УДК 681.391

Д. О. Письмак, В. П. Малайчук, С. В. Клименко

Дніпропетровський національний університет імені Олеся Гончара

ПЕРЕШКОДОСТІЙКЕ КОДУВАННЯ ПОВІДОМЛЕННЯ ЕЛЕКТРОННОГО ПІДПИСУ

Проведено роботу з вивчення і обрання радіоліній зв'язку, алгоритмів формування і обробки електронного підпису. Розроблено функціональні блоки, які дають можливість здійснювати передачу електронного підпису по радіолініях зв'язку. Проведено обчислювальні експерименти для визначення характеристик повідомлення електронного підпису, при яких досягається висока перешкодостійкість.

Ключові слова: *електронний підпис; перешкодостійке кодування*.

Проведена работа по изучению и выбору радиолиний связи, алгоритмов формирования и обработки электронной подписи. Разработаны функциональные блоки, которые дают возможность осуществлять передачу электронной подписи по радиолиниям связи. Проведены вычислительные эксперименты для определения характеристик сообщения электронной подписи, при которых достигается высокая помехоустойчивость.

Ключевые слова: *электронная подпись; помехоустойчивое кодирование*.

Work was carried out on the study and selection of radio links, algorithms for the formation and processing of electronic signatures. Functional blocks, which allow the possibility to carry out the transmission of the electronic signature on the radio communication lines are developed. Computational experiments were carried out to determine the characteristics of the electronic signature notification, in which high impedance is achieved.

Keywords: *electronic signature; noise immunity encoding*.

Постановка проблеми. У сучасному суспільстві набирає популярність спосіб ідентифікації користувача за допомогою електронного підпису. Сучасні методи досить надійні, але і вони мають ряд недоліків, наприклад вплив перешкод і спотворення в повідомленнях.

Виходячи з цього, запропоновано новий алгоритм передачі та обробки повідомлень з електронним підписом. У ході дослідження проведено аналіз існуючих методів передачі повідомлень з

використанням електронного підпису за допомогою радіолінії зв'язку. Розглянуто задачу прихованої передачі повідомлення, яке містить у собі електронний підпис при використанні звичайної радіолінії зв'язку, і при цьому забезпечує високу стійкість перед перешкодами.

Аналіз літературних даних і постановка проблеми. Дану проблему було розглянуто в небагатьох публікаціях [1, 2]. Для вирішення цього завдання необхідно розробити алгоритм, який дозволить при мінімальних модифікаціях використовувати стандартну радіолінію зв'язку для прихованої передачі електронного підпису. Для формування повідомлення, що має в собі електронний підпис, необхідно створити дві послідовності Хаффмана. Перша послідовність буде використана для формування самого електронного підпису, а друга – так звана «несуча», в якій і буде приховано наш електронний підпис. Так як перші послідовності можуть бути практично необмеженої довжини, реалізовано механізм одноденних електронних підписів (можлива реалізація на один місяць або один тиждень). Зміна паролів здійснюється методом «нарізання» послідовності на шматочки заданої довжини, і при цьому довжина задається виходячи з початкових умов, у подальшому ці шматочки і є змінними електронними підписами. Необхідною умовою є те, що одержувач так само повинен мати у себе список з такими підписами, для можливості порівняння і встановлення достовірності отриманого повідомлення. Друга послідовність буде так званою «несучою», в ній і буде приховано електронний підпис. Двійково-кодова послідовність повинна бути значно довшою (як мінімум у 10 разів) електронного підпису для забезпечення секретності і перешкодостійкості. Функціональну схему такого приладу представлено на рис. 1.

Блоки формування та прийому перешкодостійкого двійково-кодовового електронного підпису. Реалізація блоків формування та прийому перешкодостійкого двійково-кодового електронного підпису дозволяє доволі легко перетворювати будь-яку радіолінію зв’язку, яка має змогу передавати сигнали у цифровому вигляді, на радіолінію прихованої передачі повідомлення, яке містить у собі електронний підпис [3].

Насамперед необхідно розглянути блок формування перешкодостійкого двійково-кодового електронного підпису, який представлено на рис. 2.

