БЕЗПЕКА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ

ОЦІНКА ЯКОСТІ ВІДНОВЛЕННЯ МОВИ В ЗАХИЩЕНИХ БЕЗПРОВОДОВИХ КАНАЛАХ ЗВ'ЯЗКУ

Георгій Конахович, Юлія Беженар, Олексій Голубничий, Роман Одарченко

Національний авіаційний університет

КОНАХОВИЧ Георгій Філімонович, д.т.н., професор

Рік та місце народження: 1944 рік, м. Васильків, Київська область, Україна.
Освіта: Київський інститут інженерів цивільної авіації (з 2000 року – Національний авіаційний університет), 1968 рік.
*Посада:*доктор технічних наук, професор, завідувач кафедри телекомунікаційних систем з 2003 року.
Наукові інтереси: захист інформації телекомунікаційних систем, ефективність телекомунікаційних систем
Публікації: більше 150 наукових публікацій, серед яких монографії, словники, підручники, навчальні посібники, наукові статті, 18 винаходів.
E-mail: tks@nau.edu.ua

ГОЛУБНИЧИЙ Олексій Георгійович, к.т.н.

Рік та місце народження: 1983 рік, м. Київ, Україна.
Освіта: вища.
Посада: доцент кафедри телекомунікаційних систем.
Наукові інтереси: спеціальні телекомунікаційні системи.
Публікації: більше 30 наукових та навчально-методичних праць.
E-mail: dept265@yandex.ru

ОДАРЧЕНКО Роман Сергійович

Рік та місце народження: 1988 рік, с. Култук, Слюдянський р-н, Іркутська область, РФ.
Освіта: Національний авіаційний університет, 2010 рік.
Посада: аспірант.
Наукові інтереси: захист інформації в телекомунікаційних системах.
Публікації: 15 наукових публікацій.
E-mail: odarchenko.r.s@mail.ru

БЕЖЕНАР Юлія Вікторівна

Рік та місце народження: 1990 рік, м.Вінниця, Україна.
Освіта: Національний авіаційний університет, 2012 рік.
Посада: студент.
Наукові інтереси: якість відновлення мови в захищених телекомунікаційних каналах зв'язку.
Публікації: 5 наукових публікацій.
E-mail: el1ce@mail.ru

Анотація. *У даній статті розглянуто додаткову затримку, що вноситься в мережу при використанні засобів захисту інформації та розроблено модель передачі мовного повідомлення по захищеному безпроводовому каналу зв'язку і проаналізовано його якість відновлення. Основні положення статті реалізовані у вигляді розрахункової моделі, яку можна використовувати для проектування безпроводових захищених систем.*

Ключові слова: *мовне повідомлення, додаткова затримка, шифрування (AES), безпроводовий канал зв'язку, BER, якість відновлення.*

Постановка проблеми

В даний час важлива роль відводиться методам дослідження якості відновлення мови в цифрових безпроводових телекомунікаційних системах. Особливістю зазначених методів є, так званий, людський фактор, оскільки людина аналізує мовну інформацію за допомогою органів чуття, які складно змоделювати. Традиційно для оцінки якості мовної інформації використовуються так звані "експертні" або "суб'єктивні" оцінки якості мови. Відповідно такі процедури є дорогими, тривалими і складними в організації, тому необхідно розробляти рішення, що забезпечать об'єктивну (автоматизовану) оцінку якості мови.

Аналіз досліджень і публікацій

Дослідження в області обробки, передачі і оцінювання мовної інформації проводяться вітчизняними науковцями Інституту кібернетики ім. В.М. Глушкова, ХАІ, НТУУ КПІ та ін. Серед закордонних науково-дослідних організацій необхідно виділити робочі групи МСЕ, а саме її сектор МСЕ-Т. Провідними закордонними закладами, де проводяться дослідження по обробці і оцінюванню МС, є: СПбГУТ, СибГУТИ, Univevsity of Sheffield, Cambridge University. Значний внесок у наукові досягнення в області обробки та оцінки якості МС внесли: Дж. М. Уайт, С. Я. Левінсон, Л. Р. Рабінер, Ф. Ітакура, А. І. Розенберг, А. Х. Грей, Т. К. Вінцюк, та ін. ***Метою*** дослідження є аналіз додаткової затримки пакета, що вноситься при включенні в мережу засобів захисту (в даній роботі – це час витрачений на зашифрування/розшифрування пакета) та розробка моделі оцінки якості відновлення МП при їх передачі по захищених безпроводових КЗ.

