УДК 519.725 DOI: 10.30748/nitps.2021.45.13

О.М. Бітченко, Л.Ф. Сайківська, О.І. Цопа, А.О. Мерзлікін

*Харківський національний університет радіоелектроніки, Харків*

# МЕТОД ПІДВИЩЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ В НЕАЛГЕБРАЇЧНИХ ДЕКОДЕРАХ МЕГГІТА ПРИ НЕСАНКЦІОНОВАНОМУ ЇЇ ПЕРЕХОПЛЕННІ

*Робота присвячена вдосконаленню структури неалгебраїчного декодера, що дозволяє підвищити захист інформації при несанкціонованому її перехопленні, шляхом введення додаткових синдромних регістрів зсуву зі зворотними зв'язками та блоку управління цими регістрами. У статті детально описано принцип роботи декодера, обумовлено введення синдромних регістрів зсуву зі зворотними зв'язками та показано, що така структура дозволяє за законом випадкових чисел постійно змінювати вид утворюючого полінома і тим самим суттєво зменшити вірогідність правильного декодування інформаційної посилки при її перехопленні.*

***Ключові слова:*** *неалгебраїчний декодер, декодер Меггіта, синдромний регістр зсуву, коригувальні коди, захист інформації від перехоплень.*

## Вступ

**Постановка проблеми.** Будь-яка інформаційно-комунікаційна система повинна забезпечувати передачу інформації з високою швидкістю та її вірогідністю в умовах завад на лініях зв'язку. Крім того, вона повинна забезпечувати захист інформації від несанкціонованих перехоплень зловмисниками. Але жодна система захисту не може довгий час протистояти цілеспрямованим діям озброєного сучасними технологіями кваліфікованого порушника через наявність в них тих чи інших каналів витоку інформації.

Залежно до способів перехоплення інформації, а також середовища розповсюдження, канали витоку та перехоплення інформації можна розділити на електромагнітні, електричні, акустичні, індукційні тощо.

Метою захисту інформації є унеможливлення або суттєве утруднення реалізації загроз для інформації.

При завадостійкому кодуванні в потік переданих символів вводяться додаткові (надлишкові) символи для виправлення на приймальній стороні помилок, що виникають. Це вимагає збільшення швидкості передачі по каналу, що еквівалентно розширенню смуги частот сигналу і зменшення енергії посилки.

Проте, надлишкове кодування стало широко застосовуватися з метою підвищення якості передачі, переважно в останні десятиліття, коли проблема створення складних обчислювальних пристроїв в малих габаритах була практично вирішена [4; 8].

При побудові систем кодування-декодування використовуються спеціальні коди, такі як коди Хемінга, коди Боуза-Чоудхурі-Хоквінгема (БЧХ), коди Голея, мажоритарні коди, ітеративні коди, систематичні і несистематичні згорткові коди тощо [6–7; 10–12]. Ці коди можуть мати різну довжину кодового слова $\tilde{C}(x)$ , що складається з інформаційної групи $i(x)$ і декількох надлишкових розрядів та різну кодову відстань *d*, від якої залежить кількість можливих виправлених помилок. Тип коду визначає принцип, за яким вносяться надлишкові символи [1; 8].

**Аналіз останніх досліджень і публікацій.** В роботі [2] описано неалгебраїчний декодер Меггіта для декодування кодових слів досконалого коду Голея, що включає додатково коригувальну схему, керовану керуючою схемою й з'єднану з *k* розрядами (тригерами) зсувного буферного регістра (синдромного декодера), що дозволяє в 1,5 рази підвищити швидкість декодування.

Недоліком даного пристрою є неможливість повної обробки несистематичних кодових слів без додаткового пристрою-виділювача з них інформаційних груп та низький рівень захисту від перехоплень.

В роботі [3] описано синдромний декодер для несистематичного (15, 11) коду Хеммінга що містить 4-розрядний синдромний регістр зі зворотними зв'язками, пристрій зберігання всіх синдромів з організацією 16 кодових слів по 15 бітів кожне, два 15-бітових зсувних регістри, суматор за модулем два (коректор помилок), пристрій виділення інформаційної групи $i(x)$ з оцінки кодового слова $\tilde{C}(x)$ на виході декодера й регістр, що являє собою зсувний регістр зі зворотними зв'язками (цифровий фільтр).

