетворення Фур'є (відмінність віконного перетворення від звичайного перетворення Фур'є полягає в тому, що віконне перетворення є функцією від часу, частоти та амплітуди, в той час як звичайне перетворення є функцією лише від частоти, що не дозволяє визначати час в який ми фіксуємо ту чи іншу частоту звуку), що визначаються наступним чином:

$$F(t,\omega)=\int_{-\infty}^{\infty} f(\tau)W(\tau-t)e^{-i\omega t}d\tau \qquad (1)$$

де $W(\tau-t)$ – деяка віконна функція.

Виконується цифрова вибірка даних в деякій часовій області. Сигнал розбивається на частини, які, як правило, перекриваються, а після цього проводиться перетворення Фур'є, для того щоб розрахувати величину частотного спектру для кожної частини. Ці частини відповідають вертикальній лінії на зображенні – значення амплітуди в залежності від частоти в кожний момент часу [3].

Суть віконного перетворення полягає в тому, що ми наш звук розбиваємо на частини – вибірки, після чого до цих вибірок застосовується перетворення Фур'є і, після перетворення ці частини разом утворюють повну спектрограму.

Зазвичай використовуються різні віконні функції: вікно Ханна, Хемінга, вікно Блекмана та інші.

Візьмемо вікно Ханна. Воно характеризується наступною формулою:

$$W(n)=0{,}5*\left(1-\cos\left(\frac{2\pi n}{N-1}\right)\right), \qquad (2)$$

де $N-1$ – вибірка. На рис. 1 представлений загальний вигляд вікна Ханна.

Рис. 1. Вікно Ханна

Перевагою вікна Ханна є дуже низький рівень, так званого, аліасингу. Це явище накладання або нечіткості різних безперервних сигналів. Наприклад накладання високих частот на низькі в результаті чого сигнал спотворюється. Якщо вікно Ханна використовується в якості вибірки сигналу, для перетворення Фур'є, то при зворотному перетворенні в нас буде утворюватися мінімальна кількість спотворень.

Після застосування до обраної вибірки перетворення Фур'є, у нас вийде зображення що показано на рис. 2.

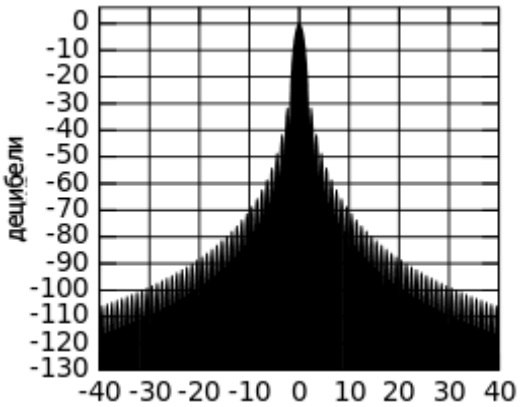

Рис. 2. Вибірка, з перетворенням Фур'є

Отже ми маємо аудіо файл. За допомогою перетворень Фур'є, звуковий потік представляємо у вигляді спектрограми. Під час перетворення, після обчислення віконної функції, змінюватимемо значення цієї функції на певну величину – Z. Цю величину можна зберігати різноманітними стеганографічними способами. Наприклад, значення цієї величини буде окремо зберігатися і передаватися разом із зображенням, а саме вбудовуватиметься в зображення шляхом поміщення цієї величини в молодші біти зображення. Таким чином при розшифровуванні зображення ми спочатку зчитуємо перші молодші біти зображення, отримуємо необхідне число, після цього відбуватиметься декодування спектрограми назад у звук.

Потрібно зазначити, що при застосуванні шифрування до аудіопотоку, наприклад в системі передачі цифрового звуку, сам потік буде розділятися на блоки. Певна частина звуку буде записуватися в буфер, потім до цієї частини буде застосоване шифрування, і вже після цього, зашифроване повідомлення буде відправлене до отримувача. Зі сторони отримувача знову ж таки буде так саме. Спочатку розшифровується частина звукозапису – прийнятий буфер, після цього розшифроване повідомлення поступає на аудіовихід до користувача. Для забезпечення вищого рівня надійності, до кожного блоку відправленого в потоці, можна застосовувати різну величину числа Z. І в разі, якщо зловмисник отримує одну частину блока з відомим йому одним секретним числом, то іншу частину він не зможе розшифрувати.

