Література

1. Биковцев І.С. – Захист інформації в системі організації повітряного руху/ Биковцев І.С., Дем'янчук В.С., Клименко В.О., Дорошко В.О. та інші. – К.:ДП ОПР України, 2008. – 236 с.
2. Невойт Л.В. – Практичні аспекти забезпечення інформаційної безпеки/ Невойт Л.В., Дорошко В.О., Чередниченко В.С.// Сучасний захист інформації, №2, 2010. – с. 4-9.
3. Петров А.А. – Оценка эффективности комплексной системы защиты информации в сетях общею пользования/ Петров А.А., Хорошко В.А.// Збір.наук.праць ВІКНУ ім. Т. Шевченка, Вип. № 21, 2009. – с. 128-131.

В даній статі розглянуті питання направлені на вирішення проблеми інформації залежності системи зв'язку, та зроблена спроба оцінки характеристик захищеності системи зв'язку.

В данной статье рассмотренные вопросы направленные на решение проблемы информации зависимости системы связи, и сделанная попытка оценки характеристик защищенности системы связи.

In this article the considered questions the problems of information of dependence of communication network, and done attempt of estimation of descriptions of protected of communication network, directed on a decision.

Рецензент: д.т.н., проф. Шелест М.Є.
Надійшла 27.01.2011

УДК 621.396

Дідковський Р.М., Фауре Е.В.,Олексієнко В.В. (ЧДТУ)

ПРИХОВАНА ПЕРЕДАЧА ІНФОРМАЦІЇ У ПОЛОСІ ЗВУКОВИХ ЧАСТОТ

Вступ

Проблема захисту інформації при її передачі по каналах зв'язку є надзвичайно актуальною в сучасних умовах [1].

Не існує і, напевне, не може бути однозначно оптимального вирішення цієї проблеми. Її різноманітними засобами намагаються вирішувати фахівці багатьох галузей науки і техніки: криптографії [2], стеганографії [3], зв'язку та телекомунікацій [4].

Криптографічні методи не передбачають приховування факту передачі інформації. Їх, як правило використовують у комбінації з іншими методами.

Якщо розглядати методи, що безпосередньо спрямовані на приховування або маскування передачі, то увага багатьох фахівців прикута до двох напрямків: цифрова стеганографія [5] та маскування мовних сигналів [6-7]. В останньому випадку аналоговий мовний сигнал маскується спеціально сформованим (в деяких випадках цифровими методами) псевдошумовим сигналом.

У системі зв'язку, яка запропонована в даній роботі, мовний (або в більш загальному звуковий) та псевдошумовий сигнали міняються ролями. Звуковий сигнал маскує передачу цифрової інформації за допомогою псевдошумового сигналу малої потужності.

До такого рішення підштовхують активні дослідження останніх десятиліть у галузі передачі інформації за допомогою шумоподібних [4], хаотичних [8-9] та істино шумових сигналів [10, 11]. Перевагою таких систем є їх здатність працювати «під шумом». Однак, на шляху використання методів передачі даних, розроблених для систем такого типу, виникає ряд проблем.

Звуковий частотний діапазон, обраний для побудови системи, дозволяє легко здійснювати фіксацію і цифровий аналіз сигналів загальнодоступними мультимедійними засобами. Тому специфічна форма осцилограми і спектру сигналу з стрибкоподібною зміною

фази або частоти (класичного шумоподібного сигналу) в даному випадку може розглядатися як значний демаскуючий фактор.

В той же час, системи з хаотичними та шумовими носійними значно поступаються системам з шумоподібними сигналами в завадостійкості [12]. Виникає задача розробки системи, яка би поєднала властивості скритності передачі, притаманної системам з хаотичними та шумовими сигналами, з високою завадостійкістю систем з шумоподібними сигналами.

Постановка задачі

Основна ідея роботи полягає у використанні існуючих проводових ліній зв'язку, призначених для передачі аналогових сигналів звукового діапазону частот (проводове радіо, телефонні лінії, тощо), з метою скритої передачі конфіденційної цифрової інформації.

Обидві системи зв'язку (основна аналогова і прихована цифрова) мають функціонувати одночасно в одному частотному діапазоні.

1. Структура системи

На рис. 1 зображено структурну схему запропонованої системи зв'язку. Фактично, з точки зору базової системи передачі звукового сигналу (системи прямого призначення), прихована цифрова система будується шляхом паразитного підключення до лінії зв'язку та використання ресурсів каналу базової системи.

