УДК 681.32

Л. В. Крупельницький
В. П. Семеренко
О. І. Савчук

ЗАВАДОСТІЙКЕ КОДУВАННЯ ТА ЗАХИСТ ДАНИХ В СИСТЕМАХ ІДЕНТИФІКАЦІЇ ОБ'ЄКТІВ

Вінницький національний технічний університет

Анотація

Розроблена апаратна та програмна частини мікропроцесорної безпровідної системи обміну короткими кодовими повідомленнями через радіоканал. Запропоновано використання циклічних кодів для забезпечення завадостійкості та криптостійкості.

Ключові слова: криптографія, циклічні коди, радіопередача.

Abstract

The hardware and software components of a microprocessor wireless system for the exchange of short code messages through the radio channel have been developed. Cyclic codes for ensure noise immunity and cryptostability are suggected.

Keywords: cryptography, cyclic codes, radio broadcasting.

Найбільш поширені дві технічні галузі, які забезпечуть захист даних в різноманітних каналах передачі даних: криптографія та завадостійке кодування. Як правило, розглядають окремо принципи функціонування цих галузей.

Однак, при передачі даних по сучасним каналам зв'язку необхідно одночасно виконувати дві задачі: забезпечувати криптографічний захист даних та захист цих даних від атмосферних завад і несправностей апаратури. Тому необхідно розглядати криптографію і завадостійке кодування у їх тісній взаємодії.

Ці дві технічні галузі мають багато взаємних відмінностей: відносно параметрів вхідних і вихідних повідомлень, вимог складності та часу відновлення вхідних повідомлень, типів математичних перетворень. Однак є також багато у них і спільного. Недаремно ці галузі мають одного основоположника – К. Шеннона [1].

В своїх роботах видатний американський вчений довів можливість створення як досконалого шифру, що не піддається зламу, так і ідеального коду, який дає змогу передавати інформацію із як завгодно малою ймовірністю похибки.

Теореми К.Шеннона не дають відповіді про способи побудови конкретних кодів та шифрів, вони є лише теоретичним підґрунтям для інженерних розробок. Розглянемо можливість одночасного виконання операцій криптографії та завадостійкого кодування в системах персональної ідентифікації людей або матеріальних об'єктів на місцевості [2].

Першою теоретичною проблемою, яку необхідно розв'язати – це оптимальний вибір математичного аппарату. Внаслідок відокремленого розвитку зазначених галузей вони базуються переважно на різних теоретичних моделях.

Обмежимость лише одним класом завадостійких кодів – циклічними кодами, і одним алгоритмом шифрування – потоковим шифруванням [3]. В цьому випадку можна інтегрувати криптографію та завадостійке кодування за допомогою єдиного математичного апарату – теорії лінійних послідовнісних схем (ЛПС) [4]. ЛПС, як лінійний автомат в двійковому полі Галуа, в дискретні моменти часу t задається функцією переходів (станів)

$$S(t+1) = A \times S(t) + B \times U(t), \quad GF(2),$$

та функцією виходів

$$Y(t) = C \times S(t) + D \times U(t), \quad GF(2),$$

де A, B, C, D – характеристичні матриці ЛПС, S, U, Y – слова стану, вхідне, вихідне.

На основі теорії ЛПС розроблені пристрій, програма криптографічного та завадостійкого захисту даних під час передавання даних по радіоканалу.

Функціональна схема пристрою, яка наведена на рисунку 1, складається з радіомодуля НС-12, мікроконтролера, індикації та пристрою введення.

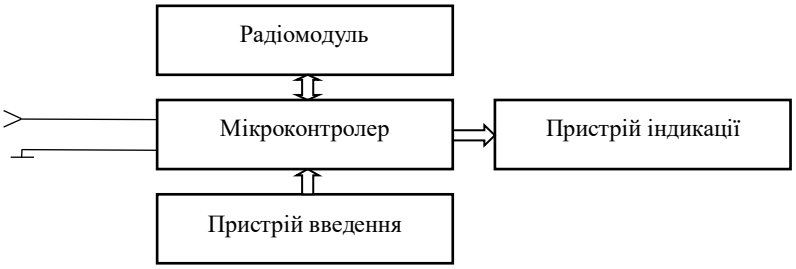

Рисунок 1 – Функціональна схема пристрою ідентифікації

Пристрій введення являє собою блок кнопок, кожній з яких відповідає певна команда (зашифроване повідомлення). Мікроконтролер, отримавши повідомлення від пристрою, декодує, дешифрує та порівнює його з наперед визначеним набором повідомлень. При збігу команди відбувається певна запланована реакція. На пристрої індикації, який складається з набору світлодіодів, відображається стан «Тривога», «Перевірка» та автоматично відправляється відповідь на запит.

На приладі адміністратора є набір кнопок для кожного пристрою та додаткові можливості: блокування модуля користувача, який був втрачений, зміна паролю.

Ініціатором сесії зв'язку може виступати як користувач, так і адміністратор або працювати в автоматичному режимі.

У результаті розробки отримано пристрої, здатні обмінюватись короткими, захищеними повідомленнями через радіоканал зв'язку.

Перспективою на майбутнє є розробка програмного забезпечення для ПК, що дасть можливість управляти даними пристроями, змінювати характеристики шифрування повідомлень.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Шеннон К. Работы по теории информации и кибернетике / К. Шеннон – М. : Изд-во иностр. лит., 1963. – 829 с.
2. Овчинников С.В. Системы позиционирования и мониторинга / С.В. Овчинников // Технологии и средства связи. – 2014. – № 2. – С. 18–22.
3. Семеренко В.П. Интегрированная защита информации: криптография плюс помехоустойчивое кодирование/ В.П. Семеренко // Захист інформації. – 2011. – № 3. – С. 44-52.
4. Семеренко В. П. Теорія циклічних кодів на основі автоматних моделей : монографія / В. П. Семеренко. – Вінниця : ВНТУ, 2015. – 444 с.

Леонід Віталійович Крупельницький – канд. техн. наук, доцент, зам. зав. кафедри обчислювальної техніки, Вінницький національний технічний університет, Вінниця.

Василь Петрович Семеренко – канд. техн. наук, доцент кафедри обчислювальної техніки, Вінницький національний технічний університет, Вінниця, e-mail: vasilsemerenko@gmail.com

Олександр Ігорович Савчук – студент групи 1КІ-17м, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця

Leonid V. Krupelnytskyi – PhD, Associate Professor, vice-head of the Department of computer technique, Vinnytsia National Technical University, Vinnytsia.

Vasyl P. Semerenko – PhD, Associate Professor, Department of computer technique, Vinnytsia National Technical University, Vinnytsia, e-mail: vasilsemerenko@gmail.com

Oleksandr I. Savchuk – student, Department of computer technique, Vinnytsia National Technical University Vinnytsia.