На рисунку 3 приведена схема для шифрування окремого файлу.

Видно, що на вхід подається аудіофайл, і над ним відразу ж застосовується метод шифрування. Спочатку застосовуємо віконне перетворення Фур'є. Отримані значення функції ми перетворюємо, домножуючи на певну величину Z. Вона може задаватися як користувачем, так і статично або випадковим чином у самій програмі шифрування.

Після побудови спектрограми ми стеганографуємо цю величину Z. Для цього методу я вирішив використати метод стеганографування LSB (Least Significant Bit) [2]. Суть цього методу заключається в тому, що в більшості випадків, людина не може помітити зміну в останньому біті кольорових компонентів зображення. Фактично LSB це шум, тому його можна використовувати для вбудови інформації шляхом заміни найменш значущих бітів пікселів зображення секретним повідомленням.

В нашому випадку необхідно записати отриману величину на яку буде змінюватися отримана віконна функція. Згідно цього методу, найменш значущі біти заміняються під час кодування зображення у формат для збереження. Під час формування JPG або BMP формату, ми помістимо в перші пікселі зображення наше секретне число.

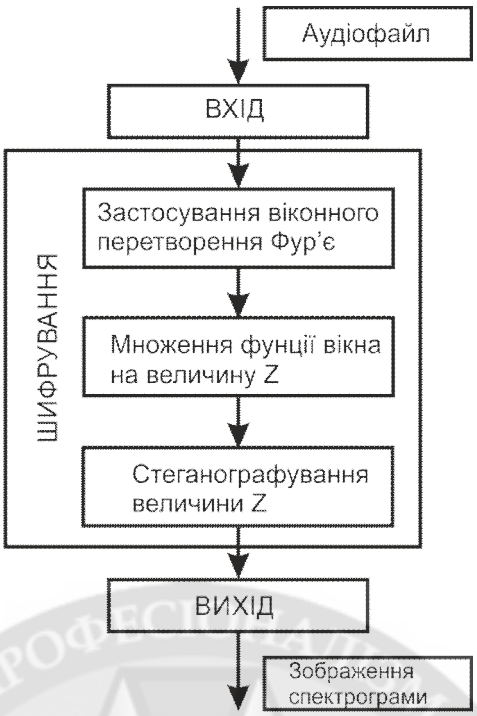

Рис. 3. Застосування методу для готового файлу

Для шифрування одного готово файлу, робота методу зрозуміла. Для потокової передачі, метод ускладняється тим, що нам потрібно ділити потік не блоки, до яких ми будемо застосовувати шифрування. Від розміру шифрованих блоків буде залежати швидкодія та величина затримок при передачі голосового повідомлення. Якщо голосове повідомлення просто записується і відразу ж шифрується то розмір блоків можна використовувати великий, так як зашифроване повідомлення не буде передане відразу ж для розшифровки. Якщо це буде потік відразу ж до клієнта, де необхідна буде розшифровка повідомлення, то чим менший розмір блоку буде, тим краще.

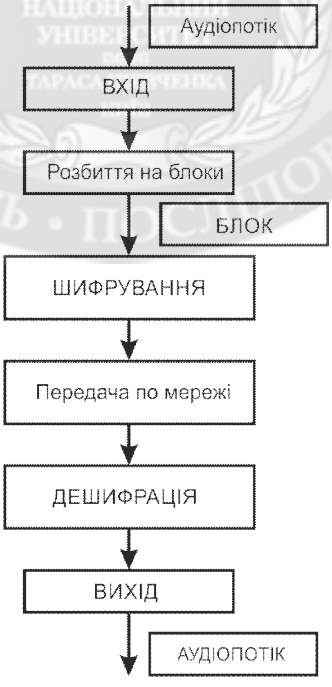

Рис. 4. Застосування методу до аудіопотоку

Як видно з рис. 4, на вході та на виході ми маємо аудіопотік. Зображення спектрограми використовується саме для передачі по мережі. Відразу ж, в процесі отримання цифрового сигналу, ми його розділяємо на блоки, про які вказувалось вище, і відправляємо зашифровані блоки отримувачу. Зі сторони отримувача проходить дешифрація отриманого блоку, і передача розшифрованого аудіо далі з наступним її відтворенням.