Рис. 1. Структурна схема системи зв'язку

Як зазначено вище, використання сигналів звукового діапазону частот дає можливість здійснювати формування і обробку сигналів повністю цифровими методами в дискретному часі за допомогою стандартного мультимедійного комп'ютерного обладнання.

Це дозволило, по перше, запропонувати вирішення поставленої задачі, яке базується на повній відмові від гармонійної носійної. Роль носійної виконує фіксована реалізація гауссового випадкового процесу. По друге – досить обмеженими засобами побудувати діючий експериментальний макет системи.

Експериментальна система складається з двох рознесених комп'ютерів, апаратури узгодження з лінією та спеціального програмного забезпечення. Формування і обробка сигналів відбувається у відкладеному часі, а процедура обміну повідомленнями нагадує процес передачі і отримання SMS в мережах мобільного зв'язку.

2. Формування і обробка сигналів

Розглянемо принципи побудови і функціонування системи. Передавач і приймач системи містять в собі ідентичний за змістом фазовий накопичувач (ФН), який зберігає довгу числову послідовність (в експериментальному макеті $2^{26} = 67\,108\,864$ відліків). Дана послідовність є реалізацією дискретного гауссового випадкового процесу з незалежними

відліками і нульовим математичним сподіванням. Кожен відлік представлений 16-бітним цілим числом (із знаком). Значення відліків змінюються в межах від -16 000 до 16 000.

У розпорядженні системи існує цілий набір файлів з цифровими фіксаціями реалізацій гауссового випадкового процесу. Наповнення цих файлів може бути отримане різними шляхами: за допомогою цифрових генераторів випадкових чисел або шляхом фіксації шумового сигналу знятого з технічних пристроїв (наприклад, радіо- або телевізійного приймача відстроєного від сигналу передаючих станцій). Дані одного із таких файлів завантажуються у фазовий накопичувач перед початком передачі даних.

Для кожного сеансу зв'язку на передавальній і приймальній стороні встановлюється кодове слово, по якому розраховується початкове зміщення у ФН. Вибірка даних з ФН здійснюється за принципом кільцевого буфера.

2.1. Передавач

Фрагменти дискретного сигналу заданої довжини T, що надходять з ФН, піддаються бінарній фазовій маніпуляції. Після цифро-аналогового перетворення, фільтрації та підсилення сигнал подається до лінії зв'язку.

Перші чотири біта повідомлення мають фіксований вигляд («1111») і використовуються як старт-сигнал. Стоповий сигнал формується як інверсія в часі від стартового сигналу. Рис. 2 ілюструє принцип формування сигналу системи.

Префікс і суфікс сигналу мають випадкову довжину. Їх призначення – маскування істинного положення в часі моменту початку та закінчення кадру даних. Кожне дискретне значення вибране для формування префіксу або суфіксу помножається на випадково вибраний коефіцієнт 1 або -1. Цей процес на рисунку умовно позначений як «Рандомізація».