Недоліками пристрою є складність схеми декодера для несистематичного коду за рахунок приєднання до нього пристрою виділення інформаційної групи (цифрового фільтра-дільника), вузька межа використання декодера, великий час обробки кодових слів та низький рівень захисту від перехоплень.

В роботі [4] описано неалгебраїчний декодер коригувальних кодів, в якому за допомогою введен-

ня додаткових ключів як пристрій виділення інформаційної групи використовується синдромний регістр зсуву зі зворотними зв'язками.

Але при практичних дослідженнях роботи цього декодера було виявлено його суттєвий недолік, який полягає в тому, що при деяких комбінаціях прийнятої посилки (від восьми до десяти відсотків можливих комбінацій), декодер не виявляє та не виправляє помилки.

В роботі [5] описано метод підвищення ефективності неалгебраїчного декодера коректуючих кодів системи зв'язку в якому, шляхом введення блоків додаткової перевірки, вирішено проблему не виявлення та не виправлення помилок при деяких комбінаціях прийнятої посилки.

Але і цей декодер, як і всі описані вище, не захищений від несанкціонованого перехоплення інформації.

**Мета статті** – розробка методу підвищення захисту інформації при її несанкціонованому перехопленні.

## Виклад основного матеріалу

З метою вирішення поставленої задачі в даній роботі пропонується пристрій, побудований на основі декодера, описаного в роботі [5]. Структурну схему пропонованого декодера наведено на рис. 1.

Неалгебраїчний декодер з підвищеним захистом інформації при її перехопленні містить неалгебраїчний декодер коригувальних кодів, реалізований за схемою прототипу, блок додаткових синдромних (*n-k*)-розрядних регістрів зсуву зі зворотними зв'язками та блок управління синдромними (*n-k*)-розрядними регістрами зсуву зі зворотними зв'язками.

