Министерство образования Республики Беларусь
учреждение образования
«Белорусский государственный университет информатики
и радиоэлектроники»

# ТЕЛЕКОММУНИКАЦИИ: СЕТИ И ТЕХНОЛОГИИ, АЛГЕБРАИЧЕСКОЕ КОДИРОВАНИЕ И БЕЗОПАСНОСТЬ ДАННЫХ

МАТЕРИАЛЫ МЕЖДУНАРОДНОГО НАУЧНО-ТЕХНИЧЕСКОГО СЕМИНАРА
(Минск, ноябрь – декабрь 2021 г.)

# TELECOMMUNICATIONS: NETWORKS AND TECHNOLOGIES, ALGEBRAIC CODING AND DATA SECURITY

Минск, 2021

УДК 654:004.056
ББК 32.88+32.971.35-5
Т31



Т31 **Телекоммуникации**: сети и технологии, алгебраическое кодирование и безопасность данных : материалы Международного научно-технического семинара (Минск, ноябрь – декабрь 2021 г.) Telecommunications: Networks and Technologies, Algebraic Coding and Data Security – Минск : БГУИР, 2021. – 80 с.

ISBN 978-985-488-834-7.

Сборник содержит статьи, тематика которых посвящена научно-теоретическим разработкам в области сетей телекоммуникаций, информационной безопасности, алгебраического кодирования и обработки изображений.

Предназначен для научных сотрудников в области телекоммуникаций, преподавателей, аспирантов, магистрантов и студентов технических вузов.

*Научное издание*

Корректор *В.В. Чепикова*
Ответственный за выпуск *В.Ю. Цветков*
Компьютерный дизайн и верстка *Е.Г. Макейчик*

Подписано в печать 08.12.2021. Формат 60×84 ⅛. Бумага офсетная. Гарнитура «Таймс». Отпечатано на ризографе. Усл. печ. л. 10,46. Уч.-изд. л. 8,9. Тираж 50 экз. Заказ 760.

Издатель и полиграфическое исполнение: учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники»
ЛИ №02330/264 от 14.04.2014. ЛП №02330/0494175 от 03.04.2009.
220013, Минск, П. Бровки, 6

**ISBN 978-985-488-834-7** 

**СОДЕРЖАНИЕ**

**CONTENTS**

*УДК 621.391*

# КОМПАКТНОЕ ПРЕДСТАВЛЕНИЕ ИЗОБРАЖЕНИЙ С ШИРОКИМ ДИНАМИЧЕСКИМ НА ОСНОВЕ БЕССЕТОЧНОЙ АППРОКСИМАЦИИ ОБЛАСТЕЙ ЛОКАЛЬНЫХ ЭКСТРЕМУМОВ

А.Т. НГУЕН, В.Ю. ЦВЕТКОВ

*Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь*

*Поступила в редакцию 1 ноября 2021*

**Аннотация.** Для компактного представления изображений с широким динамическим диапазоном предложен алгоритм на основе бессеточной аппроксимации областей локальных экстремумов с монотонным изменением яркости с использованием ограниченного набора перестраиваемых примитивов. Проведено сравнение результатов аппроксимации с помощью предложенного алгоритма и вейвлет-преобразования.

*Ключевые слова*: компактное представление изображений, бессеточная аппроксимация изображений, области локальных экстремумов с монотонным изменением яркости.

## Введение

Изображения с широким динамическим диапазоном широко используются в системах технического зрения. Из-за большого объема данных актуальной является задача их компактного представления. Наряду с классическими подходами к сжатию таких изображений возможно также использование аппроксимации их областей с монотонным изменением яркости с помощью простых двухмерных функций с перестраиваемыми параметрами. В качестве таких функций могут использоваться глобальные функции IQ (Inverse Quadric), относящиеся к радиальным базисным функциям RBF (RBF – Radial Basic Function) [1–4]. Для аппроксимации явных функций двух переменных на основе RBF возможен бессеточный подход. Ключевым моментом аппроксимации на основе RBF является поиск базовых точек, которые дают хорошее приближение с высокой точностью. В качестве таких точек могут использоваться локальные экстремумы, а также дополнительные пиксели при недостаточной точности [5–8]. Для аппроксимации на основе RBF необходимо решение системы линейных уравнений.

Цель работы: повышение компактности представления полутоновых изображений с широким динамическим диапазоном.

## Алгоритм компактного представления изображений с широким динамическим диапазоном

Для компактного представления полутоновых изображений с широким динамическим диапазоном предлагается использовать бессеточную аппроксимацию областей локальных экстремумов с монотонным изменением яркости на основе ограниченного набора перестраиваемых примитивов. При бессеточной аппроксимации изображения каждая его область с монотонным изменением яркости рассматривается как выпуклая или вогнутая двумерная функция яркости в пространстве пикселей, для которой может быть подобрана с некоторой точностью соответствующая простая монотонная математическая функция. Компактность описания изображения достигается за счет уменьшения объема информации, представляющей коэффициенты преобразования: положение областей локальных экстремумов и параметры аппроксимирующих эти области функций. Для поиска и выделения областей локальных экстремумов с монотонным изменением яркости используются алгоритмы, предложенные в [9, 10].

На вход схемы компактного представления (рис. 1) поступает исходное полутоновое изображение $A(0)$. На выходах НЧ-фильтров формируются отфильтрованные изображения $A(n)_{n=\overline{1,N}}$, используемые для поиска необходимых примитивов $C_{SI}(n)_{n=\overline{1,N-1}}$ на разных уровнях пространственной фильтрации (преобразования). Для интерполяции изображения $SI\left(C_{SI}(n)\right)_{n=\overline{N,1}}$ на основе набора примитивов $C_{SI}(n)_{n=\overline{N,1}}$ используются глобальные функции IQ и бессеточный подход к аппроксимации на основе RBF.

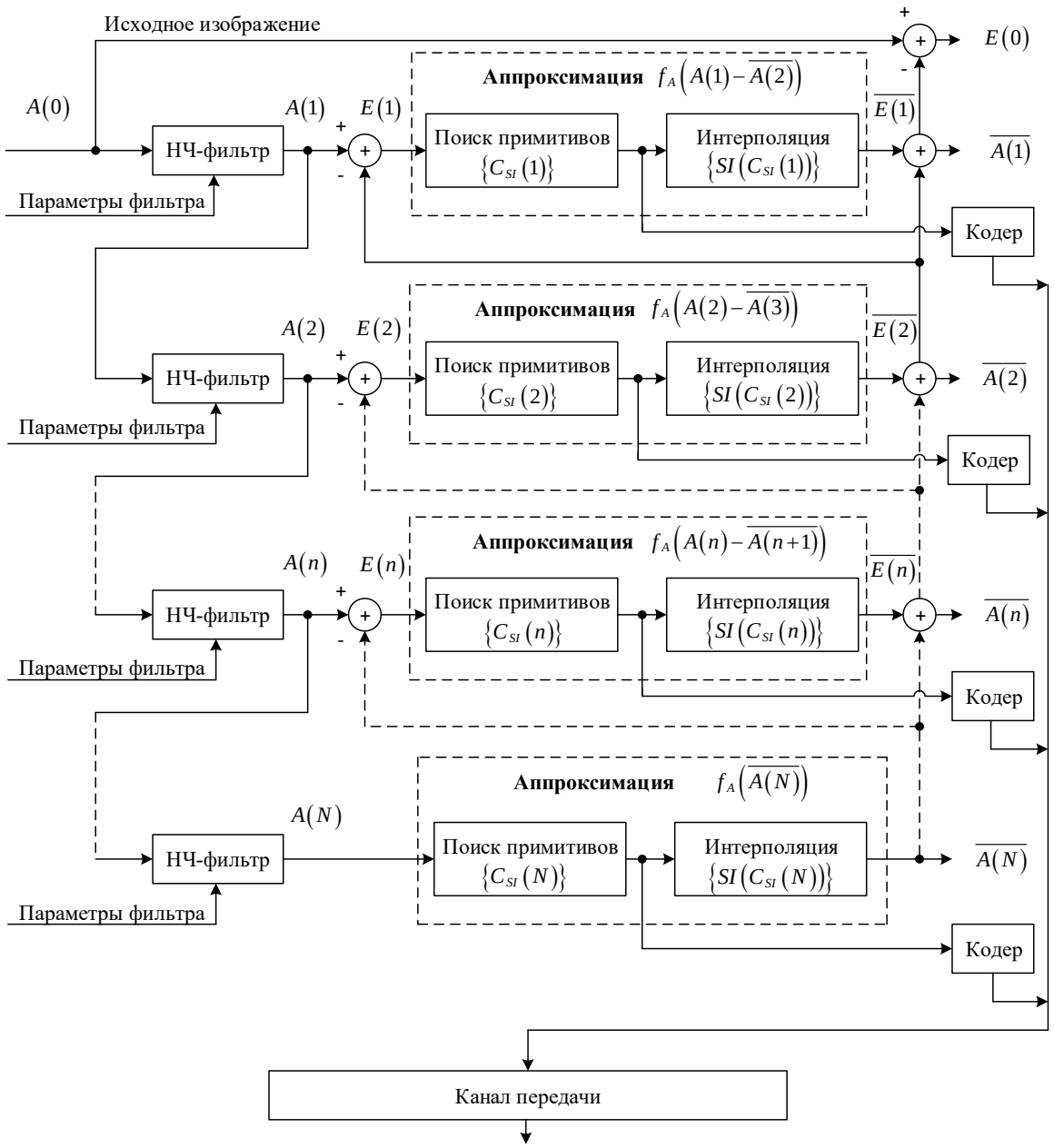



Рис. 1. Схема компактного представления изображений на основе ограниченного набора аппроксимирующих перестраиваемых примитивов

При последующем синтезе, приближение $\overline{A(n)}$ последовательности приближений $\overline{A(n)}_{n=\overline{N,1}}$ исходного изображения $A(0)$ рекурсивно вычисляется по следующей многоуровневой схемы интерполяции:

$$E(n)=A(n)-\overline{A(n+1)}, \qquad (1)$$

$$\overline{E(n)} = f_A\left(E(n)\right) = f_A\left(A(n) - \overline{A(n+1)}\right) = SI\left(C_{SI}(n)\right), \quad (2)$$

$$\overline{A(n)} = \overline{A(n+1)} + \overline{E(n)}, \quad (3)$$

$$A(0) = \overline{A(N)} + \overline{E(N-1)} + \ldots + \overline{E(n)} + \ldots + \overline{E(1)} + E(0), \quad (4)$$

где $E(n)$ – изображение ошибок *n*-ого уровня; $f_A\left(E(n)\right)$ – функция аппроксимации изображения $E(n)$ ошибок *n*-ого уровня; $\overline{A(N)}$ – приближение (низкочастотная информация) исходного изображения $A(0)$; $\overline{E(n)}$ – интерполированное изображение ошибок *n*-ого уровня; $E(0)$ – итоговая ошибка.