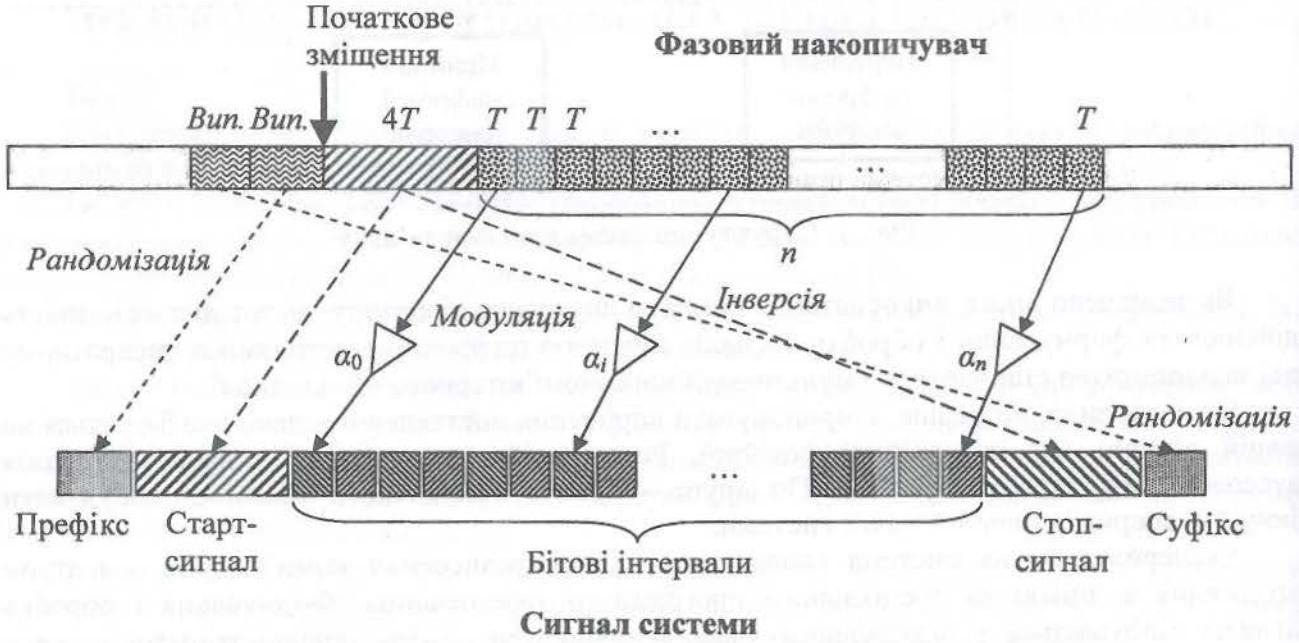


Рис. 2. Принципи формування сигналу системи

Коефіцієнт $\alpha_i = 1$, якщо i-ий біт інформаційного повідомлення дорівнює «1», і $\alpha_i = -1$, якщо i-ий біт – «0». Множення всіх значень амплітуди i-го бітового інтервалу на цей коефіцієнт забезпечує модуляцію сигналу.

Отже, маємо систему зв'язку з бінарною фазовою маніпуляцією гауссового псевдошумового сигналу.

Відмітимо, що імовірнісний розподіл сигналу симетричний відносно нуля, тому множення фрагментів сигналу на 1 або -1 не вносить в цей сигнал ніяких ознак модуляції. Не

маючи в розпорядженні джерела опорного сигналу та не володіючи всіма параметрами системи (початкове зміщення у ФН, довжина бітового інтервалу T), виділити з сигналу інформацію, більш того, навіть запідозрити, що даний сигнал переносить інформацію, третій стороні не вбачається можливим. Єдиним способом виявити невипадковість сигналу та встановити факт передачі є аналіз повторюваності фрагментів сигналу на тривалому періоді спостереження. Однак, і ця проблема може бути вирішена досить простими засобами.

Сигнал на виході цифрового тракту передавача протягом одного бітового інтервалу може бути представлений у вигляді вектора $\bar{x} = (x_1, x_2, ..., x_{n_o})$. Цей вектор може бути підданий деякому ортогональному перетворенню, яке зберігає середнє значення координат вектора [11]. Найпростішим прикладом такого перетворення є перестановка координат [13].

Оскільки система працює при відношенні потужності сигналу до потужності завад $\rho^2 = P_x / P_n$ багато меншому одиниці, то довжина бітового інтервалу T має бути досить великою для забезпечення надійного зв'язку. Це означає, що розмірність n_o вектора $\bar{x}$ – досить велике число (в експериментальних дослідженнях $n_o \geq 128$), оскільки кількість координат вектора визначається як $n_o = T / \Delta t_n$, де Δt_n – період роботи цифро-аналогового перетворювача (ЦАП) передавача.

Набір перестановок координат вектора $\bar{x}$ налічує $n_o!$ елементів, отже алфавіт перетворень достатньо великий для усунення повторюваності фрагментів сигналу протягом тривалого часу експлуатації системи. Зауважимо, що з системи перетворень необхідно вилучити перестановки, що залишають незмінними довгі неперервні ланцюги координат вектора.

При передачі кожного наступного кадру даних використовується нове перетворення. Якщо ж алфавіт перетворень вичерпано, то в ФН завантажується наступна послідовність.

Такий комплекс заходів усуває повторюваність сигналу протягом часу досяжного для спостереження і аналізу третьою особою.

2.2. Приймач

Специфікою досліджуваної системи є те, що роль завад в ній виконує мовний або інший звуковий сигнал. Важливою особливістю такого сигналу є його нестаціонарність [14].

В умовах нестаціонарних завад саме побудова бінарної системи зв'язку з протилежними сигналами є оптимальним рішенням, оскільки пороговий рівень детектора в приймачі такої системи дорівнює нулю не залежно від відношення сигнал-завада.