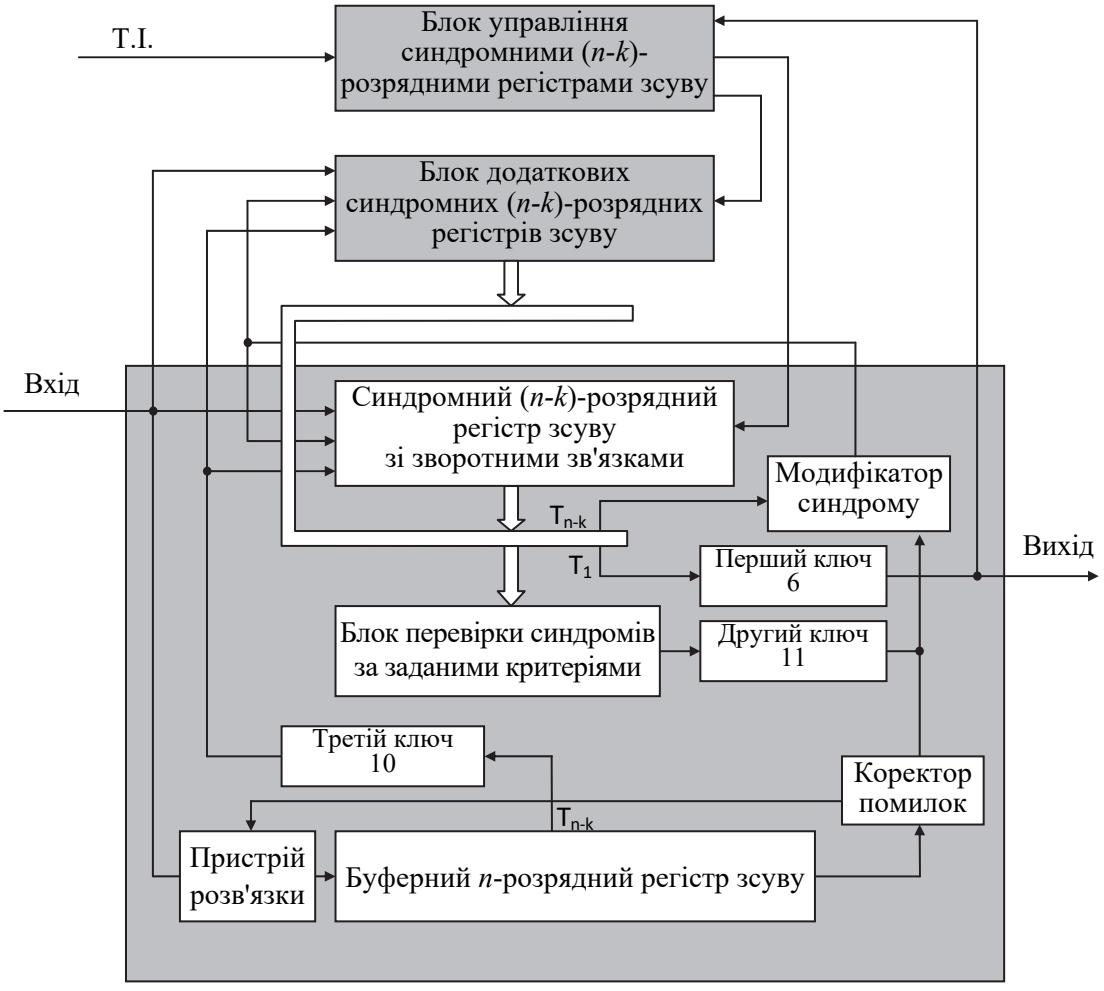


Рис. 1. Декодер Меггіта з підвищеним захистом інформації при її перехопленні
Джерело: розроблено авторами за даними [5].

Декодер працює у такий спосіб.

Попередньо всі блоки неалгебраїчного декодера коригувальних кодів, блоку додаткових синдромних *(n-k)*-розрядних регістрів зсуву зі зворотними зв'язками та блоку управління синдромними (*n-k*)-розрядними регістрами зсуву зі зворотними зв'язками обнулені. Вхідне кодове слово $v(x)$, можливо уражене перешкодами в каналі зв'язку (тобто з помилками), послідовно подається на перший вхід синдромного (*n-k*)-розрядного регістра зсуву зі зво-

ротними зв'язками, де $n$ – довжина кодового слова, а $k$ – довжина інформаційної частини кодового слова і, через пристрій розв'язки, на вхід буферного $n$-розрядного регістра зсуву. Декодер обробляє вхідні кодові слова за три цикли роботи з $n$ часових тактів у кожнім циклі.

Протягом 1-го циклу роботи у синдромному регістрі зсуву зі зворотними зв'язками формується синдром, а буферний $n$-розрядний регістр зсуву послідовно заповнюється символами кодового слова $v(x)$, що надходить на вхід декодера. Оскільки синдром, по визначенню, є залишком від ділення $v(x)$ на утворюючий поліном $g(x)$, то синдромний регістр зсуву зі зворотними зв'язками, структура якого задається структурою $g(x)$, є цифровим фільтром інформаційних груп.

На цьому циклі другий ключ розімкнутий, а тому стан виходу логічного блоку перевірки синдромів за заданими критеріями не аналізується. Якщо продекодоване кодове слово $c(x)$ не має помилок, то $v(x) = c(x)$, до кінця 1-го циклу роботи синдромний регістр зсуву зі зворотними зв'язками обнуляється. У випадку наявності помилок у кодовому слові, що надходить на декодер, $v(x) \neq c(x)$, то до кінця 1-го циклу роботи на виході синдромного регістра зсуву формується деяка кодова комбінація. Протягом 1-го циклу роботи перший та третій ключі також розімкнуті.

З початком 2-го циклу роботи другий ключ замикається і логічний блок перевірки синдромів на кожному такті аналізує кодові комбінації на виходах осередків синдромного регістра зсуву зі зворотними зв'язками. Такий аналіз відбувається шляхом одержання відповідей по двох критеріях:

1. У старшому розряді синдромного регістра зсуву зі зворотними зв'язками присутня логічна одиниця?