Процес шифрування заключається в зчитуванні оцифрованих параметрів звуку і застосуванні до них віконного перетворення Фур'є. В залежності від обраного вікна, ми отримаємо різні варіанти спектрограми. Для роботи методу не є важливим яке саме вікно буде використовуватися, але для збереження якості сигналу краще використати вікно Ханна. Як було сказано в попередньому розділі, перевагою цього вікна є те, що при зворотньому перетворенні, в нас буде утворюватися мінімальна кількість шумів. Візьмемо тестовий звуковий файл. На рис. 5 показана спектрограма з програмного продукту Audacity. Це є безкоштовна програма для редагування звуку.

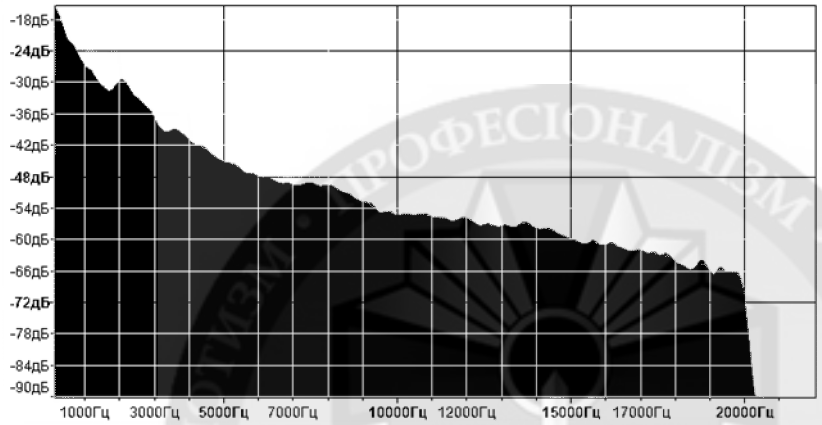

Рис. 5. Спектрограма тестового звукового файлу

В налаштуваннях відображення було вказано використовувати вікно Ханна. Це є звичайне нешифроване зображення в самому загальному способу відображення.

Після застосування шифрування, зображення набуде вигляду подібного до наступного рис. 6.

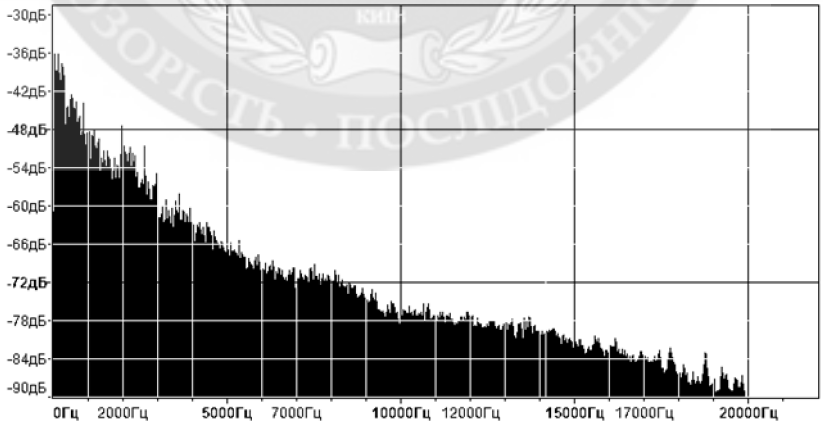

Рис. 6. Зображення подібне до зашифрованої спектрограми

Відповідно, що в готовому програмному продукті ми не можемо змінювати процес створення самої спектрограми. Тому метод буде написаний з використанням мови програмування С. При шифруванні цього ж самого тестового аудіофайлу, ми отримаємо наступне зображення спектрограми, показане на рис. 7.