Основна частина дослідження

Якість передавання інформації оцінюють достовірністю приймання повідомлень, яка характеризує відповідність прийнятого і переданого повідомлень. Можлива відмінність між цими повідомленнями пов'язана із впливом завад і спотворень у КЗ. Спотворення в КЗ можна компенсувати, до того ж вони у більшості випадків є досить малими. Тому головною причиною зменшення достовірності є завади.

Для додатків, де не важливий порядок та інтервал приходу пакетів, наприклад, e-mail, час затримок між окремими пакетами не має вирішального значення. Передача МП є однією з областей передачі даних, де важлива динаміка передачі сигналу.

Одними із факторів, що впливають на якість пакетної пакетної передачі мови є фактори якості мережі, що включають: максимальну пропускну здатність, затримки, джиттер, втрату пакетів та ін. Втрачені пакети порушують якість мови і створюють спотворення тембру. Передбачається, що втрата до 5% пакетів непомітна, а понад 10-15% – недопустима. Причому дані величини істотно залежать від алгоритмів компресії та декомпресії.

До критеріїв, що впливають на якість відновлення МП, можна віднести:

Відношення сигнал/шум (SNR) – загальноприйнятий спосіб вираження якості сигналу в системі. Чим більше SNR, тим менший вплив завади на сигнал.

Параметр BER – це величина, яка чисельно характеризує вплив завад на певну СЗ. Чим менше його величина, тим краще працює система і тим менше вона сприйнятлива до дії зовнішніх завад. Основними чинниками, які впливають на BER є: рівень шуму в КЗ, код передачі інформації і його параметри та вибраний тип модуляції.

Шум квантування – це завади, що виникають при перетворенні цифрового аудіосигналу в аналоговий. Шум квантування не пов'язаний із перешкодами в КЗ і повністю визначається вибором числа рівнів квантування.

Безпека роботи в мережі, а тим більше безпека особистих даних користувача завжди була і буде тим питанням, якому приділяється підвищена увага. Навіть незважаючи на те, що різні дані представляють різну цінність, вони в будь-якому випадку повинні бути захищені від крадіжки і використання без відома користувача. Захист даних за допомогою шифрування – одне з можливих рішень проблеми їхньої безпеки. Зашифровані дані стають доступними тільки для того, хто знає як їх розшифрувати, і тому їх викрадення є трудомістким й дорогим процесом для несанкціонованих користувачів.

Для шифрування повідомлень стандарт IEEE 802.16 передбачає використання алгоритму DES або алгоритму AES. На даний час DES вважається ненадійним в основному через малу довжину ключа (56 біт) та розмір блоку (64 біти), тому перевагу надають алгоритму AES. Високу надійність AES підтверджує астрономічними числами. 128-бітний ключ забезпечує 340 андеціліонів ($340 \cdot 10^{36}$) можливих комбінацій, а 256-бітний ключ збільшує це число до $11 \cdot 10^{76}$. Для порівняння: алгоритм DES дає загальне число комбінацій в $72 \cdot 10^{15}$. На їх перебір у спеціально побудованій машині "DES Cracker" йде кілька годин. Навіть якщо б вона робила це всього за одну секунду, то на перебір 128-бітного ключа машина витратила б 149 трильйонів років.

В ході дослідження розроблено програму, яка генерує ключ для алгоритму шифрування AES та зашифровує і розшифровує файл даним алгоритмом (див. рис. 1).

Мережа VoIP є критичною до часу затримки. Затримка в мережі VoIP розраховується за наступною формулою:

$$Z_{заг} = Z_{код} + Z_{інк} + Z_{чер} + Z_{пер} + Z_{мереж} + Z_{пер} + + Z_{розп} + Z_{декод},$$

де $Z_{заг}$ – загальна затримка; $Z_{код}$ – затримки, що вносяться алгоритмом кодування; $Z_{інк}$ – затримки, що вносяться інкапсуляцією пакетів; $Z_{чер}$ – затримки, що вносяться побудовою черги; $Z_{пер}$ – затримки, що вносяться передаванням; $Z_{мереж}$ – затримки, що вносяться мережею; $Z_{розп}$ – затримки, що вносяться розпакуванням пакету; $Z_{декод}$ – затримки, що вносяться алгоритмом декодування.