Набор примитивов $C_{SI}(n)_{n=\overline{N,1}}$, полученных на выходе блоков поиска примитивов последовательно поступает на вход кодера для последующего сжатия с помощью подходящих алгоритмов эффективного кодирования изображений.

**Оценка эффективности работы алгоритмов преобразования динамического диапазона**

Произведена оценка эффективности используемого подхода к представлению изображения на основе бессеточной аппроксимации с использованием ограниченного набора перестраиваемых примитивов относительно вейвлет-преобразования, а также влияния точности выделения областей локальных экстремумов различными алгоритмами на компактность представления изображения. Компактность представления оценена по энергии коэффициентов преобразования (сумма модулей значений коэффициентов) на всех уровнях вейвлет-разложения и бессеточной аппроксимации с использованием ограниченного набора перестраиваемых примитивов. Для экспериментов использованы тестовые полутоновые изображения с широким динамическим диапазоном, приведенные на рис. 2. Для этого изображения на рис. 3–5 приведены изображения, формируемые в процессе определения положения и выбора аппроксимирующих примитивов.

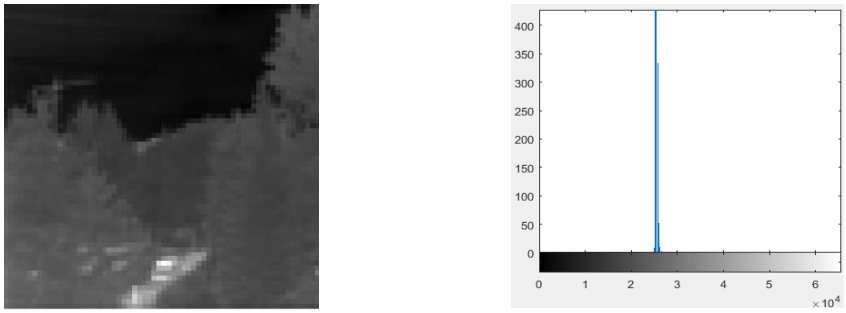
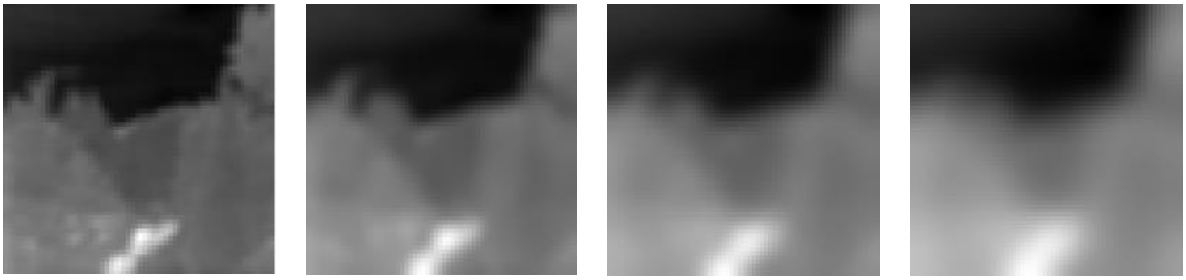


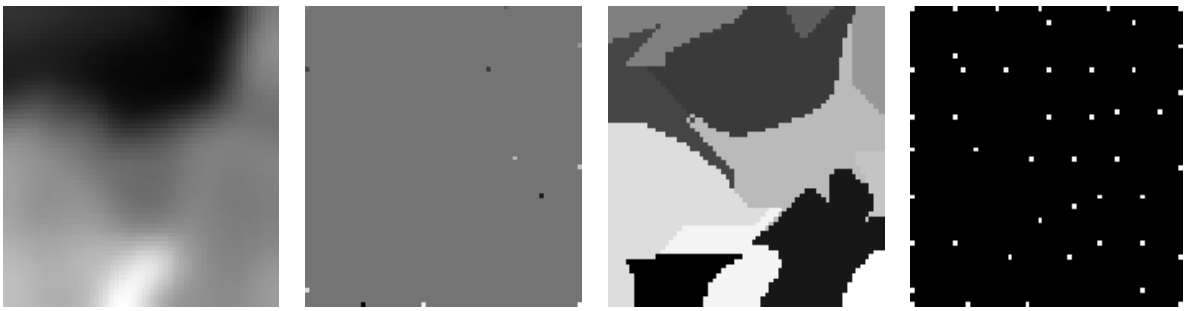

Рис. 2. Тестовое 16-битное изображение и его гистограмма



*а* *б* *в* *г*

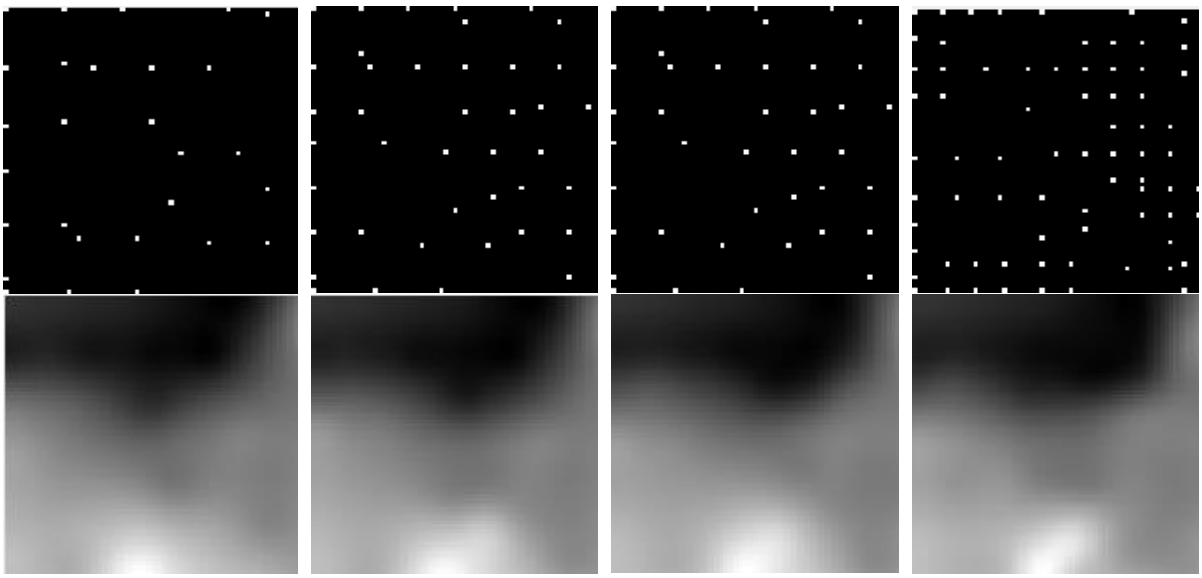
Рис. 3. Результат применения каскада фильтров к изображению на различных уровнях аппроксимации: *а* – с окном 3×3 пикселей на 1-ом уровне; *б* – с окном 5×5 пикселей на 2-ом уровне; *в* – с окном 7×7 пикселей на 3-ем уровне; *г* – с окном 9×9 пикселей на 4-ом уровне

Из рис. 3–5 следует, что блочно-сегментный поиск локальных экстремумов в сочетании с предложенным алгоритмом CLERG выделения областей с монотонным изменением яркости дает визуально схожий результат по сравнению с блочным поиском локальных экстремумов в сочетании с алгоритмом OSRG волнового выращивания областей. На рис. 6, 7 приведены изображения, восстановленные из приведенного на рис. 2 изображения, в результате бессеточной аппроксимации с использованием ограниченного набора перестраиваемых примитивов и с помощью обратного вейвлет-преобразования.



*а* *б* *в* *г*

Рис. 4. Результаты обработки изображений на 4-ом уровне аппроксимации:
*а* – отфильтрованное изображение; *б* – локальные экстремумы;
*в* – области локальных экстремумов с монотонным изменением яркости;
*г* – локализация примитивов для интерполяции



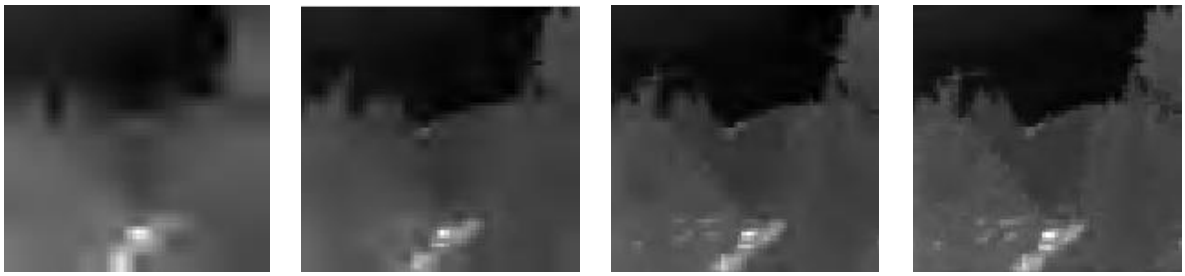
*а* *б* *в* *г*

Рис. 5. Локализации примитивов и результаты интерполяции изображения на 4-ом уровне:
*а* – 33 примитива; *б* – 47 примитивов; *в* – 56 примитивов; *г* – 82 примитива

*а* *б* *в* *г* *д*

Рис. 6. Восстановление изображения при 4-уровневой аппроксимации:
*а* – уровень 1 (33 примитива); *б* – уровни 1, 2 (33+69 примитивов);
*в* – уровни 1–3 (33+69+154 примитивов); *г* – уровни 1–4 (33+69+154+356 примитивов);
*д* – ошибка интерполяции для уровней 1–4

Из рис. 6, 7 следует, что результаты восстановления изображения для 4-х уровневой аппроксимации примерно схожи с результатами восстановления изображения по первому уровню 4-х уровневого вейвлет-преобразования. Различия в качестве восстановления изображения на одинаковых уровнях аппроксимации и вейвлет-преобразования объясняются различной концентрацией информации на этих уровнях.