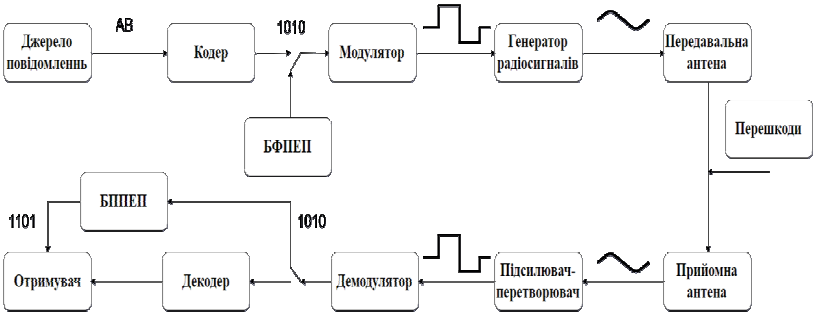

Рисунок 1 – Функціональна схема радіолінії зв'зку з прихованою передачею повідомлень електронного підпису (БФПЕП – блок формування електронного підпису, БППЕП – блок прийому електронного підпису)

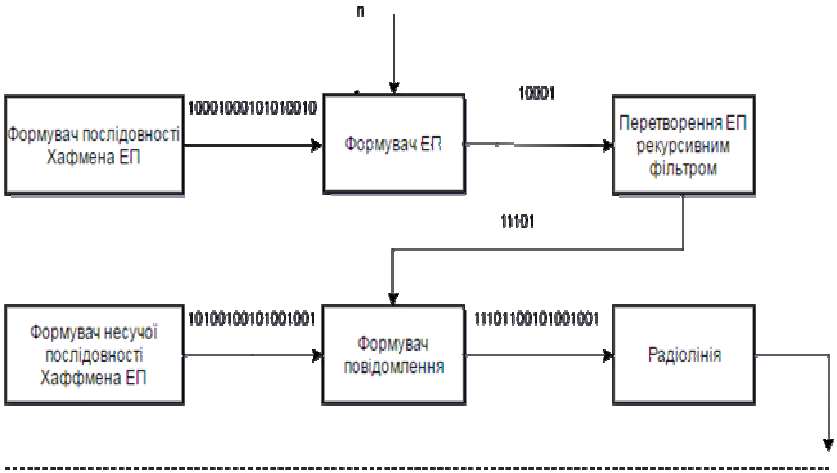

Рисунок 2 – Блок формування перешкодостійкого двійково-кодового електронного підпису (n – розмір підпису, ЕП – електронний підпис)

Розглянемо принцип роботи блоку: спочатку формується послідовність Хаффмена, яка і буде вихідним матеріалом для формування повідомлення електронного підпису. Формується вона залежно від заданих параметрів за спеціальними таблицями, ключовим значенням, необхідним для її формування, є довжина послідовності,

яку ми хочемо отримати, виходячи з довжини, яка нам необхідна, обираються формуючі коефіцієнти і формуються послідовності [4].

Далі, слідуючи заданій задачі, виокремлюється послідовність деякої довжини, яка і буде електронним підписом, це відбувається у формувачі $ЕП_i$. Простішими словами це можна описати як вирізання за обраним нами алгоритмом з довгої послідовності, деяку кількість "0" і "1" довжиною n символів. Залежно від поставленого завдання може бути сформовано довільну кількість підписів (можливо формування до 31 підпису для одного користувача, аби він мав змогу змінювати його кожен день протягом місяця).

Наступним кроком є перетворення отриманого підпису нерекурсивним фільтром. В ньому залежно від характеристик фільтра проходить “шифрування” електронного підпису. На виході ми отримаємо довшу послідовність, і до того ж значно видозмінену. Це буде гарантувати її захищеність.

Після проходження даного фільтра отриману послідовність вбудовуємо в іншу послідовність Хаффмена. Вона сформована за таким самим принципом, тільки її довжина як мінімум на порядок більше довжини електронного підпису (рекомендованою довжиною є довжина, яка більше в 30 разів). Дана послідовність буде виконувати роль несучого повідомлення, в яке і ховається електронний підпис, для передачі його по радіолініях зв’язку.

Потім відбувається додавання електронного підпису шляхом вирізання з несучої послідовності шматка довжиною n, і врізкою на це місце нашого електронного підпису, на виході ми отримуємо деяку послідовність "0" і "1", яку і буде передано по радіолінії зв'язку.

Розглянемо блок прийому повідомлення електронного підпису (рис. 3).

Далі відбувається пошук електронного підпису. Одержувач знаходить його за розумний час, так як він заздалегідь знає місце його розташування та вилучає електронний підпис з місця, де він знаходиться. Отримана послідовність проходить через нерекурсивний фільтр. Це необхідно для того, щоб ми змогли відновити початковий електронний підпис.