2. Сума логічних одиниць в інших розрядах менше або дорівнює двом?

Тільки при позитивній відповіді на обидва ці питання на виході логічного блоку перевірки синдромів 7 формується сигнал логічної одиниці, що надходить на коректор помилок і модифікатор синдрому, виправляючи на наступному такті помилку в буферному регістрі і модифікуючи синдром, перетворюючи в "0" сигнал зворотного зв'язку в синдромному регістрі зсуву зі зворотними зв'язками.

За час 2-го циклу роботи перший і третій ключі розімкнуті. У результаті вхідна послідовність $v(x)$ примусово повторно проходить осередки буферного $n$-розрядного регістра зсуву, що забезпечує скорочення відстані між широко розташованими помилками (більше ніж $n$-$k$ біт) і дозволяє обробляти і виправляти їх.

На третьому циклі роботи, функціонування декодера залежить від способу формування кодових слів.

У випадку формування кодового слова систематичним методом другий ключ замкнутий, третій ключ розімкнутий, перший ключ замкнутий протягом перших $k$ тактів, пропускаючи на "Вихід" інформаційну групу $i(x)$, після чого розмикається.

У випадку формування кодового слова несистематичним методом, починаючи з ($n$-$k$)-го такту цього циклу розмикається другий ключ, а перший і третій ключі замикаються. При цьому, з виходу $T_{n-k}$ буферного регістра зсуву подається прийнята кодова послідовність $c(x)$ з виправленими помилками на вхід синдромного регістра зсуву зі зворотними зв'язками, а з виходу першого тригера цього регістра знімається виділена інформаційна послідовність $i(x)$, яка через перший ключ передається на "Вихід".

З метою захисту переданої інформації від ймовірного несанкціонованого перехоплення в пропонованому декодері використовуються декілька синдромних регістрів зсуву зі зворотними зв'язками, місця розташування яких визначаються структурою утворюючого поліному.

Структурна схема блока додаткових синдромних регістрів наведена на рис. 2. Блок додаткових синдромних ($n$-$k$)-розрядних регістрів зсуву зі зворотними зв'язками (рис. 3) містить перший, другий та $m$-й синдромний ($n$-$k$)-розрядний регістр зсуву зі зворотними зв'язками, реалізованими з різними структурами утворюючих поліномів $g(x)$, перші, другі та треті входи та виходи кожного розряду усіх додаткових синдромних регістрів зсуву зі зворотними зв'язками з'єднані між собою та з відповідними входами і виходами синдромного ($n$-$k$)-розрядного регістру зсуву зі зворотними зв'язками неалгебраїчного декодера коригувальних кодів. Четверті входи є входами дозволу роботи обраного синдромного ($n$-$k$)-розрядного регістра зсуву зі зворотними зв'язками.

Синдромні регістри зсуву зі зворотними зв'язками реалізуються на D-тригерах з трьома станами на виході. Місця розташування зворотних зв'язків визначаються структурою утворюючого поліному [8–9].

Функціональна схема синдромного регістра зсуву для випадку використання бінарного коду Голея (23,12,7), для якого описана робота пристрою, і утворюючого полінома $g(x)=x^{11}+x^{10}+x^6+x^5+x^4+x^2+1$, наведена на рис. 3.

Вибір того або іншого синдромного регістру зсуву зі зворотними зв'язками забезпечується блоком управління цими регістрами. Функціональна схема блока управління синдромними регістрами наведена на рис. 4.