На приймальній стороні аналогово-цифровий перетворювач (АЦП) приймача працює з частотою кратною частоті ЦАП передавача. З метою підвищення точності синхронізації відповідний множник частоти k_Δ може бути встановлений більшим ніж 1: 2, 4, 8 і т.д.

При однаковій частоті цифро-аналогового та аналогово-цифрового перетворення (на передавальній та приймальній стороні відповідно) період роботи АЦП дорівнює періоду роботи ЦАП $\Delta t_{пр} = \Delta t_n$ і помилка визначення моментів вибірки даних за абсолютною величиною може набувати значень в межах від 0 до $0.5\Delta t_n$. Найбільш несприятливою є ситуація, коли ця помилка близька до $0.5\Delta t_n$.

Для спрощення міркувань будемо вважати, що проміжні значення амплітуди сигналу між точками дискретизації можна (з певною похибкою) визначити шляхом лінійної інтерполяції. Якщо помилка часу вибірки становить $0.5\Delta t_n$, то до цифрового тракту приймача замість відліку із значенням x_i надійде значення $\xi_i = 0.5(x_i + x_{i+1})$. Цей ефект еквівалентний застосуванню до сигналу цифрового фільтра ковзаючого усереднення з вікном довжиною два відліки. Така фільтрація суттєво зменшує потужність дискретного сигналу з незалежними відліками, що негативно впливає на завадостійкість системи.

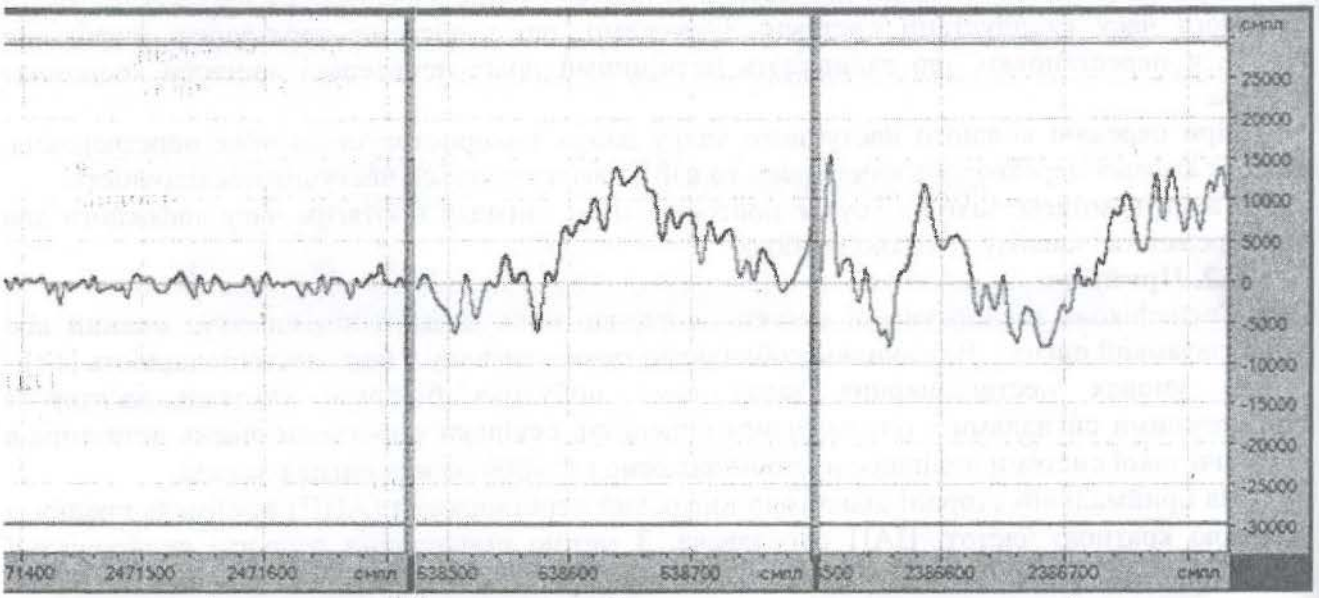
В експериментальних дослідженнях використовувався множник частоти дискретизації $k_\Delta = 4$. У такий спосіб $\Delta t_{пр} = 0.25\Delta t_n$, а абсолютна величина помилки часу вибірки даних не перевищує $0.125\Delta t_n$.