*а* *б* *в* *г*

Рис. 7. Восстановление изображения при 4-х уровневом вейвлет-преобразовании по убыванию значимости вейвлет-коэффициентов: *а* – при 33 значимых коэффициентах; *б* – при 102 значимых коэффициентах; *в* – при 256 значимых коэффициентах; *г* – при 612 значимых коэффициентах

В табл. 1, 2 приведены распределения энергии коэффициентов по уровням вейвлет-разложения и бессеточной аппроксимации. Из табл. следует, что суммарная энергия коэффициентов на 4-х уровнях бессеточной аппроксимации в 7,2 раза меньше суммарной энергии на 4-х уровнях вейвлет-преобразования. Среднее уменьшение суммарной энергии коэффициентов по инфракрасным 16-битным изображениям составляет 6 раз (при дисперсии от 4,7 до 7,2 раза). Таким образом, для некоторых типов изображений с широким динамическим диапазоном возможно более компактное их представление на основе бессеточной аппроксимации по сравнению с вейвлет-разложением. Однако, бессеточная аппроксимация по сравнению с вейвлет-разложением имеет значительно большую вычислительную сложность.

Табл. 1. **Распределение энергии изображения при вейвлет-разложении**

| Разложение на 4 уровня | | Разложение на 0–6 уровней | |
|---|---|---|---|
| Уровень разложения | Энергия | Число уровней разложения | Энергия |
| 1 | $4{,}7368\times10^{4}$ | 0 | $1{,}0395\times10^{8}$ |
| 2 | $3{,}3746\times10^{4}$ | 1 | $5{,}2018\times10^{7}$ |
| 3 | $2{,}29409\times10^{4}$ | 2 | $2{,}6059\times10^{7}$ |
| 4 | $6{,}5008\times10^{6}$ | 3 | $1{,}3086\times10^{7}$ |
| По четырем уровням | $6{,}6048\times10^{6}$ | 4 | $6{,}6048\times10^{6}$ |
| | | 5 | $3{,}3693\times10^{6}$ |
| | | 6 | $1{,}7621\times10^{6}$ |

Табл. 2. **Распределение энергии изображения при бессеточной аппроксимации**

| Уровень | Число узлов | Энергия |
|---|---|---|
| $0\ \left(E(0)\right)$ | – | $8{,}5573\times10^{4}$ |
| $1\ \left(C_{SI}(1)\right)$ | 356 | $0{,}9064\times10^{4}$ |
| $2\ \left(C_{SI}(2)\right)$ | 154 | $0{,}3597\times10^{4}$ |
| $3\ \left(C_{SI}(3)\right)$ | 69 | $0{,}2251\times10^{4}$ |
| $4\ \left(C_{SI}(4)\right)$ | 33 | $8{,}3795\times10^{5}$ |
| $(0)+(1)+(2)+(3)+(4)$ | 612 | $9{,}2352\times10^{5}$ |

## Заключение

Разработан алгоритм компактного представления изображений с широким динамическим, основанный на многоуровневой бессеточной аппроксимации областей локальных экстремумов с монотонным изменением яркости при помощи двухмерных примитивных функций яркости с

перестраиваемыми параметрами. Произведена оценка компактности представления изображений с помощью вейвлет-разложения и бессеточной интерполяции. Компактность представления изображений оценена по энергии коэффициентов их преобразования и аппроксимации как сумма модулей значений коэффициентов на всех уровнях. Установлено, что 4-уровневая бессеточная аппроксимация областей локальных экстремумов позволяет уменьшить до 7 раз суммарную энергию коэффициентов по сравнению с 4-уровневым вейвлет-разложением для 16-битных инфракрасных изображений. Недостатком бессеточной аппроксимации по сравнению с вейвлет-разложением является значительно большая вычислительная сложность.

## COMPACT REPRESENTATION OF WIDE DYNAMIC RANGE IMAGES BASED ON GRIDLESS APPROXIMATION OF LOCAL EXTREME REGIONS

A.T. NGUYEN, V.Yu. TSVIATKOU

**Abstract.** For a compact representation of images with a wide dynamic range, an algorithm is proposed based on a gridless approximation of the regions of local extrema with a monotonic change in brightness using a limited set of tunable primitives. Comparison of the results of approximation using the proposed algorithm and wavelet transform is carried out.

*Keywords*: compact representation of images, gridless approximation of images, areas of local extrema with monotonic brightness changes.

### Список литературы

1. International Conference on Mathematics and Computers in Sciences and in Industry, Greece, 24–27 August. 2017. P. 212–218.
2. Smolik M., Skala V. // Integrated Computer-Aided Engineering. 2018. Vol. 25, Iss. 1. P. 49–62.
3. Demaret L., Iske A. // Curve and Surface Fitting. 2003. P. 107–117.
4. Iske A. // Mathematical methods for curves and surfaces. 2000. P. 211–220.
5. Majdisova Z., Skala V., Smolik M. // Proceedings of the Computational Methods in Systems and Software. 2018. P. 213–224.
6. Cervenka M., Smolik M., Skala V. // Computational Science and Its Application, ICSSA 2019 proceedings, Part I, LNCS 11619. 2019. P. 322–336.
7. Skala V., Karim S.A.A., Cervenka M. // International Conference on Computational Science. 2020. P. 239–250.
8. Majdisova Z., Skala V., Smolik M. // Integrated Computer-Aided Engineering. 2020. Vol. 27, Iss. 1. P. 1–15.
9. Нгуен А.Т., Цветков В.Ю. // Системный анализ и прикладная информатика. 2019. № 4. С. 4–9.
10. Нгуен А.Т., Цветков В.Ю. // Докл. БГУИР. 2021. № 19(4). С. 61–69.

*УДК 621.391*

# СТРУКТУРНЫЕ И КОРРЕЛЯЦИОННЫЕ СВОЙСТВА ПОСЛЕДОВАТЕЛЬНОСТЕЙ КОДА ГОППА

С.Б. САЛОМАТИН, В.В. ПАНЬКОВА

*Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь*

*Поступила в редакцию 8 ноября 2021*

**Аннотация.** Рассматриваются свойства апериодической функции автокорреляции и профиля линейной сложности последовательностей, сформированных на основе бинарных кодов Гоппа. Для решения данной задачи разработаны алгоритмы формирования последовательностей кодов Гоппа, вычисления апериодической корреляционной функции, построения профиля линейной сложности на основе процедуры Берлекэмпа-Мэсси. Показано, что апериодическая корреляционная функция последовательностей кодов Гоппа имеет малый уровень максимального бокового лепестка. Графики линейной сложности последовательностей кода Гоппа имеют профиль близкий к профилю линейной сложности эталонного криптографического генератора BBS. Данные свойства позволяют рекомендовать последовательности кода Гоппа для синхронизации блочных помехоустойчивых кодов в системах связи и зондирующих сигналов в системах радиолокации.

*Ключевые слова*: помехоустойчивый код Гоппа, автокорреляционная функция, линейная сложность булевых функций, алгоритм Берлекэмпа-Мэсси.

## Введение

Код Гоппа относится к классу альтернантных кодов [1, 2]. Широко известно применение кодов Гоппа в качестве ядра криптосистемы Мак-Элис [3, 5]. В системах кодирования и защиты данных блочными кодами важными являются задачи поиска последовательностей с «хорошими» корреляционными свойствами и линейной сложностью булевой структуры. Один из путей задач такого рода состоит в исследовании свойств блочных помехоустойчивых кодов.

В настоящей работе рассматриваются свойства бинарных последовательностей кода Гоппа с точки зрения оценки автокорреляционной функции и линейной сложности.

## Коды Гоппа

Определим полином Гоппа [1, 2] $g(x)=g_0+g_1x+..,+g_tx^t=\sum_{i=0}^{t}g_ix^i,\ g_i\in GF\left(p^m\right)$. Пусть $L$ образует конечное подмножество расширенного поля $GF\left(p^m\right)$, $p$ – простое число $L=\{\alpha_1,...,\alpha_n\}\subseteq GF\left(p^m\right)$, такое, что $g(\alpha_i)\neq 0$ для всех $\alpha_i\in L$.

Задавая кодовый вектор $\mathbf{c}=(c_1,...,c_n)$ над $GF(q)$ мы получаем функцию

$$R_c(z)=\sum_{i=1}^{n}\frac{c_i}{x-\alpha_i}, \qquad (1)$$

где $(1/(x-\alpha_i))$ единственный полином, степень которого меньше или равна $(t-1)$ и удовлетворяет условию $(x-\alpha_i)/(x-\alpha_i)\equiv 1 \bmod g(x)$.

Код Гоппа $\Gamma(L,g(x))$ содержит все кодовые векторы с такие, что $R_c(z)\equiv 0 \bmod g(x)$.