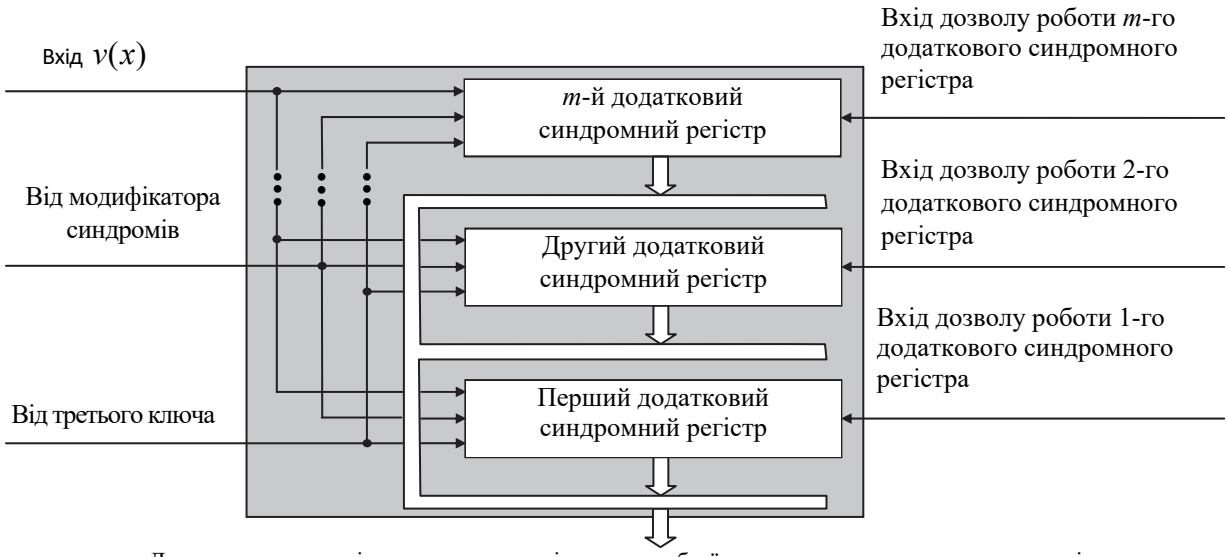


Рис. 2. Блок додаткових синдромних ($n$-$k$)-розрядних регістрів зсуву
Джерело: розроблено авторами.

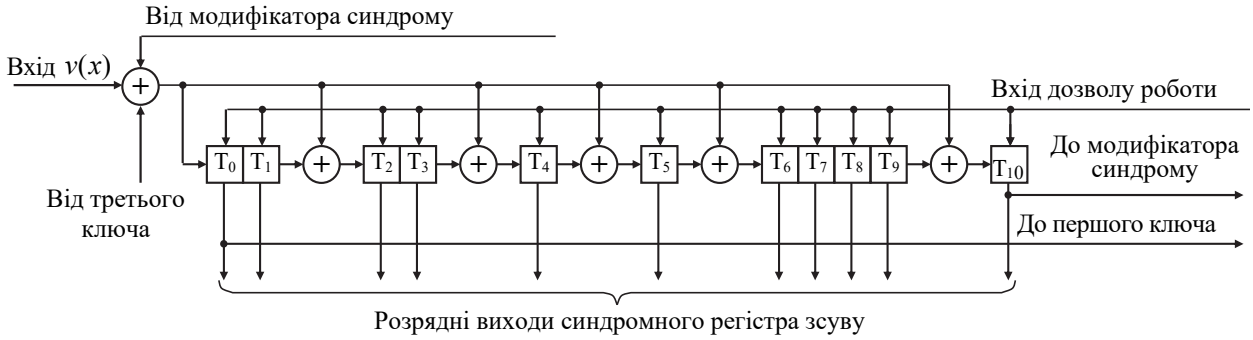


Рис. 3. Функціональна схема синдромного регістра зсуву
Джерело: [5].