На рис. 3 подано приклади фрагментів осцилограм сигналів зафіксованих на приймальній стороні системи. З рисунку видно, що амплітуда завад (рис. 3,б) значно перевищує амплітуду модульованого шуму (рис. 3,а), тому визначити візуально наявність прихованого сигналу за осцилограмою суміші сигналу і завад практично не можливо (рис. 3,в).

Розглянемо базовий алгоритм роботи приймача. Початковий стан приймача – режим очікування. У цьому стані працює лише пороговий пристрій увімкнення. Якщо модуль амплітуди вхідного сигналу перевищує заданий поріг, то приймач переходить у режим пошуку старт-сигналу.

У цьому режимі приймач здійснює виявлення старт-сигналу у вхідному потоці. Якщо прийнято рішення про виявлення старт-сигналу, то приймач синхронізується по його положенню і переходить в режим прийому повідомлення.

У режимі прийому відбувається детектування вхідного сигналу, точна синхронізація та виявлення стоп-сигналу. Якщо стоп-сигнал виявлено, то прийом повідомлення завершується і приймач повертається в режим очікування.



а) б) в)

Рис. 3. Фрагменти осцилограм сигналів зафіксованих на приймальній стороні:
а) модульований псевдошумовий сигнал; б) чистий звуковий сигнал; в) суміш сигналів.

Виявлення та прийом сигналів здійснюються кореляційними методами. Якщо множник частоти дискретизації більший одиниці, то перед тим, як сигнал надійде до корелятора, відбувається процедура децимації з відповідним коефіцієнтом. Формування опорного сигналу відбувається шляхом вибірки даних із ФН у повній відповідності до формування інформаційного сигналу в передавачі (за виключенням модуляції).

Точна синхронізація виконується завдяки наявності трьох паралельних кореляторів, які працюють із запізненням 0, 1 і 2 відліки. Якщо максимум відгуку припадає не на центральний корелятор, то відбувається корекція синхронізації.

Окрему увагу слід приділити процедурі виявлення старт-сигналу. Оскільки завади в системі мають суттєво нестаціонарний характер, то класичні методи виявлення сигналу, що ґрунтуються на перевищенні відгуком узгодженого фільтра заданого порогового рівня не

ефективні. Запропоновано адаптивний метод виявлення старт-сигналу, що враховує особливості шумоподібної носійної з незалежними відліками.

Пристрій початкової (грубої) синхронізації приймача обчислює модуль взаємно-кореляційної функції для потоку дискретних значень y_1, y_2, …, y_i вхідного сигналу та вектору $\bar{s} = (s_1, s_2, ..., s_{n_s})$, що представляє у дискретному вигляді старт-сигнал. З урахуванням множника частоти k_Δ маємо:

$$r_i = \left| \sum_{j=1}^{n_s} y_{i+(j-n_s)k_\Delta} s_j \right|.$$

Таблиця з $k + k_\Delta$ останніх значень r_i зберігається в пам'яті приймача.

Відлік y_{i-1} буде визнано приймачем останнім відліком старт-сигналу, якщо послідовно виконані наступні три умови:

1. У цій позиції знаходиться локальний максимум модуля взаємно-кореляційної функції, тобто виконуються нерівності $r_{i-1} > r_i$ та $r_{i-1} > r_{i-2}$.
2. Значення r_{i-1-k_Δ}, що відповідає попередньому відліку сигналу передавача знаходиться нижче порогового рівня: $r_{i-1-k_\Delta} < K \cdot r_{i-1}$.
3. Середнє значення попереднього фрагменту модуля взаємно-кореляційної функції $R = \frac{1}{k} \sum_{j=1}^{k} r_{i-1-k_\Delta-j}$ менше порогового рівня: $R < K \cdot r_{i-1}$.

Відмітимо, що пороговий рівень визначається відносно знайденого локального максимуму. Такий підхід забезпечує адаптивність системи до нестаціонарних завад.

Параметри K (коефіцієнт порогового рівня), та k (довжина вікна усереднення) вибираються в залежності від завадової обстановки. В експериментальних дослідженнях використовувалися наступні значення: $K = 0.15$, $k = 256$.

Рис. 4,а ілюструє стан пам'яті блоку синхронізації приймача в момент виявлення старт-сигналу. На рис. 4,б показано випадок хибного викиду модуля взаємно-кореляційної функції, який виникає за рахунок значного зростання амплітуди аналогового сигналу (завад). Хоча абсолютна величина відповідного локального максимуму навіть перевищує істинний максимум функції r, наведені вище правила відбору (пункти 2 і 3) чітко фіксують хибну тривогу.