*Параметры кода*. Код Гоппа –линейный код, имеющий параметры $(n, k, d_{\min})$. Длина $n$ зависит от подмножества $L$. Размерность $k$ кода Гоппа $\Gamma(L, g(x))$ над полем $GF(p^m)$, длины $n$, больше или равна величине $n - mt$ или $k \geq n - mt$. Минимальное кодовое расстояние $d_{\min}$ кода Гоппа $\Gamma(L, g(x))$длины $n$, больше или равно $(t+1)$ или $d_{\min} \geq t+1$.

*Бинарные коды Гоппа*. Проверочная матрица кода определяется как матрица $\mathbf{H}$, для которой справедливо соотношение $\mathbf{H}\mathbf{c}^T = 0$, для всех векторов кодовых слов $\mathbf{c}$ в $GF(2^m)$, удовлетворяющих требованиям кода Гоппа.

*Предложение.* Пусть $g(x)$ – неприводимый полином над полем $GF(2^m)$ и пусть

$$\mathbf{H} = \mathbf{XYZ}, \tag{2}$$

где

$$\mathbf{Y} = \begin{bmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_{\mathbf{n}} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{\mathbf{t-1}} & \alpha_2^{\mathbf{t-1}} & \dots & \alpha_{\mathbf{n}}^{\mathbf{t-1}} \end{bmatrix}, \quad \mathbf{X} = \begin{bmatrix} g_t & 0 & 0 & \dots & 0 \\ g_{t-1} & g_t & 0 & \dots & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ g_1 & g_2 & g_3 & \dots & g_n \end{bmatrix}, \tag{3}$$

$$\mathbf{Z} = \begin{bmatrix} 1/g(\alpha_1) & 0 & \dots & 0 \\ 0 & 1/g(\alpha_2) & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1/g(\alpha_n) \end{bmatrix},$$

тогда матрица $\mathbf{H}$ является проверочной матрицей кода Гоппа $\Gamma(L, g(x))$.

*Пример* 1. Пусть задано поле $GF(2^m)$, $m = 4$, $f(x) = x^4 + x + 1 = (19)_{dec}$. Построим код Гоппа с параметрами $(n, k) = (16, 4)$, исправляющий $t = 3$ три ошибки. Используя алгоритм Рабина [5], найдем неприводимый полином Гоппа $g(x) = \alpha + \alpha^{14}x + \alpha^{13}x^2 + \alpha^{11}x^3$.

Конечное подмножество расширенного поля $L = \{\alpha_1, \dots, \alpha_n\}$ определим как $L = (\alpha^{14}, \alpha^6, \alpha^{10}, \alpha^{15}, \alpha^2, \alpha^7, \alpha^9, \alpha^3, \alpha^{12}, \alpha^5, \alpha^{11}, \alpha, \alpha^4, \alpha^8, \alpha^0) = (14,6,10,15,2,7,9,3,12,5,11,1,4,8,0)_{\deg}$.

Проверочная матрица кода Гоппа будет иметь вид

$$\mathbf{H} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

Используя соотношения (2) и (3), генераторная матрица $\mathbf{G}$ может быть построена с использованием проектирования в нулевое подпространство $\mathbf{G} = \mathit{Nullspace}(\mathbf{H}) \bmod p$.

## Автокорреляционные свойства последовательностей кода Гоппа

В системах синхронизации блочных кодов используются последовательности с малыми боковыми лепестками апериодических автокорреляционных функций. Покажем, последовательности кода Гоппа имеют низкий уровень боковых лепестков апериодической автокорреляционной функции.

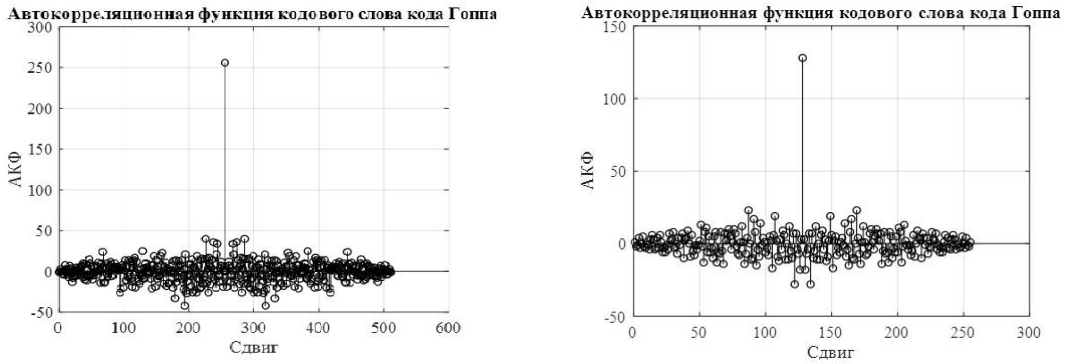
Кодовое слово $\mathbf{c} = (c_0, c_1, ..., c_{n-1}), c_i \in \{0,1\}$ определится как произведение случайного вектора данных $\mathbf{a} = (a_0, a_1, ..., a_{k-1}), a_i \in \{0,1\}$ на генераторную матрицу $\mathbf{G}$: $\mathbf{c} = \mathbf{aG} \bmod p$.

Последовательности $\mathbf{s} = (s_0, s_1, ..., s_{n-1}), s_i \in \{\pm 1\}$ кода Гоппа определим через отображение $s_i = (-1)^{c_i}$. Тогда для последовательности **s** длиной $N$ апериодическая автокорреляционная функция (АКФ) может быть записана следующим образом:

$$r_{xx}(m) = \frac{1}{N} \sum_{i=0}^{N-m-1} s_{i+m} s_i^*.$$

*Пример* 2. Пусть $n = 256$, $k = 224$, $t = 4$, поле $GF(2^8)$ построено с помощью полинома $f(x) = (285)_{dec}$, полином Гоппа имеет вид $g(x) = \alpha + \alpha^{39}x + \alpha^{132}x^2 + \alpha^{121}x^3 + \alpha^{145}x^4$. Апериодическая АКФ приведена на рис. 1, *а*.

Пусть $n = 128$, $k = 100$, $t = 4$, поле $GF(2^7)$, $f(x) = (137)_{dec}$ полином Гоппа имеет вид $g(x) = \alpha + \alpha^{32}x + \alpha^{88}x^2 + \alpha^{120}x^3 + \alpha^{20}x^4$. Апериодическая АКФ приведена на рис. 1, *б*.




*а* *б*

Рис. 1. Апериодические АКФ последовательностей кода Гоппа: *а* – код Гоппа длиной $n = 256$; *б* – код Гоппа длиной $n = 128$.

Анализ максимального уровня боковых лепестков апериодической АКФ $\rho_{\max}$ показывает, что для последовательностей кода Гоппа он не превышает величину $\rho_{\max} \le 2{,}6\sqrt{n}$, где $n$ – длина кодовой последовательности.

## Оценка линейной сложности кода Гоппа на основе алгоритма Берлекэмпа-Мэсси

Линейной сложностью $LS(c)$ последовательности $\mathbf{c}_i(l) = (c_{0,i}, c_{1,i}, ..., c_{l-1,i})$ называется длина $L$ самого короткого РСЛОС, который может сгенерировать вектор **c**, когда первые $L$ цифр последовательности **c** являются начальным заполнением регистра. Эквивалентное определение: линейная сложность $LS(c)$ определяется как наименьшее неотрицательное целое $L$, такое, что существует линейная рекуррента с фиксированными константами $(c_0, c_1, ..., c_l)$, удовлетворяющая равенству $c_j + \beta_1 c_{j-1} + ... + \beta_L c_{j-L} = 0, \quad L \le j \le 1$. Коэффициенты $\{\beta_i\}$ определяют полином обратной связи РСЛОС $C(D) = 1 + \beta_1 D + \beta_2 D^2 + ... + \beta_L D^L$ [2].

*Алгоритм БМ*

Вход: Бинарная последовательность $\mathbf{c}(m) = (c_0, c_1, ..., c_{n-1})$ длиной $n$.

Выход: Линейная сложность $LS\left(\mathbf{c}(n)\right)$.

1. Инициализация исходных данных $C(D)\leftarrow 1,\ L\leftarrow 0,\ m\leftarrow(-1),\ B(D)\leftarrow 1,\ N\leftarrow 0$.

2. До тех пор пока $N<n$, выполнять следующие операции:

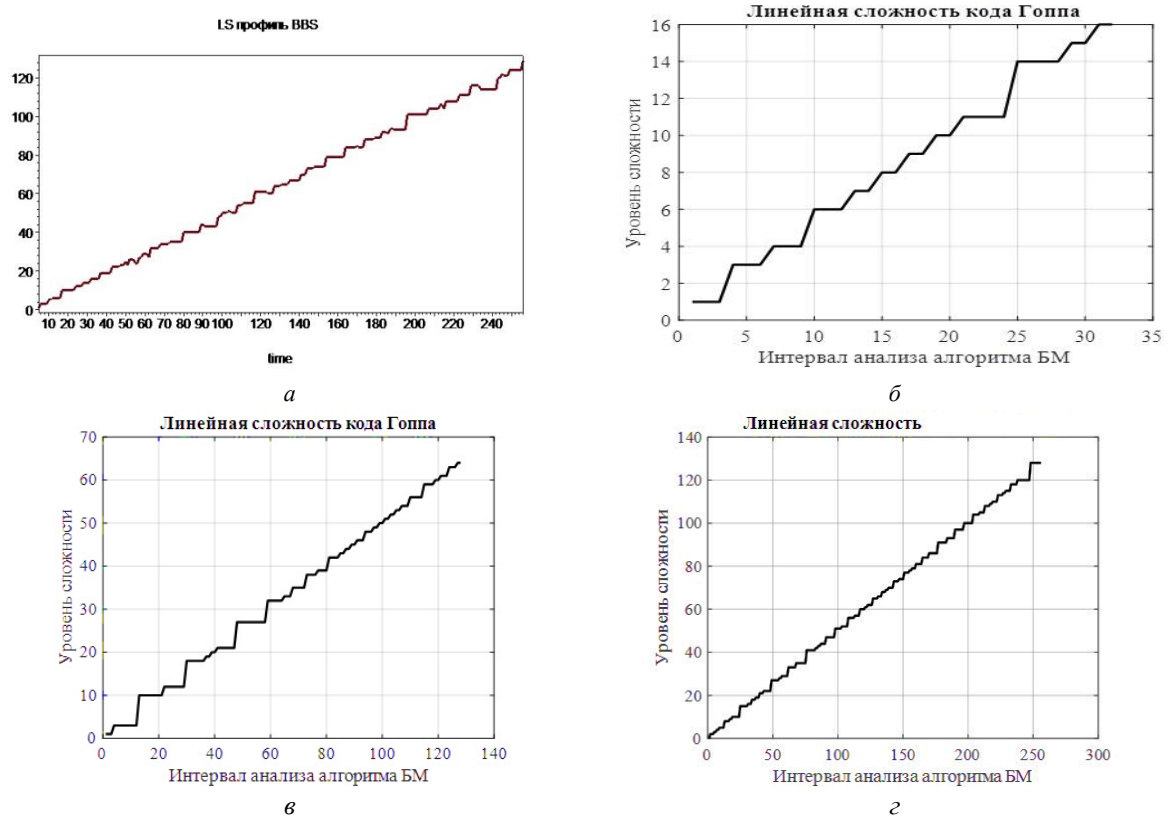
2.1. Вычислять невязку $d\leftarrow c_N+\sum_{i=1}^{L}\beta_i c_{N-i} \bmod 2$.

2.2. Если $d=1$, то выполнять следующие действия: $T(D)\leftarrow C(D)$, $C(D)\leftarrow C(D)+B(D)D^{N-m}$, если $L\le N/2$, тогда $L\leftarrow N+1-L$, $m\leftarrow N$, $B(D)\leftarrow T(D)$.

2.3. $N\leftarrow N+1$.

3. Получение значения $L$.

Применим алгоритм БМ для оценки линейной сложности кода Гоппа. Для сравнения вычислим профиль линейной сложности последовательности криптографического генератора BBS. На рис. 3, *б*, *в*, *г* приведены графики профилей линейных сложностей последовательностей кода Гоппа и последовательности криптографического генератора BBS [5] (рис. 1, *а*).




*а* *б* *в* *г*

Рис. 2. Профили линейной сложности последовательностей кода Гоппа: *а* – последовательность BBS, $N=256$; *б* – последовательность кода Гоппа, $N=64$; и *в* – последовательность кода Гоппа, $N=128$; *г* – последовательность кода Гоппа, $N=256$

Анализ результатов вычислений показывают, что последовательности кода Гоппа имеют линейную сложность, близкую к сложности последовательностей криптографических булевых функций.

## Заключение

Альтернантные коды Гоппа образуют обширное многообразие кодовых последовательностей. Анализ апериодических автокорреляционных функций показывает, что уровень максимального бокового лепестка не превышает величины $\rho_{\max}\le 2{,}6\sqrt{N}$, что является приемлемым для применения в системах локации и связи, например в устройствах блочной синхронизации. Кроме того, последовательности бинарных кодов Гоппа обладают профилем

линейной сложности, близким к профилю эталонных тестовых криптографических последовательностей BBS. Такое свойство обеспечивает дополнительную криптографическую защиту последовательностей кода Гоппа.

## STRUCTURAL AND CORRELATION PROPERTIES OF SEQUENCES OF THE GOPPA CODE

S.B. SALOMATIN, V.V. PANKOVA

**Abstract.** The properties of the aperiodic autocorrelation function and the linear complexity of sequences formed on the basis of binary Goppa codes are considered. To solve this problem, algorithms have been developed for generating sequences of Goppa codes, calculating the aperiodic correlation function, constructing a linear complexity profile based on the Berlekamp-Massey procedure. It is shown that the aperiodic correlation function of Goppa code sequences has a low level of the maximum side lobe. Linear complexity graphs of Goppa code sequences have a profile close to the linear complexity profile of the BBS reference cryptographic generator. These properties make it possible to recommend Goppa code sequences for the synchronization of block error-correcting codes in communication systems and sounding signals in radar systems.

*Keywords*: error-correcting Goppa code, autocorrelation function, linear complexity of Boolean functions, Berlekamp-Massey algorithm.

### Список литературы

1. Goppa V.D. // Problemy Peredachi Informatsii [Problems of information transmission]. 1970. Vol. 6. P. 207–212.
2. MacWilliams F.J., Sloane N.J.A. The Theory of Error Correcting Codes. New York. North-Holland Publ. 1977. P. 762.
3. Токарева Н.Н. Нелинейные булевы функции: бент-функции и их обобщения. Lap Lambert Academic Publishing (Saarbrucken, Germany). 2011. С. 180.
4. Саломатин С.Б. Поточные криптосистемы. Минск, БГУИР. 2006. С. 76.
5. Bernstein D.J., Buchmann J., Dahmen E. Post Quantum Cryptography. Springer Publishing Company, Incorporated, 1st edition. 2009. P. 249.

*УДК 621.391*

# ДВОЙНОЕ УМЕНЬШЕНИЕ ДИНАМИЧЕСКОГО ДИАПАЗОНА ИК-ИЗОБРАЖЕНИЙ С УПРАВЛЕНИЕМ ФОРМОЙ ГИСТОГРАММЫ

С.И. РУДИКОВ[1], В.Ю. ЦВЕТКОВ[2], А.П. ШКАДАРЕВИЧ[1]

*1 – Научно-технический центр «ЛЭМТ» БелОМО, Республика Беларусь*
*2 – Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь*

*Поступила в редакцию 1 ноября 2021*

**Аннотация.** Для повышения качества и расширения интервала управления характеристиками воспроизведения ИК-изображений в статье предложен алгоритм двойного уменьшения динамического диапазона изображения с промежуточным управлением формой его гистограммы. Проведено сравнение характеристик предложенного алгоритма с характеристиками известных алгоритмов уменьшения динамического диапазона и улучшения качества изображений.

*Ключевые слова*: уменьшение динамического диапазона изображений, повышение качества воспроизведения изображений, инфракрасные изображения, эквализация гистограммы.

## Введение

Для уменьшения динамического диапазона и повышения качества многоразрядных инфракрасных (ИК) изображений используются методы на основе: преобразования яркости с линейной, кусочно-линейной и нелинейной (логарифмическая, гамма, арктангенс и др.) коррекцией яркости [1, 2]; эквализации гистограммы (глобальной и локальной) [3–5]; преобразования (гомоморфные, пространственно-частотные) [6, 7]; модели человеческого визуального восприятия (в сочетании с методами машинного и глубокого обучения) [7, 8]; фильтрации и многоканальной обработки [9]; гибридные. Наиболее эффективны блочные методы преобразования на основе локальной эквализации гистограммы [4, 5]. Они обеспечивают достаточно высокое качество изображений после преобразования, но не позволяют управлять формой гистограммы формируемого изображения.

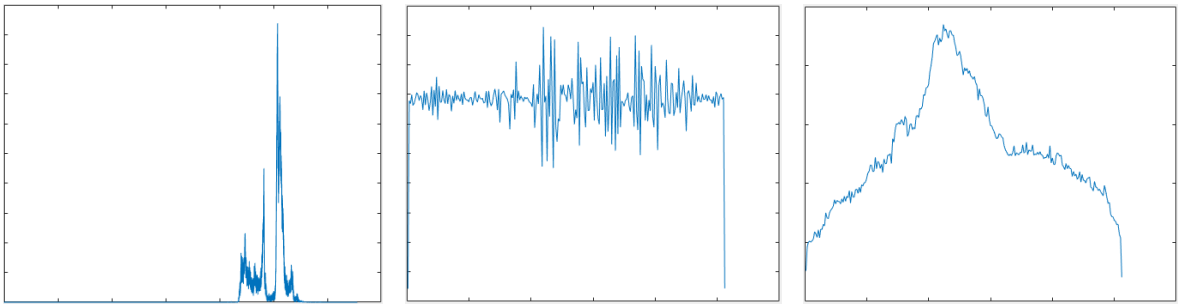
Цель работы: повышение качества и расширение интервала управления характеристиками воспроизведения ИК-изображений при уменьшении их динамического диапазона.

## Постановка задачи

На рис. 1, *а* приведена гистограмма ИК-изображения $I_{HDR} = \left\| i_{HDR}\left(y,x\right)\right\|_{\left(y=\overline{0,Y-1},\, x=\overline{0,X-1}\right)}$ с динамическим диапазоном $\left[0, L_{HDR}-1\right]$, $L_{HDR}=16384$. Эквализация (HE) [3] выравнивает гистограмму (рис. 1, *б*) и формирует изображение $I_{HE}\left(L_{LDR}\right) = \left\| i_{LDR}\left(L_{LDR},y,x\right)\right\|_{\left(y=\overline{0,Y-1},\, x=\overline{0,X-1}\right)}$ с динамическим диапазоном $\left[0, L_{LDR}-1\right]$ $\left(L_{LDR} < L_{HDR}\right)$, переопределяя значения пикселей на основе вектора $H_E\left(L_{LDR}\right) = \left\| h_E\left(L_{LDR}, l\right)\right\|_{\left(l=\overline{0,L_{HDR}-1}\right)}$ выравнивания. Значения $H_E\left(L_{LDR}\right)$ вычисляются на основе вектора $H_{CDF} = \left\| h_{CDF}\left(l\right)\right\|_{\left(l=\overline{0,L_{HDR}-1}\right)}$ значений интегральной функции распределения яркостей.