Для забезпечення прийнятної якості звуку на приймальній стороні при передачі мовних пакетів в IP-мережі затримка при їх доставці від приймальної сторони не повинна перевищувати 250 мс.

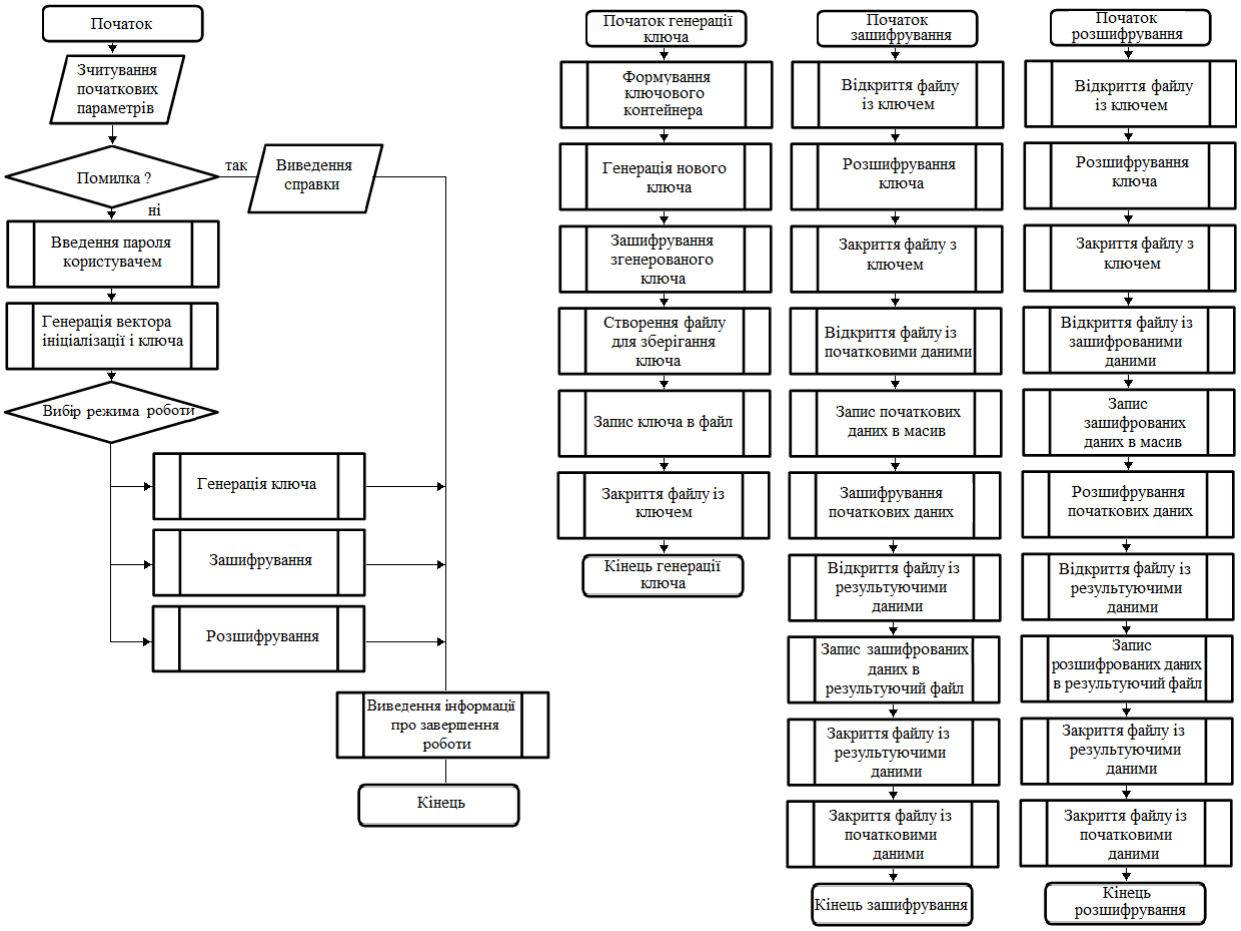

Рис. 1. Блок-схема алгоритму роботи програми

При включенні в мережу засобів захисту виникає додаткова затримка, яка дорівнює:

$$Z_{дод} = Z_{шифр} + Z_{дешиф},$$

де $Z_{дод}$ – додаткова затримка, що виникає при підключенні в мережу засобів захисту; $Z_{шифр}$ – затримки, що вносяться алгоритмом шифрування; $Z_{дешиф}$ – затримки, що вносяться алгоритмом дешифрування.

Використовуючи розроблену програму, знайдено додаткову затримку, яка вноситься при зашифруванні/розшифруванні пакета (див. рис. 2).

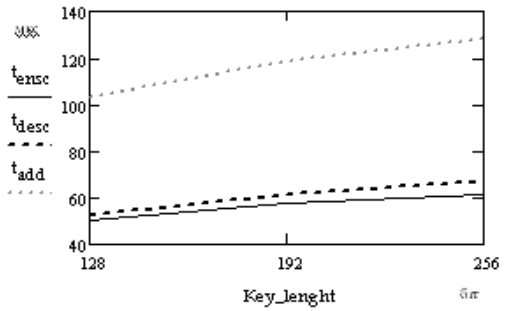

Рис. 2. Графік залежності часу зашифрування, розшифрування та додаткової затримки від довжини ключа

Як видно із графіка на рис. 2, час необхідний для зашифрування/розшифрування, а відповідно і додаткова затримка із збільшенням довжини ключа збільшуються. Оскільки алгоритм AES досі не зломаний, тому нерентабельно використовувати ключі довжиною 192 і 256 біт з огляду на те, що додаткова затримка при їх використанні більша, ніж у ключа 128 біт.

Всі криптографічні протоколи і протокол стиснення мовного потоку вибираються програмами динамічно і непомітно для користувача, надаючи йому природний інтерфейс, подібний звичайному телефону.

Реалізація ефективних криптографічних алгоритмів і забезпечення якості звуку вимагають значних обчислювальних ресурсів. В більшості випадків ці вимоги виконуються при використовуванні достатньо могутніх і продуктивних комп'ютерів, які, як правило, не уміщаються в корпусі телефонного апарату.

Але міжкомп'ютерний обмін мовною інформацією не завжди влаштовує користувачів. Набагато зручніше використовувати невеликий, а краще мобільний апарат. Такі апарати вже з'явилися, хоча вони забезпечують стійкість шифрування мовного потоку значно нижче, ніж комп'ютерні системи. За прогнозами експертів, майбутнє саме за такими телефонними апаратами: невеликими, мобільними, надійними, мають гарантовану стійкість захисту мовної інформації і високу якість звуку.

В процесі дослідження змодульовано передачу мовного повідомлення по безпроводовому
КЗ. Для цього записано мовне повідомлення в аудіофайл. За допогою вбудованої функції MathCad його

представлено вектором амлітудних відліків, який потім передено у вигляд вектора бітового потоку, що надалі використовувався для моделювання.

В стандарті IEEE 802.16 використовуються схеми модуляції BPSK, QPSK, QAM-16, QAM-64, оскільки вони є найбільш ефективними. В даній моделі здійснено передачу мовних повідомлень за допомогою даних схем модуляції.

На рис. 3 а) зображено частину змодульваного сигналу за допомогою QAM-16.