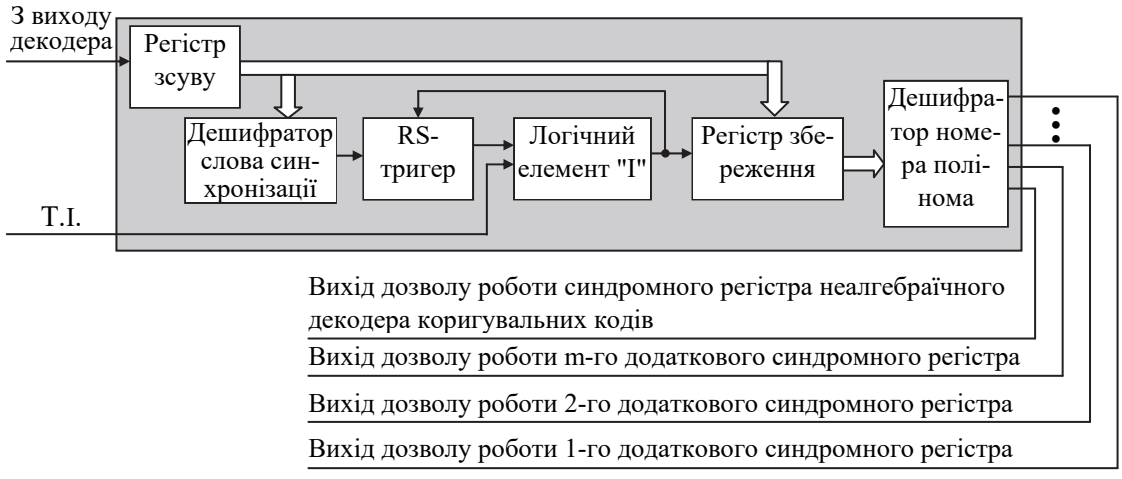


Рис. 4. Блок управління синдромними ($n$-$k$)-розрядними регістрами зсуву
Джерело: розроблено авторами.

Блок управління синдромними ($n$-$k$)-розрядними регістрами зсуву зі зворотними зв'язками містить регістр зсуву, дешифратор слова синхронізації, RS-тригер, логічний елемент "І", регістр збереження та дешифратор номера полінома.

Робота блока управління синдромними регістрами здійснюється відповідно до часових діаграм, наведених на рис. 5.

В довільний момент часу з передавального пристрою на декодер поступає слово синхронізації, а за ним код номера синдромного регістра зсуву зі зворотними зв'язками, який буде використовуватись при наступній серії інформаційних посилок. Блок управління, при одержанні слова синхронізації, приймає код номера синдромного регістра зсуву зі зворотними зв'язками і виробляє сигнал дозволу роботи відповідного синдромного регістра зсуву зі зворотними зв'язками декодера.

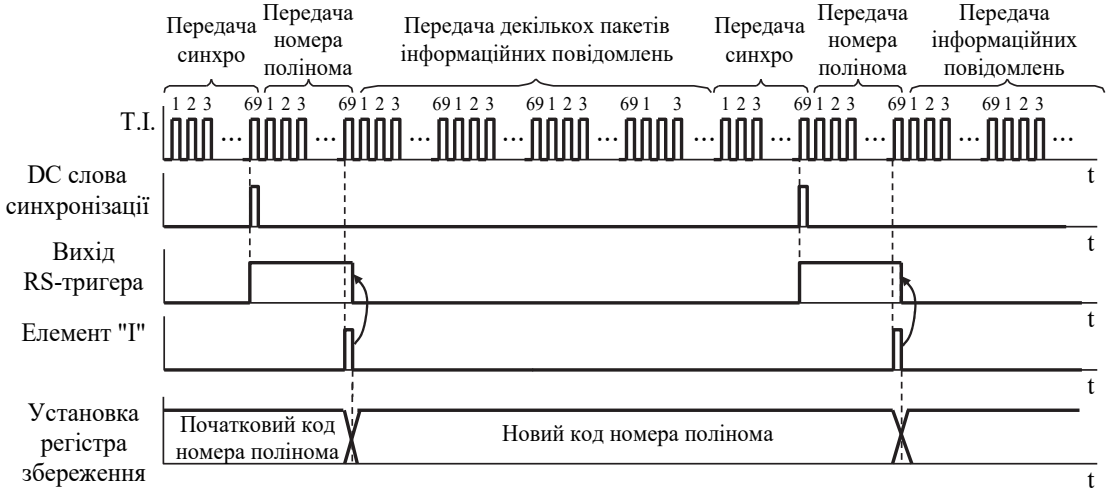


Рис. 5. Часові діаграми роботи блока управління
Джерело: розроблено авторами.