Для ИК-изображений $I_{LDR} = \left\| i_{LDR}\left(y,x\right)\right\|_{\left(y=\overline{0,Y-1},\, x=\overline{0,X-1}\right)}$, полученных в результате преобразования динамического диапазона с помощью алгоритмов на основе эквализации (HE), адаптивной эквализации (AHE), адаптивной эквализации с ограничением контраста (CLAHE), в

табл. 1 приведены блочные (для 16 центральных блоков размером 64×64 пикселей) значения средней яркости $V_M$, контрастности (стандартного отклонения) $D_{ST}$, среднего градиента $G_A$, энтропии $E_I$ и количества локальных экстремумов $N_{LE}$.



*а* *б* *в*

Рис. 1. Преобразованные ИК-изображения и гистограммы яркостей:
*а* – гистограмма исходного изображения; *б* – гистограмма изображения после эквализации;
*в* – гистограмма изображения после адаптивной эквализации

Табл. 1. **Блочные характеристики ИК-изображения после преобразования динамического диапазона с помощью различных алгоритмов (для 16 центральных блоков 64×64 пикселей)**

| | НЕ | | | | АНЕ | | | | CLAHE (порог 0,7) | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $V_M$ | 56.6299 | 46.8899 | 60.8247 | 65.4817 | 139.0764 | 120.0801 | 131.9780 | 133.3284 | 138.3696 | 119.2720 | 131.4504 | 133.0400 |
| | 118.1655 | 110.8328 | 89.1611 | 89.4199 | 136.2896 | 136.7090 | 116.5271 | 139.1985 | 135.7859 | 136.0925 | 116.1260 | 138.7180 |
| | 182.6606 | 172.9255 | 166.6401 | 179.6472 | 145.9661 | 136.5193 | 138.9609 | 148.3640 | 144.8640 | 135.3958 | 137.5488 | 147.5322 |
| | 198.1091 | 189.7126 | 171.2529 | 204.5200 | 141.3127 | 141.5608 | 136.8904 | 149.9846 | 140.1589 | 139.8833 | 133.6714 | 148.5784 |
| $D_{ST}$ | 21.9333 | 13.5732 | 16.0995 | 14.1722 | 45.5368 | 41.8184 | 69.5705 | 65.5206 | 45.4996 | 41.7598 | 69.3058 | 65.3328 |
| | 57.1386 | 48.7251 | 40.1890 | 13.5223 | 51.1520 | 48.4922 | 53.7408 | 51.2669 | 50.7874 | 48.0785 | 53.4596 | 51.0176 |
| | 23.2324 | 38.6699 | 45.6273 | 43.8044 | 58.5173 | 68.4838 | 65.3261 | 54.3119 | 58.0217 | 68.0328 | 65.0301 | 53.9292 |
| | 27.2230 | 49.6122 | 56.5827 | 34.2119 | 63.3532 | 69.5779 | 68.2903 | 65.8417 | 62.8053 | 69.3316 | 67.6612 | 65.4540 |
| $G_A$ | 1.3173 | 1.1947 | 1.7782 | 1.9953 | 4.1422 | 4.7962 | 7.6560 | 8.9237 | 4.1260 | 4.7765 | 7.6317 | 8.8826 |
| | 4.8990 | 5.3019 | 3.3361 | 2.7413 | 8.3126 | 7.7338 | 7.3327 | 14.4899 | 8.2560 | 7.6350 | 7.3141 | 14.4279 |
| | 8.0839 | 8.2234 | 7.5670 | 6.7155 | 20.5580 | 14.5084 | 11.4833 | 10.9717 | 20.3731 | 14.3833 | 11.3742 | 10.9186 |
| | 7.9024 | 6.4074 | 6.1890 | 7.8415 | 19.9522 | 12.6282 | 11.1148 | 14.8632 | 19.7971 | 12.5459 | 10.9011 | 14.8030 |
| $E_I$ | 5.3324 | 5.0952 | 5.5784 | 5.6022 | 6.7951 | 6.6059 | 7.4971 | 7.7360 | 6.7814 | 6.5967 | 7.4894 | 7.7285 |
| | 6.5965 | 6.8060 | 6.0109 | 4.5902 | 7.2881 | 7.2335 | 7.3563 | 7.5657 | 7.2796 | 7.2271 | 7.3496 | 7.5610 |
| | 6.5042 | 7.0595 | 7.1229 | 7.0005 | 7.7629 | 7.7622 | 7.6408 | 7.5801 | 7.7584 | 7.7530 | 7.6272 | 7.5727 |
| | 6.6978 | 6.8900 | 6.7632 | 6.7786 | 7.8310 | 7.8758 | 7.7647 | 7.8378 | 7.8200 | 7.8636 | 7.7506 | 7.8275 |

Эквализация гистограммы не учитывает локальные особенности распределения яркостей пикселей. В методе АНЕ [4] исходное изображение $I_{HDR}$ делится на блоки размером $Y_B \times X_B$ по вертикали и горизонтали, для центров которых вычисляются векторы $H_E(y_B, x_B, L_{LDR}) = \left\| h_E(y_B, x_B, L_{LDR}, l) \right\|_{\left(l=\overline{0, L_{HDR}-1}\right)}$ выравнивания в пределах блока, где $y_B, x_B$ – координаты центра блока; $B_Y, B_X$ – число блоков по вертикали и горизонтали. На основе векторов выравнивания смежных блоков с помощью интерполяции вычисляются остальные значения пикселей $i_{AHE}(L_{LDR}, y, x)$ изображения $I_{AHE}(L_{LDR})$ с динамическим диапазоном $[0, L_{LDR}-1]$, что позволяет снизить вычислительную сложность преобразования. Разделение изображения на блоки в АНЕ позволяет адаптироваться к структуре изображения, хотя и не обеспечивает равномерность глобальной гистограммы (рис. 1, *в*). Для некоторых изображений применение АНЕ приводит к чрезмерной контрастности и росту заметности шума. Для ИК-изображений с концентрацией значений в центральной части гистограммы CLAHE также не эффективен (его использование приводит к незначительному растяжению гистограммы по равнению с АНЕ).

Из табл. 1 следует, что АНЕ превосходит методы НЕ и CLAHE по всем показателям качества, уступая только CLAHE по средней яркости. При этом CLAHE не позволяет управлять характеристиками изображения, а только уменьшением контрастности, что сопровождается ухудшением и других характеристик. Для повышения качества и расширения интервала управления характеристиками воспроизведения ИК-изображений при уменьшении

динамического диапазона необходим алгоритм, параметры которого могут быть подобраны с учетом распределения значений в гистограмме исходного изображения.

### Алгоритм уменьшения динамического диапазона ИК-изображений

Для повышения качества и расширения интервала управления характеристиками воспроизведения ИК-изображений при уменьшении их динамического диапазона разработан алгоритм HECS (Histogram Equalization, Compression and Stretching) на основе адаптивной эквализации, растяжения и сжатия гистограммы. Сущность алгоритма состоит в двойном уменьшении динамического диапазона изображения с промежуточным управлением формой его гистограммы за счет ее частичного растяжения и сжатия. Алгоритм включает три этапа.

1. Предварительное уменьшение динамического диапазона изображения до $[0, L_{LDR1}-1]$ (этап 1) на основе адаптивной эквализации гистограммы – формируется изображение $I_{AHE}(L_{LDR1})$ с динамическим диапазоном $[0, L_{LDR1}-1]$.

2. Управление формой гистограммы (этап 2):

2.1. Сжатие гистограммы на основе двух гамма-функций с коэффициентами $G_L$ и $G_H$, применяемых к двум частям динамического диапазона $[0, T_G-1]$ и $[T_G+1, L_{LDR1}-1]$, разделяемым на уровне $T_G = K_G(L_{LDR1}-1)$ по коэффициенту $K_G$.

2.2. Линейное растяжение центральной части гистограммы, ограниченной динамическим диапазоном $[T, L_{LDR1}-1-T]$ по порогу $T$, с коэффициентом $(L_{LDR1}-1)/(L_{LDR1}-1-2T)$ и линейное растяжение (сжатие) боковых частей гистограммы, ограниченных диапазонами $[0, T-1]$ и $[L_{LDR1}-T, L_{LDR1}-1]$ по порогу T с коэффициентами $T_L/T$ и $T_R/T$.

3. Окончательное уменьшение динамического диапазона до $[0, L_{LDR2}-1]$ на основе линейного сжатия гистограммы с коэффициентом $L_{LDR2}/L_{LDR1}$ (этап 3).

### Оценка эффективности работы алгоритмов преобразования динамического диапазона

При постоянных значениях $Y_B, X_B, L_{LDR1}, L_{LDR2}$ результаты преобразования HECS зависят от 6 параметров: $\{K_G, G_L, G_H, T, T_L, T_R\}$. Причем, существуют наборы параметров $\{K_G, G_L, G_H, T, T_L, T_R\}$, обеспечивающие лучшие характеристики $\{V_M, D_{ST}, G_A, E_I, N_{LE}\}$ по сравнению с алгоритмами HE, AHE и CLAHE (табл. 2).