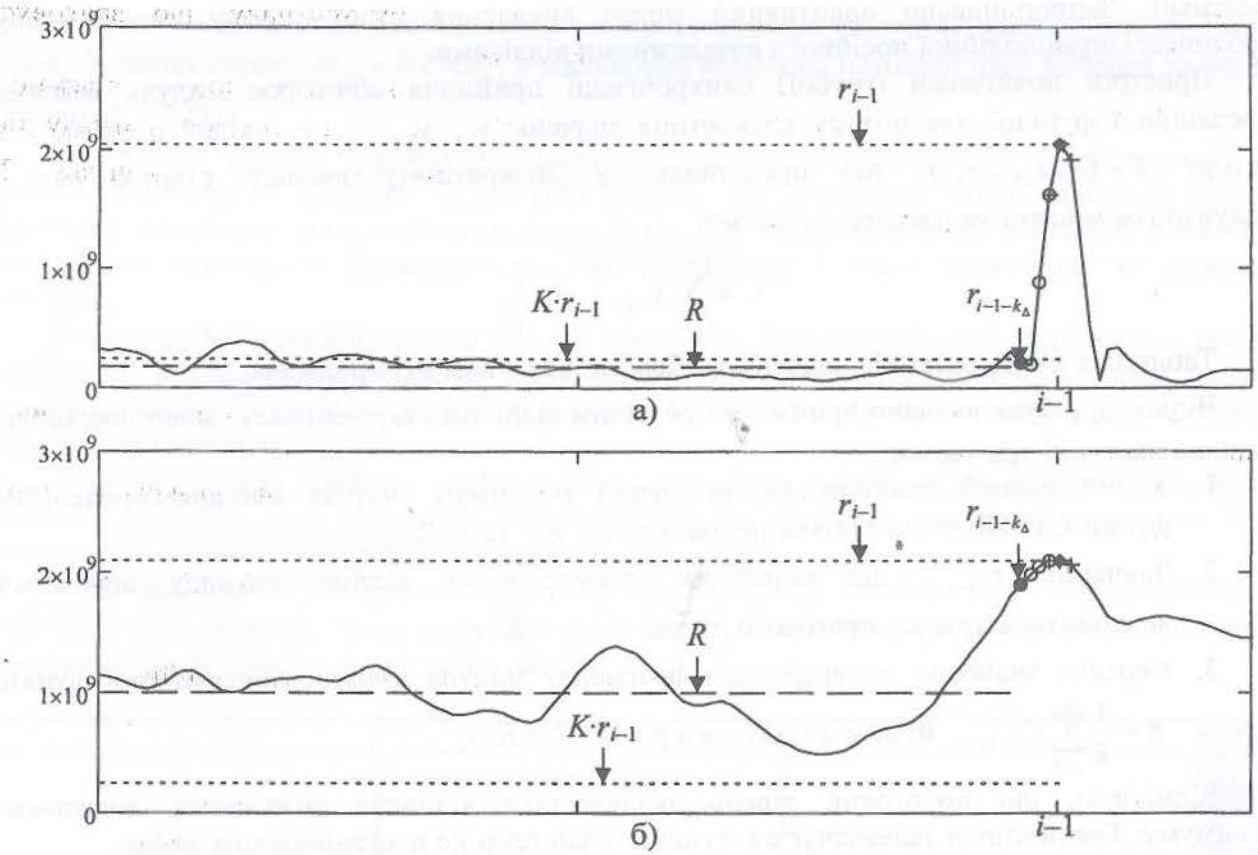


Рис. 4. Процедура виявлення старт-сигналу: а) старт-сигнал виявлено; б) хибна тривога.

Оскільки можливе положення стоп-сигналу цілком визначене і може бути розраховане від закінчення чергового бітового інтервалу, то виявлення стоп-сигналу відбувається набагато простіше. Достатньо перевірити перевищення модулем відповідної взаємно-кореляційної функції порогового рівня розрахованого відносно максимуму визначеного для старт-сигналу. В експериментальних дослідженнях коефіцієнт порогового рівня виявлення стоп-сигналу був вибраний рівним 0.75.

3. Експериментальні дослідження

Експериментальний макет системи був виконаний у двох варіантах. Перший варіант призначений для лабораторних досліджень з повністю керованими параметрами. Система складається з трьох комп'ютерів та акустичної колонки. Лінійний вихід звукової карти одного з комп'ютерів з'єднується з колонкою кабелем довжиною 15 м. Ця пара пристроїв імітує основну аналогову систему і дозволяє відтворювати звукові файли із заданою потужністю сигналу. До цього кабелю підключено також лінійний вихід звукової карти комп'ютера оснащеного програмою «Передавач», а на іншому кінці лінійний вхід комп'ютера оснащеного програмою «Приймач».

