УДК 004.3

АЛГОРИТМИ ЗАХИСТУ МОВНИХ СИГНАЛІВ ЗА ДОПОМОГОЮ СКРЕМБЛЕРІВ ТА ШИФРАТОРІВ

Касянчук М.М.[1)], Фещук М.А.[2)], Савка Н.Я.[3)]
Тернопільський національний економічний університет
[1)] к.ф.-м.н., доцент; [2)] магістрант; [3)] к.т.н., викладач

І. Постановка проблеми

У сучасних умовах захисту мовної інформації конфіденційного характеру приділяється все більша увага. З одного боку це обумовлено високою інформативністю мовних повідомлень. З іншого боку, різноманітністю інформаційних загроз у ставленні до мовної інформації [1], що знайшло своє відображення в великому різноманітті сучасних методів і засобів захисту мовних повідомлень від несанкціонованого доступу.

Пристрої та способи захисту мовної інформації різко зменшують можливості незаконно прослуховуючих пристроїв і дозволяють користуватися каналами передачі інформації, не беручи до уваги фактор прослуховування ліній зв'язку (несанкціонованого доступу) з боку зловмисника.

Мовний сигнал слід розглядати як особливий вид інформаційного повідомлення, що обумовлює застосування специфічних заходів власного захисту, під якими розуміється використання спеціальних засобів, методів, що і визначає актуальність даної роботи.

ІІ. Мета роботи

Метою даної роботи є розробка алгоритмів захисту мовних сигналів в каналах передачі інформації за допомогою скремблерів та шифраторів.

ІІІ. Алгоритм захисту мовних сигналів за допомогою скремблерів та шифраторів

Аналогові скремблери перетворюють вихідний мовний сигнал шляхом зміни його амплітудних, частотних і часових параметрів. Потім скрембльований сигнал передається в тій же смузі частот, що і вихідний. Всі перестановки маскованих мовних фрагментів у більшості аналогових скремблерів у часовій і частотній областях здійснюється по псевдовипадковому закону, відповідно до послідовності, що виробляється ключем, яка змінюється від одного повідомлення до іншого. На приймальній стороні здійснюється дешифрування цифрових кодів, які отримані з каналу зв'язку, і перетворення їх в аналогову форму.

Якість відновленої мови залежатиме від якості (на передавальній та приймальній сторонах) змішувачів та фільтрів, якими обмежується спектр вхідного сигналу і виділяється нижня смуга частот перетвореного сигналу, та від корекції частотних спотворень каналу на приймальній стороні, вплив яких позначається також інверсно: загасання каналу для високочастотної частини спектра на прийомі впливає на низькочастотну частину сигналу і навпаки. У випадку перехоплення сигнал з інвертованим спектром легко може відновлюватися будь-яким аналогічним апаратом (причому не обов'язково однотипним), а при відповідному тренуванні – і безпосередньо сприйнятий людиною. Для підвищення стійкості при захисті доцільно вводити змінну частоту гетеродина, який встановлюється партнерами за домовленістю у вигляді числового коду-пароля, який вводиться у апарат при переході у захищений режим.

Альтернативним аналоговому скремблюванню методом передачі мови в закритому вигляді є асиметричне шифрування [2] мовних сигналів, які перетворені у цифрову форму перед їх передачею. У системах, що використовують уявлення мовного сигналу на основі теореми Хургіна-Яковлєва, в результаті проведених досліджень, було отримано, що для якісного відновлення сигналу необхідно по 3 ітерації за відліками розрідженого та нерозрідженого сигналів.

Висновок

У даній роботі представлено та досліджено алгоритми захисту мовних сигналів в каналах передачі інформації за допомогою скремблерів та шифраторів.

Список використаних джерел

1. Петраков А.В. Защита абонентского телетрафика / А.В.Петраков, В.С.Лагутин. - М.: Радио и связь, 2002. - 504 с.
2. Касянчук М.М. Теорія алгоритмів RSA та Ель-Гамаля в розмежованій системі числення Радемахера – Крестенсона / М.М. Касянчук, І.З. Якименко, О.І. Волинський, І.Р. Пітух // Вісник Хмельницького національного університету. Технічні науки. – 2011. – № 3. – С. 265–273.