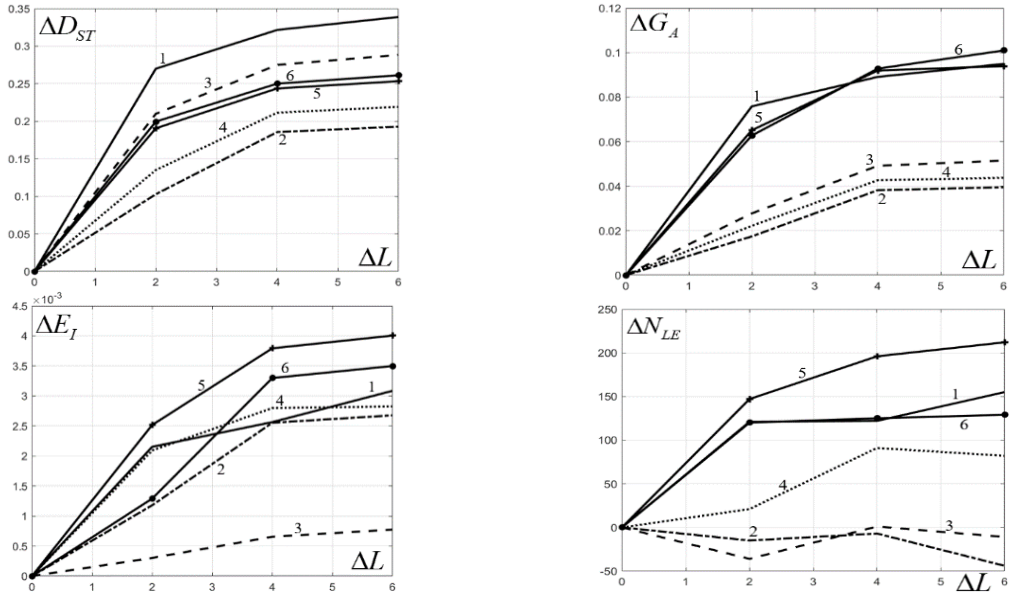
Табл. 2. **Блочные характеристики ИК-изображения после преобразования динамического диапазона с помощью алгоритма HECS (для 16 центральных блоков 64×64 пикселей)**

| | $G_L=1,0;\ T=0,25;\ T_L=1$ | | | | $K_G=0,52;\ G_L=1,2;\ T=0,3;\ T_L=1$ | | | | $K_G=0,5;\ G_L=1,58;\ T=0,13;\ T_L=1$ | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $V_M$ | 134,679 | 103,228 | 129,911 | 138,72 | 130,483 | 100,267 | 130,979 | 139,161 | 140,346 | 122,407 | 133,22 | 133,144 |
| | 129,257 | 130,461 | 103,448 | 144,552 | 126,184 | 127,752 | 103,79 | 144,7 | 137,321 | 137,822 | 118,068 | 139,427 |
| | 148,945 | 129,55 | 128,58 | 147,17 | 147,501 | 129,285 | 126,31 | 145,094 | 146,444 | 137,098 | 140,296 | 149,61 |
| | 145,113 | 142,104 | 132,797 | 153,431 | 144,425 | 140,54 | 131,172 | 151,998 | 141,417 | 142,128 | 137,243 | 149,882 |
| $D_{ST}$ | 69,3271 | 61,8439 | 86,8645 | 81,2686 | 67,6154 | 58,9855 | 79,2623 | 75,9073 | 44,0355 | 40,7059 | 69,3043 | 65,9684 |
| | 77,5715 | 70,7298 | 78,5493 | 73,8501 | 78,8093 | 70,5348 | 74,7419 | 69,8253 | 49,6155 | 46,9932 | 52,3309 | 50,3646 |
| | 75,4276 | 85,2185 | 84,0918 | 70,9141 | 71,6261 | 80,5479 | 80,7015 | 67,7475 | 58,1275 | 66,9678 | 64,4772 | 54,4829 |
| | 80,1182 | 84,263 | 80,7222 | 81,2298 | 75,3926 | 79,6093 | 76,1135 | 77,1129 | 63,055 | 68,6331 | 67,2359 | 64,4554 |
| $G_A$ | 7,95323 | 8,81321 | 12,0919 | 13,5764 | 8,58887 | 9,19957 | 12,0385 | 13,9779 | 4,09587 | 4,70267 | 8,2001 | 9,38829 |
| | 12,3054 | 12,6273 | 13,4567 | 22,6722 | 13,261 | 13,2373 | 14,4376 | 23,077 | 8,35645 | 7,49952 | 7,30333 | 14,3721 |
| | 27,3601 | 19,2297 | 15,6852 | 16,5017 | 26,9364 | 19,3573 | 16,2279 | 17,0813 | 20,6173 | 14,7596 | 11,9258 | 11,1959 |
| | 27,0372 | 16,2228 | 14,4942 | 19,8411 | 26,4846 | 16,5677 | 14,9972 | 19,9611 | 20,0698 | 12,8697 | 11,4318 | 15,0585 |
| $E_I$ | 7,3657 | 7,28271 | 7,47567 | 7,61709 | 7,4243 | 7,28465 | 7,45765 | 7,61821 | 6,78842 | 6,57631 | 7,57311 | 7,83037 |
| | 7,78524 | 7,77985 | 7,64784 | 7,80486 | 7,85252 | 7,82472 | 7,6091 | 7,74005 | 7,25016 | 7,16682 | 7,39644 | 7,58231 |
| | 7,80593 | 7,69683 | 7,70292 | 7,82463 | 7,77948 | 7,69407 | 7,75383 | 7,81544 | 7,75887 | 7,76604 | 7,63545 | 7,58427 |
| | 7,76705 | 7,71467 | 7,80059 | 7,71923 | 7,75579 | 7,71989 | 7,85002 | 7,72522 | 7,84839 | 7,87996 | 7,73511 | 7,82546 |

Из табл. 1 и 2 следует, что при таком же отклонении от среднего по сравнению с CLAHE нелинейное сжатие гистограммы в HECS позволяет повысить градиент, энтропию и детализацию изображения после уменьшения динамического диапазона. Нелинейное сжатие гистограммы в HECS позволяет также ограничить контраст. Причем, при ограничении контраста (параметр $D_{ST}$) на таком же уровне, как в CLAHE, алгоритм HECS обеспечивает примерно такую же энтропию (параметр $E_I$) и более высокие значения $G_A$ и $N_{LE}$ (при большем отклонении средней яркости от 128).

Вычислительная сложность алгоритма HECS растет с увеличением $\Delta L = L_{LDR1} - L_{LDR2}$ (из-за увеличения размера гистограммы) и уменьшением $Y_B \times X_B$ (из-за увеличения числа блоков). Вычислительная сложность алгоритмов AHE и CLAHE также растет с уменьшением размера блока. Для выбора значений параметров $\Delta L$ и $Y_B \times X_B$ в алгоритме HECS необходимо учесть значения показателей качества воспроизведения и детализации ИК-изображений после уменьшения их динамического диапазона при этих параметрах.

Для средних значений интервалов перестройки параметров HECS на рис. 2 приведены зависимости разностей между показателями качества воспроизведения и детализации ИК-изображений $\Delta D_{ST} = D_{ST}(\Delta L_1) - D_{ST}(\Delta L_2)$, $\Delta G_A = G_A(\Delta L_1) - G_A(\Delta L_2)$, $\Delta E_I = E_I(\Delta L_1) - E_I(\Delta L_2)$, $\Delta N_{LE} = N_{LE}(\Delta L_1) - N_{LE}(\Delta L_2)$ при $\Delta L_1 = \{0,2,4,6\}$ и $\Delta L_2 = 0$ $(L_{LDR2} = 8)$ от $\Delta L = L_{LDR1} - L_{LDR2}$.

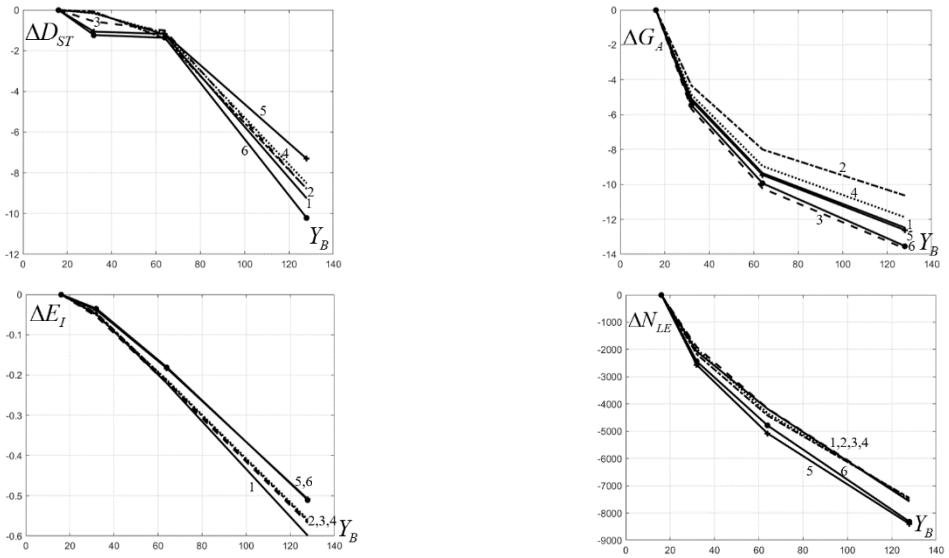



1 – $G_L = 1;\ T = 0,1;\ T_L = 2$, 2 – $K_G = 0,5;\ G_L = 2;\ T = 0,2;\ T_L = 1$, 3 – $G_L = 1;\ T_L = 1;\ T = 0,2,$
4 – $K_G = 0,5;\ G_L = 1,5;\ T_L = 1;\ T = 0,2,$ 5 – $K_G = 0,5;\ T = 0,3;\ T_L = 1;\ G_L = 1,4,$
6 – $G_L = 1,2;\ T = 0,3;\ T_L = 1;\ K_G = 0,5$

Рис. 2. Зависимости разностей показателей качества воспроизведения изображения при $\Delta L > 0$ и $\Delta L = 0$ $(L_{LDR2} = 8)$ от $\Delta L$ для средних значений перестраиваемых параметров алгоритма HECS

Из рис. 2 следует, что с увеличением $\Delta L$ показатели качества растут. При этом показатель $N_{LE}$ растет за исключением двух случаев. Для варианта $L_{LDR1} = 10$ и $L_{LDR2} = 8$ наблюдается наиболее резкий рост показателей качества воспроизведения изображения по сравнению с вариантом $L_{LDR1} = L_{LDR2} = 8$. Лучшее качество воспроизведения изображения обеспечивается при $L_{LDR1} = 14$, но оно незначительно отличается от качества воспроизведения при $L_{LDR1} = 10$.