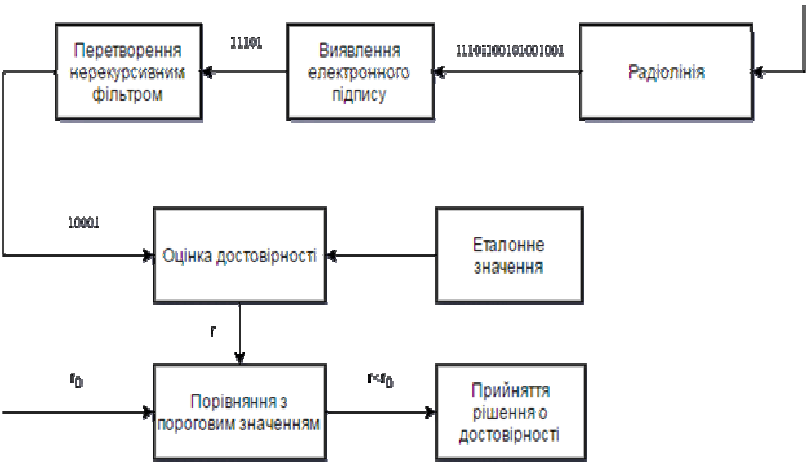

Рисунок 3 – Блок прийому повідомлення електронного підпису

(r_o – гранична кодова відстань, r – кодова відстань)

Після цього нам необхідно на місці одержувача прийняти рішення про достовірність даного електронного підпису, адже під час передачі на нього впливали випадкові фактори, які передбачити ми ніяк не можемо, та й відкидати ймовірність перехоплення і заміни послідовності теж не варто.

Для перевірки достовірності необхідно обчислити кодову відстань шляхом порівняння отриманого електронного підпису і еталонного, далі відбувається порівняння отриманого значення з пороговим, яке вибирається залежно від поставлених умов, і приймаємо рішення – достовірний даний електронний підпис чи ні.

На практиці використано два різницевих рівняння послідовностей Хаффмана такого вигляду:

$$S(k) = \sum_{i=1}^{m} a_i \cdot S(k-i) \qquad (1)$$

Для підвищення перешкодостійкості і додаткового шифрування даних пропустимо електронний підпис через рекурсивний фільтр. Секретність буде досягатися використанням пари фільтрів (рекурсивного і нерекурсівного), і без знання їх дискретної передавальної функції неможливо отримати шуканий електронний підпис, після того як він пройде через нерекурсивний фільтр.

Електронний підпис видозміниться за таким математичним законом:

$$U(k) = S(k) \oplus \sum_{i=1}^{n} a_i \cdot S(k-i), \quad (2)$$

U(k) – електронний підпис після проходження його через нерекурсивний фільтр.

Отриманий електронний підпис вставимо в несучу послідовність на якесь місце, яке може змінюватися статично або динамічно, слідуючи деякому заздалегідь заданому алгоритму (за домовленістю одержувача і відправника).

Так як сам факт передачі і прийому повідомлення в більшості випадків відбувається непомітно від можливого порушника і ймовірність різного виду атак дуже незначна, то при цьому з'являється інша проблема – випадкові перешкоди різного роду, які будуть впливати на сигнал під час передачі. Під впливом перешкод виконавчі сигнали перекручуються, в результаті чого символи інвертуються. Вплив перешкод математично описується таким чином:

$$X(k) = S(k) \oplus \xi(k), \quad (3)$$

де *S (k)* – сигнал на вході; *ξ (k)* – двійковий сигнал перешкоди, який викликає інверсію; *X (k)* – сигнали, які надходить на вхід приймача.

Для того щоб нівелювати вплив перешкод, використовуються довгі несучі послідовності і кілька фільтрів (рекурсивний і нерекурсивний). Але перешкоди можуть все одно з'являтися, тому здійснюється перевірка ступеня спотворення повідомлення шляхом порівняння його з еталонним значенням, яке зберігається в одержувача, і прийняття рішення про те, підпис це чи ні.

Відмінності між еталонним і отриманим повідомленням визначається кодовою відстанню за такою формулою:

$$r(i, j) = \sum_{k=1}^{n} S_i(k) \oplus S_j(k), \quad (4)$$

де $S_i(k)$ – прийнятий електронний підпис; $S_j(k)$ – еталонний електронний підпис.