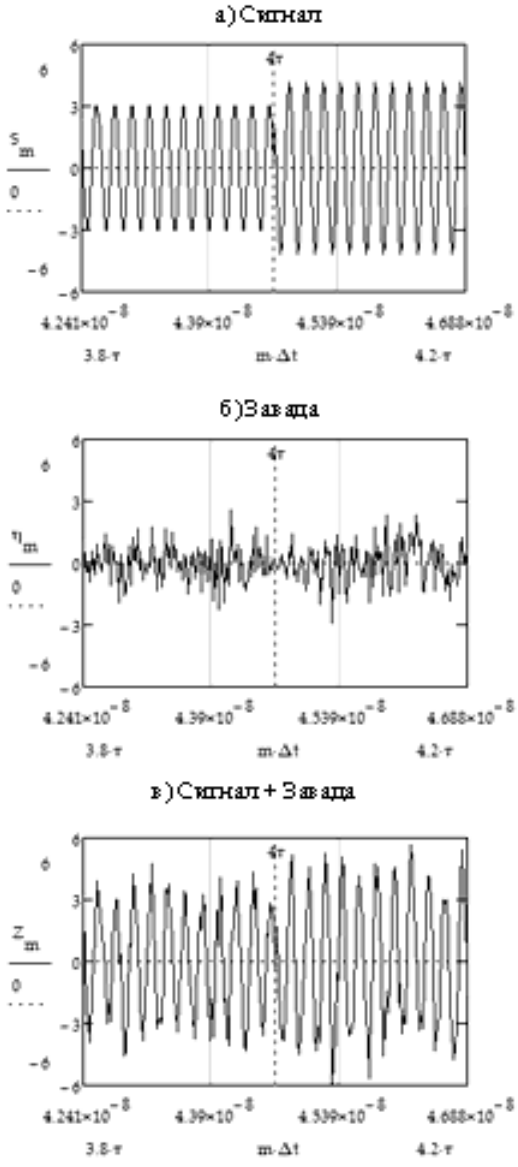

Рис. 3. Графік а) змодульованого сигналу;
б) завади в КЗ; в) С+З

В результаті моделювання було отримано оцінку ймовірності неправильної передачі біта (BER) по КЗ (див. рис. 4).

Із графіка видно, що найкраща якість відновлення повідомлення буде для модуляції BPSK, оскільки при однаковому значенні с/ш в каналі зв'язку при її використанні параметр BER – найменший.

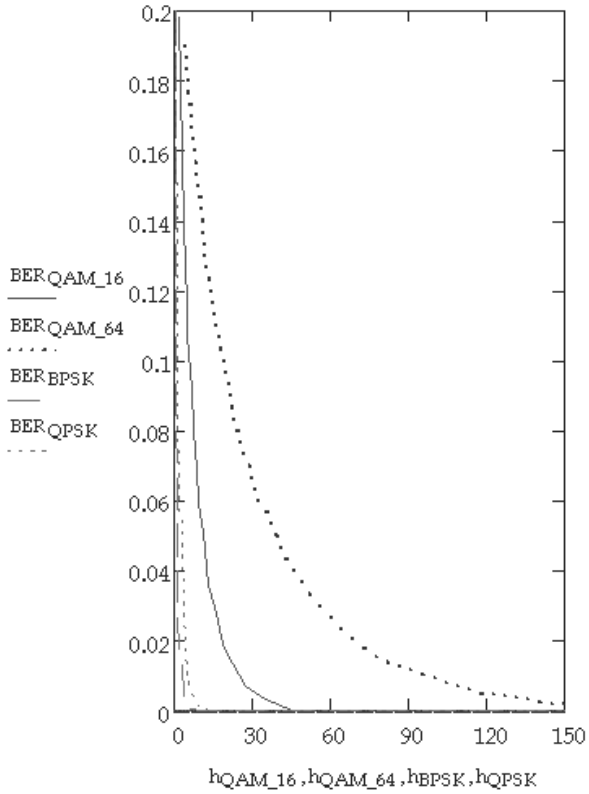

Рис. 4. Графік залежності параметра BER від відношення с/ш для QAM-16, QAM-64, BPSK, QPSK

Висновки

Таким чином в даній роботі було проведено аналіз додаткової затримки, що вноситься в мережу при використанні засобів захисту та змодульовано передачу мовного повідомлення по безпроводовому КЗ. Результати моделювання довели, що зі збільшенням довжини ключа додаткова затримка збільшується, а відповідно якість мови зменшується. Але, разом з тим, рівень захисту каналу значно підвищується.

Із графіка залежності параметра BER від відношення с/ш в КЗ видно, що найкраща якість відновлення повідомлення буде для модуляції BPSK, оскільки при однаковому значенні с/ш в каналі зв'язку при її використанні параметр BER – найменший.