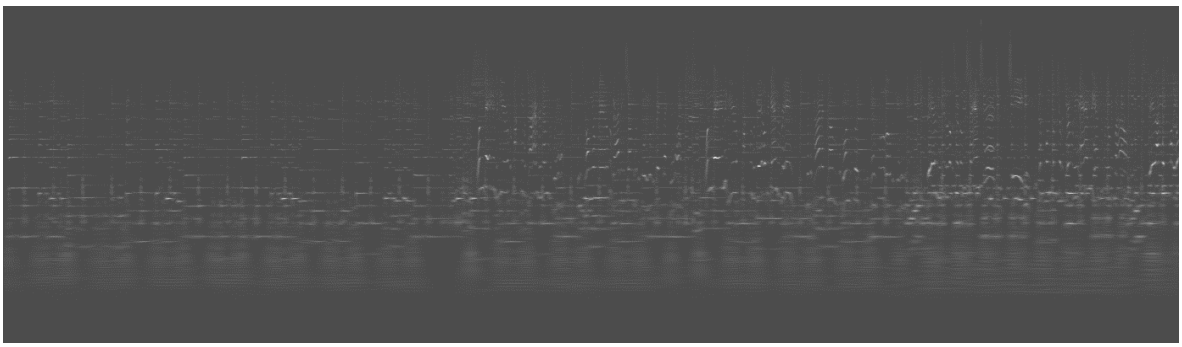

Рис. 7. Спектрограма тестового звуку

Відмінність між виглядом спектрограми отриманої за допомогою програми Audacity та програмою на мові С викликана тим, що я використав інший тип відображення, подібний до того, як відображаються спектрограми в аналогових спектрографах. Саме таким чином ми бачимо повне розподілення по часу наших віконних вибірок. Так як в програмі Audacity відображення йде в двовимірному просторі і не показує часової розділеності.

В програмному продукті Matlab також є можливість створювання спектрограми.

Реалізація приведена на мові програмування С. Все зображення в нас являється масивом бітів. Побудова спектрограми по суті являється створенням цього масиву бітів, завантажуючи в комірки масивів колір що відповідає амплітуді.

```
for (i=0; i<Mo; i++)
  {
        pos_in = (double) i * ratio;
        coef_sum = 0;
        for (j=roundup(pos_in - ratio); j<=pos_in + ratio; j++)
        {if (j>=0 && j<Mi)
              {     x = j - pos_in + ratio;
                    coef = 0.42 - 0.5*cos(pi * x * ratio_i) + 0.08*cos(2*pi * x * ratio_i);
                    coef_sum += coef;
                    out[i] += in[j] * coef;
              }} out[i] /= coef_sum;}
  return out;
```

Так розраховується позиція оригінального сигналу pos_in. В вихідному масиві out ми будемо мати позиції бітів у вихідному файлі. Визначаючи позиції, ми вже можемо змінювати вихідну величину що буде отримана за допомогою цієї функції. Наприклад:

```
out[i] /= coef_sum;
out[i]*=INDEX.
```

Значення індексу ми запам’ятовуємо на початку створення вікна. Це може бути як статично задана змінна, так і динамічно змінювана змінна. Після цього застосовуємо метод малювання зображення.

Після цього як ми створимо весь масив на виході ми отримаємо вигляд спектрограми зображення подібний до рис. 7. Під час зміни отриманого розміщення значення амплітуди зображення міняється, розташування точок змінюється, що не дає без знання величини індексу розшифрувати саме початкове повідомлення.

Одним із способів використаних для передачі та збереження цього індексу значення, було стеганографування його в саме зображення спектрограми. Загалом використовується

стандартний алгоритм створення JPG зображень. І вже, під час створення зображення, в алгоритмі і буде відбуватися вбудовування індексу.

Висновки. Отже в роботі представлено метод шифрування аудіофайлу. Провівши теоретичні обрахунки для методу, було визначено, що затрати часу на шифрування файлу розміром 10 МБ, а власне пісня, тривалістю 5 хвилин, становлять 5 секунд. Це при використанні для створенні спектрограму стандартних значень амплітуди та частоти. При зміні характеристик звуку для створення спектрограми, час на створення спектрограми зменшується, але разом і з цим втрачаються звукові данні, так як при створенні спектрограми відкидаються деякі елементи звукового потоку. Але, як тільки шо було вказано, при використанні стандартних звукових параметрів для шифрованої пісні, швидкість шифрування становить 1:60, що є досить непоганим результатом та дозволяє використовувати метод на рівні з більшістю існуючих методів шифрування. При потоковому шифруванні, звісно необхідно враховувати, що має витрачатися час як на шифрування так і на дешифрування, але при потоковій передачі, і більшості випадків це йде голосе повідомлення, де ми можемо зменшувати частоту повідомлення, що пришвидшить набагато час створення спектрограми та шифрування її. Представлений метод шифрування аудіо файлу у вигляді спектрограми дозволить зберегти необхідні аудіо дані від зловмисників. Найкраще, цей метод шифрування, покаже себе при шифруванні розмов по ip-телефонії, між невеликою кількістю комп'ютерів, наприклад у невеликій корпоративній мережі.