## Висновки

Зважаючи на наявність каналів витоку інформації, унеможливити її перехоплення практично неможливо. Але саме перехоплення повинне супроводжуватись правильним декодуванням цієї інформації. В деякій мірі цю задачу вирішує застосування того чи іншого виду кодера-декодера, виду застосованого коду, його довжини та виду утворюючого полінома.

Але при тривалому спостереженні за конкретною системою передачі та наявності сучасної обчислювальної техніки можна підібрати і вид застосованого декодера, і довжину інформаційного слова, і утворюючий поліном.

Запропонований метод ведення в декодер додаткових синдромних ($n$-$k$)-розрядних регістрів зсуву зі зворотними зв'язками та блоку управління цими регістрами дозволяє за законом випадкових чисел постійно змінювати вид утворюючого полінома і тим самим суттєво зменшити вірогідність декодування інформаційної посилки при її перехопленні.

## Список літератури

1. Золотарев В. В., Овечкин Г. В. Помехоустойчивое кодирование. Методы и алгоритмы. Справочник / под ред. Ю. Б. Зубарева. Москва : Горячая линия-Телеком, 2004. 126 с.

2. Неалгебраический декодер: пат. RU №85778. № 2009112662/22; заявл. 06.04.2009; опубл. 10.08.2009, 4 с.

3. Блейхут Р. Теория и практика кодов, контролирующих ошибки / Пер. с англ. И. И. Грушко, В. М. Блиновского под ред. К. Ш. Зигангирова. Москва : Мир, 1986. 576 с.

4. Бітченко О., Макаров Л., Цопа О., Коняхін Г. Неалгебраїчний декодер коригувальних кодів. *Радиотехника. Всеукраинский межведомственный научно-технический сборник.* 2013. № 172. С. 134-140.

5. Битченко А., Макаров Л., Цопа А., Ганшин Д. Метод повышения эффективности неалгебраического декодера корректирующих кодов системы связи. *Радиотехника. Всеукраинский межведомственный научно-технический сборник.* 2014. № 178. С. 31-40.

6. Кларк Дж., Кейн Дж. Кодирование с исправлением ошибок в системах цифровой связи / Пер. с англ. под ред. Б. С. Цыбакова. Москва : Радио и связь, 1987. 392 с.

7. Золотарѐв В. В., Овечкин Г. В., Зубарев Ю. Б., Левин В. К. Многопороговые декодеры и оптимизационная теория кодирования. Москва : Горячая линия - Телеком, 2012. 239 с.

8. Макаров Л. Б., Битченко А. Н., Коняхин Г. Ф., Коваленко Н. А. Синтез инверсных пороговых схем для реализации в неалгебраических декодерах корректирующих кодов. *Системи обробки інформації.* 2011. № 8(98). С. 87-92.

9. Проектирование импульсных и цифровых устройств радиотехнических систем: учеб. пособие для радиотехнич. спец. вузов / Гришин Ю. П. и др. / под ред. Ю. М. Казаринова. Москва : Высшая. школа, 1985. 319 с.

10. Пороговый декодер сверточного кода: А.С. 964999 СССР, Н 04 L 1/10; заявл. 16.03.81; опубл. 7.10.82, 9 с.

11. Золотарев В. В. Теория и алгоритмы многопорогового декодирования / под ред. Ю. Б. Зубарева. Москва : Радио и связь, Горячая линия – Телеком, 2006. 232 с.

12. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки / Пер. с англ. под ред. Р. Л. Добрушина. Москва : Мир, 1976. 594 с.