У такій системі використовувалась частота дискретизації ЦАП передавача 48 кГц, а АЦП приймача 192 кГц. При довжині бітового інтервалу $n_o = 256$ або $5.333 \cdot 10^{-3}$с передача даних відбувається на швидкості 187.5 біт/с. Довжина кадру 10000 біт.

Наприклад, при відношенні потужностей сигналу і завад $\rho^2 = 0.0305$ отримаємо, що відношення сигнал-завада: $h^2 = \rho^2 \cdot \frac{n_o}{2} = 0.0305 \cdot \frac{256}{2} = 3.904$. Тут формула відношення сигнал-завада h^2 записана для випадку дискретної обробки сигналу (див. [15]).

Тоді за формулою

$$P_b = 1 - \Phi\left(\sqrt{2h^2}\right),$$

де $\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-\frac{t^2}{2}} dt$ – інтеграл ймовірностей, отримаємо теоретичну оцінку імовірності помилки передачі біта $P_{b\,теор} = 0.0026011$.

В експерименті при передачі 10 000 біт отримали в середньому 28.4 помилок, тобто експериментальна оцінка імовірності помилки $P_{b\,експ} = 0.00284$, що добре узгоджується з теоретичними розрахунками.

Другий варіант системи побудований для передачі даних по телефонних лініях. Система включає в себе 4 телефонні апарати і два комп'ютера. На кожній стороні системи знаходиться два паралельних телефонних апарата. На передавальній стороні до одного з них приєднується лінійний вихід звукової карти комп'ютера-передавача, а на приймальній – лінійний вхід комп'ютера-приймача. За допомогою вільних апаратів встановлюється зв'язок і ведеться бесіда як джерело маскуючого сигналу. Одночасно з бесідою через паралельні апарати передається сигнал цифрової системи.

В цьому випадку частота дискретизації ЦАП передавача 6 кГц, а АЦП приймача 24 кГц. При довжині бітового інтервалу $n_0 = 128$ або 0.021 с передача даних відбувається на швидкості 46.875 біт/с.

Отже, експериментальний макет системи виявився цілком придатним для передачі конфіденційних цифрових даних по незахищених лініях у режимі відкладеної обробки.

Висновок

Таким чином, в роботі запропонована дешева, проста в реалізації система зв'язку придатна для скритної передачі коротких інформаційних повідомлень по вже розгорнутим лініям зв'язку. Система працює паралельно в одному частотному діапазоні з аналоговою системою прямого призначення.

Низький рівень сигналу на фоні високоенергетичних завад, рівномірний розподіл енергії по всій доступній полосі частот, складність форми сигналу в комплексі з традиційними методами криптографічної обробки бітового потоку забезпечують високий рівень скритності передачі та захищеності даних, не зважаючи на використання відкритих каналів зв'язку.

Список літератури

1. Зайцев А. П. Технические средства и методы защиты информации: Учебник для вузов / Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.; под ред. А.П. Зайцева и А.А. Шелупанова. М.: Машиностроение, 2009. – 508 с.

2. Ященко В.В. Введение в криптографию: Учебник для вузов / под ред. В.В. Ященко. СПб.: Питер, 2002. – 288 с.

3. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. – М.: Солон-Пресс, 2002. – 265 с.

4. Варакин Л.Е. Системы связи с шумоподобными сигналами. – М.: Радио и связь, 1985. – 384 с.

5. Савченко Ю. Г., Сажина І. А. Організація прихованого інформаційного обміну в режимі реального часу // Наукові записки УНДІЗ. – 2010. – №1(13). – С.57-62.

6. Цирульник С.М., Роптанов В.І., Рехлецький О.С. Розв'язання задачі технічного захисту інформації за умови впливу «мовоподібної» завади // Інформаційні технології та комп'ютерна інженерія. – 2009. – №1(14). – С.5-8.

7. Архипова О.О. Дослідження кореляційного методу оцінки ефективності маскування мовного сигналу // Радіоелектроніка. Інформатика. Управління. – 2009. – № 1. – С.62-66.