За допомогою вбудованої функції MathCad отриманий вектор бітового потоку було записано в аудіофайл. Якість звуку для різних видів модуляції – різна. Із прослуханих файлів, можна зробити висновок, що найкраща якість звуку там, де використовувалася модуляція BPSK.

Література

[1] Горелов Г.В., Ромашкова О.Н., Чан Туан Ань. Качество управления речевым трафиком в телекоммуникационных сетях / Под редакцией Г.В. Горелова – М.: Радио и связь, 2001. – 112 с.: ил.

[2] Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стенография. Теория и практика. – К.: "МК-Пресс", 2006. – 288 с., ил.

[3] Шелухин О.И., Лукьянцев Н.Ф. Цифровая обработка и передача речи / Под ред. О.И. Шелухина. – М.: Радио и связь, 2000. – 456 с.: ил.

[4] Борискевич А.А. Электронный учебно-методический комплекс по дисциплине Цифровая обработка речи и изображени – Минск 2007. – 294 с.

[5] Federal Information Processing Standards Publication 197. Specification for the ADVANCED ENCRYPTION STANDARD (AES). - November 26, 2001.

УДК 004.054 (045)

Конахович Г.Ф, Беженарь Ю.В., Голубничий А.Г., Одарченко Р.С. Оценка качества восстановления речи в защищенных беспроводных каналах связи

Аннотация. *В данной статье рассмотрено дополнительную задержку, вносимую в сеть при использовании средств защиты информации, а также разработана модель передачи речевого сообщения по защищенному беспроводному каналу связи и проанализировано его качество восстановления. Основные положения статьи реализованы в виде расчетной модели, которую можно использовать для проектирования беспроводных защищенных систем.*

Ключевые слова: *речевое сообщение, дополнительная задержка, шифрования (AES), беспроводной канал связи, BER, качество восстановления.*

Konakhovych G.F, Bezhenar I.V., Golubnichiy A.G., Odarchenko R.S. Speech recovery quality assessment in secure wireless communication channels

Abstract. *This article puts under consideration the additional delay, introduced by the network using information security aids, as well as investigates the transmission model of the voice message over a secure wireless communication channel, and analyzes its playback quality. The major issues of the article are implemented as computational models that can be used to design secure wireless systems.*

Keywords: *voice message, the additional delay, encryption (AES), a wireless communication channel, BER, quality of recovery.*

Отримано *19 березня 2012 року,* затверджено редколегією *07 червня 2012 року*
(рецензент д.т.н., професор Ю.В. Куц)

МЕТОДИКА ОБРОБКИ АЕРОФОТОЗНІМКІВ ДЛЯ ПОБУДОВИ ЦИФРОВИХ КАРТ ТА ЗАХИСТУ КАРТОГРАФІЧНИХ ДАНИХ

Юлія Іваник

Національний авіаційний університет

ІВАНИК Юлія Юріївна

Рік та місце народження: 1989 рік, м. Ківерці, Волинська область, Україна.
Освіта: Національний авіаційний університет, 2012 рік.
Посада: аспірант кафедри землевпорядних технологій з 2012 року.
Наукові інтереси: створення баз картографічних даних.
Публікації: 5 наукових публікацій, серед яких наукові статті, тези та матеріали доповідей на конференціях.
E-mail: Ivanyk10@mail.ru

Анотація. *У статті пропонується методика обробки аерофотознімків, перетворення їх в геоприв'язане зображення і їх подальша векторизація., а також шляхи захисту створених таким чином картографічних даних. Дано практичні рекомендації щодо використання отриманих результатів.*

Ключові слова: *бази картографічних даних, геоприв'язані зображення, захист даних, «Digitals».*

Вступ. Сучасні геоінформаційні технології вирішують широкий спектр наукових та прикладних задач сьогодення. Разом з тим існують «вузькі» місця в цих технологіях, які стримують їх розвиток та використання. Такими проблемними задачами є методи обробки аерофотознімків для побудови цифрових карт та захисту картографічних даних. В даній статті автор пропонує свій підхід до вирішення цих задач.

Постановка задачі. Одним з методів, які картографи використовують в процесі створення карт,