*Надійшла до редколегії 07.09.2021*
*Схвалена до друку 16.11.2021*

***Відомості про авторів:***

**Бітченко Олександр Миколайович**
кандидат технічних наук доцент
доцент Харківського національного
університету радіоелектроніки,
Харків, Україна
https://orcid.org/0000-0002-4561-1046

**Сайківська Лілія Федорівна**
кандидат технічних наук доцент
доцент Харківського національного
університету радіоелектроніки,
Харків, Україна
https://orcid.org/0000-0002-4139-7732

**Цопа Олександр Іванович**
доктор технічних наук професор
завідувач кафедрою Харківського національного
університету радіоелектроніки,
Харків, Україна
https://orcid.org/0000-0002-4881-5343

**Мерзлікін Анатолій Олександрович**
асистент
Харківського національного
університету радіоелектроніки,
Харків, Україна
https://orcid.org/0000-0003-1604-8837

***Information about the authors:***

**Oleksandr Bitchenko**
PhD in Engineering Associate Professor
Associate Professor of Kharkiv National
University of Radio Electronics,
Kharkiv, Ukraine
https://orcid.org/0000-0002-4561-1046

**Liliia Saikivska**
PhD in Engineering Associate Professor
Associate Professor of Kharkiv National
University of Radio Electronics,
Kharkiv, Ukraine
https://orcid.org/0000-0002-4139-7732

**Oleksandr Tsopa**
Doctor of Engineering Science Professor
Head of Department of Kharkiv National
University of Radio Electronics,
Kharkiv, Ukraine
https://orcid.org/0000-0002-4881-5343

**Anatolii Merzlikin**
Assistant Lecturer
of Kharkiv National
University of Radio Electronics,
Kharkiv, Ukraine
https://orcid.org/0000-0003-1604-8837

## МЕТОД ПОВЫШЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ В НЕАЛГЕБРАИЧЕСКИХ ДЕКОДЕРАХ МЕГГИТА ПРИ НЕСАНКЦИОНИРОВАННОМ ЕЕ ПЕРЕХВАТЕ

А.Н. Битченко, Л.Ф. Сайковская, А.И. Цопа, А.А. Мерзликин

*Работа посвящена усовершенствованию структуры неалгебраического декодера, что позволит повысить защиту информации от перехвата путем введения дополнительных синдромных регистров сдвига с обратными связями и блока управления этими регистрами. В статье подробно описан принцип работы декодера, обусловлено введение синдромных регистров сдвига с обратными связями и показано, что такая структура позволяет по закону случайных чисел постоянно менять вид образующего полинома и тем самым существенно уменьшить вероятность правильного декодирования информационной посылки при ее перехвате.*

***Ключевые слова:*** *неалгебраический декодер, декодер Меггита, синдромный регистр сдвига, корректирующие коды, защита информации от перехвата.*

## METHOD OF INCREASING PROTECTION OF INFORMATION IN NON-ALGEBRAIC DECODERS OF MEGGIT WITH UNAUTHORIZED INTERCEPTION

O. Bitchenko, L. Saikivska, O. Tsopa, A. Merzlikin

*The work is devoted to the improvement of the non-algebraic Meggit decoder, which will increase the protection of information from interception by introducing additional syndromic feelback shift registers and a register control unit. Existing developments have such faults as the complexity of the decoder circuit for non-systematic code, the impossibility of full processing of non-systematic code words without an additional extraction device from them information groups, low level of protection against interception, non-detection and non-correction of errors for some combinations of received parcels. Therefore, the aim of the work was to increase the protection of information from interception by some complication of the hardware of the decoder. The article describes in detail the structure and working principle of the proposed Meggit decoder with increased protection against interception. It is proposed to add to the existing prototype a block of additional syndromic (n-k) -bit feelback shift registers and a register control unit. Several syndromic feelback shift registers are used in the proposed decoder to improve the protection of information from possible unauthorized interception. They are implemented on D-flip-flops with three states at the output, and the locations of the feedback are determined by the structure of the forming polynomial. The functional diagram of the syndromic shift register for the case of using the Goley binary code (23,12,7), the block diagram of the syndromic (n-k) -bit shift register control unit and the principle of its operation are described in the article. The proposed structure allows to constantly change the generating polynomial view according to the law of random numbers and by that essentially to reduce probability of correct decoding of an information parcel at its interception.*

***Keywords:*** *non-algebraic decoder, Meggit decoder, syndromic shift register, corrective codes, information protection from interception.*