8. Дмитриев А.С., Клецов А.В., Лактюшкин А.М., Панас А.И., Старков С.О., Хилинский А.Д. Сверхширокополосная беспроводная связь на основе динамического хаоса // Радиотехника и электроника. – 2006. – Т. 51. – № 10. – С.1193-1209.

9. Короновский А.А., Москаленко О.И., Храмов А.Е. Скрытая передача информации на основе режима обобщенной синхронизации в присутствии шумов // Журнал технической физики. – 2010. – Т.80,Вып.4. – С.1-8.

10. Васюта К.С. Метод передачи информации, основанный на манипуляции показателя Херста фрактального ("цветного") гауссовского шума // Системи обробки інформації. – 2010. – Вип. 6 (87). – С.62-65.

11. Дідковський Р.М., Метелап В.В. Підвищення рівня захищеності даних в системах зв'язку з фазовою маніпуляцією шумового сигналу // Вісник ЧДТУ. – 2010. – № 3. – С.53-57.

12. Дідковський Р.М. Порівняльний аналіз завадостійкості бінарних систем зв'язку з протилежними шумовими сигналами // Вісник ДУІКТ. – 2010. – Т.8, №4. – С.387-407.

13. Lau F.C.M., Cheong K.Y., Tse Chi K. Permutation-Based DCSK and Multiple-Access DCSK Systems // IEEE Trans. Circuits Syst. I. – 2003. – vol. 50, no. 6. – P.733–742.

14. Демьян Н.И., Осмоловский В.А., Хорошко В.А. Линейные и нелинейные параметрические модели речевого сигнала // Захист інформації. – 2010. – №2. – С.60-64.

15. Тихонов В.И., Харисов В.Н. Статистический анализ и синтез радиотехнических устройств и систем: Учеб. Пособие для вузов. – М.: Радио и связь, 1991. – 608 с.

В роботі запропонована система зв'язку для прихованої передачі конфіденційних цифрових даних по існуючим відкритим каналам зв'язку звукового частотного діапазону. Представлені принципи побудови та функціонування системи, методи формування та обробки сигналу.

Ключові слова: прихована передача даних, широкополосна система зв'язку, шумоподібних сигнал, бінарна фазова маніпуляція.

В работе предложена система связи для скрытой передачи конфиденциальных цифровых данных по существующим открытым каналам связи звукового частотного диапазона. Представлены принципы построения и функционирования системы, методы формирования и обработки сигнала.

Ключвые слова: скрытая передача данных, широкополосная система связи, шумоподобный сигнал, бинарная фазовая манипуляция.

This paper presents a communication system for hidden transfer confidential data via the existing open communication channels in the audible frequency band. The principles of system construction and operation, methods of signal forming and signal processing are presented.

Key words: hidden data transfer, wideband communication system, noise-like signal, binary phase shift keying.

Рецензент: д.т.н., проф. Єрохін В.Ф.
Надійшла 12.01.2011

УДК 621.391.7

Шинкаренко И.В., Цопа А.И. (ХНУРЭ)

ИМИТАЦИОННАЯ МОДЕЛЬ ОТВОДНОГО КАНАЛА С ЭЛЕКТРИЧЕСКОЙ СВЯЗЬЮ ДЛЯ ПРОВОДНЫХ ЦИФРОВЫХ СИСТЕМ ПЕРЕДАЧИ ИНФОРМАЦИИ

Введение

При создании производительных ведомственных систем связи (ВСС), одним из основных требований предъявляемым к таким сетям является обеспечение не только высокой производительности, но и защищенности каналов связи. Несмотря на большое количество разработанных протоколов защиты информации на верхних ступенях семиуровневой модели взаимодействия открытых систем (*OSI*), эффективность их значительно снижается при передаче в ВСС мультимедийной информации [1]. Кроме того, при массовом внедрении цифровых технологий передачи информации обеспечить повышенные требования безопасности только одними информационными (криптографическими) методами не представляется возможным. В этих условиях необходимо искать новые пути повышения защищенности каналов связи не только на информационном, но и на физическом (энергетическом) уровне модели *OSI*.

Учитывая то, что современный этап модернизации ВСС связан лавинообразным внедрением в этих сетях цифровых методов передачи, обработки и хранения информации, то это дает повод по новому взглянуть на роль и значение технической защиты информации (ТЗИ).

Концепция технической защиты информации в Украине, которая утверждена в 1997 г. соответствующим Постановлением Кабинета Министров Украины [2], определяет основные направления развития ТЗИ и ее роли в обеспечении безопасности государства. В наше время