Використовуючи бібліотеки для створення спектрограми та змінюючи їх під себе ми можемо отримати функції створення спектрограми такі як нам потрібно. Так як це окремі функції для створення та виведення інформації, їх легко можна використовувати в інших програмних продуктах.

ЛІТЕРАТУРА:

1. Радзишевский А.Ю. Основы аналогового и цифрового звука / А.Ю. Радзишевский – М.: Вильямс, 2006. – 288с.

2. Крюков Ю.С. Безопасность VoIP-контента / Ю.С. Крюков // Защита информации. INSIDE. – 2008. - №3. – С.83-84.

3. Кирилюк І.О. Адаптивний метод шифрування аудіофайлів способом представлення їх у вигляді зображень / Ю.В. Хмельницький, І.О. Кирилюк // Зб. наук. праць Військового інституту Київського НУ ім. Тараса Шевченко. – К.: ВІКНУ, 2014. – Вип. № 46 . – С.81

REFERENCES:

1. Radzishevskiy A.Y. Fundaments of analog and digital sound / A.Y. Radzishevskiy – Moskow.: Williams, 2006. – 288p.

2. Kriukov Y.S. VoIP content security / Y.S. Kriukov // Information security. INSIDE. – 2008. - №3. – S.83-84.

3. Kirilyuk I.O. Adaptivniy metod shifruvannya audIofaylIv sposobom predstavlennya Yih u viglyadI zobrazhen / Yu.V. Hmelnitskiy, I.O. Kirilyuk // Zb. nauk. prats Viyskovogo Institutu Kiyivskogo NU Im. Tarasa Shevchenko. – K.: VIKNU, 2014. – Vip. # 46 . – S.81

Рецензент: д.т.н., проф. Сбітнєв А.І., провідний науковий співробітник науково-дослідного центру Військового інституту Київського національного університету імені Тараса Шевченка

к.т.н. Муляр И.В., к.т.н. Ленков Е.С., Солодеева Л.В.

ШИФРОВАНИЯ ЗВУКА МЕТОДОМ ПРЕДСТАВЛЕНИЯ ЕГО В ВИДЕ СПЕКТРОГРАММЫ

В статье представлен метод шифрования аудио файла в виде спектрограммы. Это позволит сохранить необходимые аудио данные от злоумышленников. Этот метод шифрования аудиофайлов позволяет зашифровывать спектрограму самого звука и передавать ее по сети с последующим воспроизведением этого звука Лучше всего, этот метод шифрования, покажет себя при шифровании разговоров по ip-телефонии, между небольшим количеством компьютеров, например в небольшой корпоративной сети.

Используя библиотеки для создания спектрограммы и изменяя их под себя мы можем получить функции создания спектрограммы такие как нам нужно. Так как это отдельные функции для создания и вывода информации, их легко можно использовать в других программных продуктах.

Ключевые слова: аудиофайл, спектрограмма, звуковая волна, оконные преобразования Фурье.

Ph.D. Muliar I.V., Ph.D. Lenkov Y.S., Solodeeva L.V.

ENCRYPTION OF A SOUND BY ITS PRESENTATION IN THE FORM OF A SPECTROGRAM

The article presents a method to encrypt audio file in the form of a spectrogram. This will keep the necessary audio data from intruders. This method of encryption allows you to encrypt audio files to spectrogram the sound and transmit it over the network with the subsequent playback of that sound Best of all, this method of encryption, on the encryption of calls on ip telephony, between a small number of computers, for example in smaller corporate networks.

Using the library to create spectrograms and by changing them we can get the make spectrograms such as we need. As this is a separate function to create and display information, they can easily be used in other software products.

Keywords: audio, spectrogram, sound wave, short-time Fourier transform.