Отримана кодова відстань порівнюється с граничним значенням, яке вибирається виходячи з розміру електронного підпису:

$$r(i, j) < r_0, (1), \quad (5)$$

де *r(i, j)* – кодова відстань, отримана шляхом додавання підписів; r_0 – якесь порогове значення, яке вибирається виходячи з початкових умов.

Достатньою кодовою відстанню є половина довжини електронного підпису. У певних випадках може вибиратися інша довжина електронного підпису. Якщо кодова відстань задовольняє умові (5), то ми приймаємо рішення – прийняти даний електронний підпис, в іншому випадку – визнати його недійсним або підробленим.

Таким чином, запропонований алгоритм базується на використанні двійково-кодових послідовностей Хаффмана для прихованої передачі повідомлення, яке містить у собі електронний підпис, і при цьому забезпечує високу стійкість перед перешкодами. В ході дослідження проведено обчислювальні експерименти, які підтверджують працездатність представленого алгоритму [5].

Для оцінки працездатності алгоритмів формування та прийому повідомлень, які містять у собі електронний підпис, було проведено ряд експериментів, які мали на меті визначення оптимальної довжини повідомлення електронного підпису. Ця оптимальна довжина повинна при даному алгоритмі бути, з одного боку, якнайкоротшою, аби не було надлишковості, а з іншого – мати гарні показники розпізнавання під впливом на неї похибок.

Для цього було промодельовано весь алгоритм формування, передачі, прийому і розпізнання повідомлення електронного підпису для різних довжин повідомлення електронного підпису задля обрання найбільш оптимальної довжини для застосування на практиці.

Результати проведених експериментів наведено у табл. 1, що відображають яким чином довжина електронного підпису впливає на розпізнавання електронного підпису.

Таблиця 1 – Результати обчислювальних експериментів.

Довжина повідомлення електронного підпису	Кодова відстань	Кількість проведених експериментів	Ймовірність впливу похибки	Процент розпізнавання електронного підпису
10	5	10000	0	1
			0,005	0,9999
			0,01	0,9990
			0,015	0,9976
			0,02	0,9941
			0,05	0, 9819
			0,1	0, 9374
			0,15	0, 8645

Продовження таблиці 1

20	10	10000	0	1
			0,005	0,9999
			0,01	0,9992
			0,015	0, 9980
			0,02	0, 9959
			0,05	0, 9833
			0,1	0, 9411
			0,15	0, 8859
30	15	10000	0	1
			0,005	0,9999
			0,01	0, 9996
			0,015	0,9985
			0,02	0, 9969
			0,05	0, 9872
			0,1	0, 9539
			0,15	0, 9010
			0,015	0,9985
40	20	10000	0	1
			0,005	0, 9999
			0,01	0, 9996
			0,015	0,9987
			0,02	0, 9971
			0,05	0, 9875
			0,1	0, 9544
			0,15	0, 9023

Висновки. Проаналізувавши наведені результати можна виявити просту закономірність: більша довжина електронного підпису – вище ймовірність правильного розпізнавання повідомлення електронного підпису. Але, з іншого боку, необхідно пам’ятати, що безконтрольне збільшення довжини електронного підпису призводить, у свою чергу, до збільшення довжини несучої, в середньому в 30 разів, що підвищує надмірність передачі, і до того ж після деякої величини збільшення довжини втрачає сенс, бо процент вірного розпізнавання збільшується на декілька сотих, в той же час надмірність зростає у десятки разів.

Тому довжиною електронного підпису обрано довжину у 30 символів. Обрана довжина електронного підпису, з одного боку, гарантує високий процент розпізнавання, а з іншого – надає великої надмірності при передачі повідомлення, що містить у собі електронний підпис, по радіолініях зв’язку.

Бібліографічні посилання

1. Садомовский А. С., Воронов С. В. Радиотехнические системы передачи информации: учебное пособие. Ульяновск: УлГТУ, 2014. 120 с.

2. Акулиничев Ю. П., Бернгардт А. С. Теория и техника передачи информации: учебное пособие. Томск: Эль Контент, 2012. 210 с.

3. Першин В. Т. Основы современной радиоэлектроники: учебное пособие. Ростов н/Д: Феникс, 2009. 541 с.

4. Малайчук В. П. Основы теории кодирования и декодирования: учебное пособие. Дніпропетровськ: ДНУ имени Олеся Гончара, 2001. 68 с.

5. Березкин Е. Ф. Основы теории информации и кодирования: учебное пособие. Москва: НИЯУ МИФИ, 2010. 312 с.

Надійшла до редколегії 29.07.17.