Для средних значений интервалов перестройки параметров HECS на рис. 3 приведены зависимости разностей между показателями качества воспроизведения и детализации ИК-изображений $\Delta D_{ST} = D_{ST}(\Delta L_1) - D_{ST}(\Delta L_2)$, $\Delta G_A = G_A(\Delta L_1) - G_A(\Delta L_2)$, $\Delta E_I = E_I(\Delta L_1) - E_I(\Delta L_2)$, $\Delta N_{LE} = N_{LE}(\Delta L_1) - N_{LE}(\Delta L_2)$ при $Y_{B1} = \{16,32,64,128\}$ и $Y_{B2} = 16$ от $Y_B$ $(L_{HDR} = 14, L_{LDR1} = 10, L_{LDR2} = 8)$.




$1 - G_L = 1;\ T = 0,1;\ T_L = 2$ , $2 - K_G = 0,5;\ G_L = 2;\ T = 0,2;\ T_L = 1$, $3 - G_L = 1;\ T_L = 1;\ T = 0,2,$

$4 - K_G = 0,5;\ G_L = 1,5;\ T_L = 1;\ T = 0,2,$ $5 - K_G = 0,5;\ T = 0,3;\ T_L = 1;\ G_L = 1,4,$

$6 - G_L = 1,2;\ T = 0,3;\ T_L = 1;\ K_G = 0,5$

Рис. 3. Зависимости разностей показателей качества воспроизведения изображения при $Y_{B1} = \{16, 32, 64, 128\}$ и $Y_{B2} = 16$ от $Y_B$ для средних значений перестраиваемых параметров алгоритма HECS

Из рис. 3 следует, что с увеличением $Y_B$ показатели качества и детализации падают $(Y_B = X_B)$. Однако при малых размерах блока на однородном фоне может проявляться блочный эффект, возникающий в результате интерполяции в алгоритме AHE.

Произведена оценка выигрышей (в процентах) алгоритма HECS по сравнению с алгоритмами AHE и CLAHE по контрастности $D_{ST}$, среднему градиенту $G_A$, энтропии $E_I$ и количеству локальных экстремумов $N_{LE}$, с усреднением по блокам 64×64 пикселей и изображениям, при $Y_B = \{32, 64\}$, $L_{HDR} = 14$, $L_{LDR1} = 10$, $L_{LDR2} = 8$.

Тестовая выборка содержит 94 ИК-изображения, разделенные на 6 типов по форме гистограммы яркости (рис. 4) после адаптивной эквализации (этап 1 преобразования): 11 изображений типа 1; 17 – типа 2; 31 – типа 3; 27 – типа 4; 5 – типа 5; 3 – типа 6. На всех изображениях алгоритм HECS показывает лучшие значения $\{D_{ST}, G_A, E_I, N_{LE}\}$ по сравнению с алгоритмами AHE и CLAHE. По сравнению с алгоритмом AHE наибольшие выигрыши по контрастности $D_{ST}$ наблюдаются для изображений типа 3 при $Y_B = 32\,(10\,\%)$ и типа 1 при $Y_B = 64\,(12,3\,\%)$, по среднему градиенту $G_A$ – для изображений типа 4 при $Y_B = 32\,(20,6\,\%)$ и $Y_B = 64\,(50,5\,\%)$, по энтропии $E_I$ – для изображений типа 5 при $Y_B = 32\,(39,2\,\%)$ и $Y_B = 64\,(55,9\,\%)$, по количеству локальных экстремумов $N_{LE}$ – для изображений типа 4 при $Y_B = 32\,(17,2\,\%)$ и $Y_B = 64\,(25,9\,\%)$. По сравнению с AHE наименьшие выигрыши по контрастности $D_{ST}$ наблюдаются для изображений типа 1 при $Y_B = 32\,(6,1\%)$ и типа 5 при $Y_B = 64\,(0,1\%)$, по среднему градиенту $G_A$ – для изображений типа 5 при $Y_B = 32\,(9,4\,\%)$ и $Y_B = 64\,(13,4\,\%)$, по энтропии $E_I$ – для изображений типа 1 при $Y_B = 32\,(13,4\,\%)$ и $Y_B = 64\,(31,4\,\%)$, по количеству локальных экстремумов $N_{LE}$ – для изображений типа 5 при $Y_B = 32\,(4,3\%)$ и $Y_B = 64\,(6,9\,\%)$.

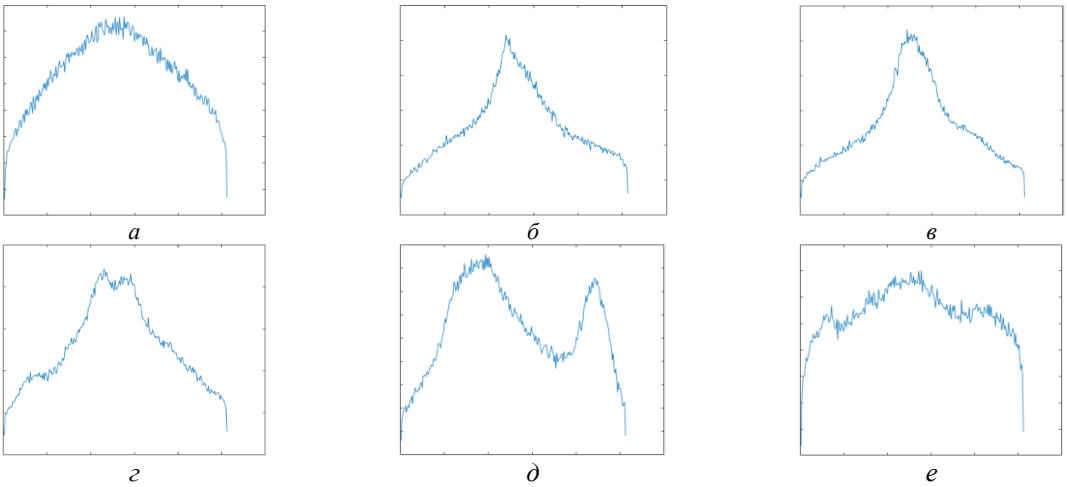


Рис. 4. Формы гистограмм яркости тестовых ИК-изображений после адаптивной эквализации: *а* – тип 1; *б* – тип 2; *в* – тип 3; *г* – тип 4; *д* – тип 5; *е* – тип 6

## Заключение

Для повышения качества и расширения интервала управления характеристиками воспроизведения ИК-изображений при уменьшении их динамического диапазона разработан алгоритм на основе адаптивной эквализации, растяжения и сжатия гистограммы. Сущность алгоритма состоит в двойном уменьшении динамического диапазона изображения с промежуточным управлением формой его гистограммы за счет ее частичного растяжения и сжатия. По сравнению с известными алгоритмами адаптивной эквализации гистограммы разработанный алгоритм обеспечивает повышение контрастности, среднего градиента, энтропии и детализации после преобразования динамического диапазона ИК-изображения. Выигрыши достигаются за счет увеличения вычислительной сложности.

## DUAL DYNAMIC RANGE REDUCTION OF IR IMAGES WITH HISTOGRAM SHAPE CONTROL

S.I. RUDIKOV, V.Yu. TSVIATKOU, A.P. SHKADAREVICH

**Abstract.** The problem of reducing the dynamic range and improving the quality of infrared (IR) images with a wide dynamic range. To improve the quality and expand the control interval for the characteristics of the reproduction of infrared images, the article proposes an algorithm for double reduction of the dynamic range of the image with intermediate control of the shape of its histogram. The characteristics of the proposed algorithm are compared with the characteristics of known algorithms for reducing the dynamic range and improving the image quality.

*Keywords*: reducing the dynamic range of images, improving the quality of image reproduction, infrared images, histogram equalization.

## Список литературы

1. San Chi Liu, [et al.] // Comput. Electr. Eng. 2018. Vol. 70. P. 538–550.
2. Zhi N., Mao S., Li M. // Journal of Liaoning Tech. 2018. Vol. 37(1) P. 191–197.
3. Nithyananda C.R., Ramachandra A.C., Preethi // International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT). 2016. P. 2512–2517.
4. Kim T.K., Paik J.K., Kang B.S. // IEEE Trans. Consum. Electron. 1998. Vol. 44(1). P. 82–87.
5. Reza A.M. // Journal of VLSI Signal Process.-Syst. Signal Image Video Technol. 2004. Vol. 38(1) P. 35–44.
6. Nandal A., Bhaskar V., Dhaka A. // IET Signal Process. 2018. Vol. 12(4). P. 514–521.
7. Xu Q., Cui J., Chen B. // Journal of Hunan Univ. Arts Sci. 2017. Vol. 29(2). P. 41–46.
8. Ren W., [et al.]. // IEEE Trans. Image Process. 2019. Vol. 28(9). P. 4364–4375.
9. Zhu D., [et al.]. // IEEE International Conference on Image Processing (ICIP). 2019. P. 4080–4084.

*УДК 621.391*

# ВЫБОР ДЕСКРИПТОРОВ ДЛЯ ИДЕНТИФИКАЦИИ ПО ИЗОБРАЖЕНИЮ СЕТЧАТКИ ГЛАЗА

А.И. МИТЮХИН

*Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь*

*Поступила в редакцию 21 октября 2021*

**Аннотация.** В работе рассматривается алгоритм получения дескрипторов изображения кровеносных сосудов глазного дна (сетчатки). Наряду с использованием традиционных пространственных и спектральных вейвлет- или Фурье-дескрипторов, рассматривается возможность применения разложения исходных данных в базисе собственных функций и эффективного кодирования. Применение интегрированного подхода при выборе дескрипторов позволяет повысить точность процесса идентификации для известных методов, основанных на выполнении операции пространственного сравнения образа входа и прототипов базы данных. В связи с существующими спецификационными ограничениями на размер входных данных этап эффективного кодирования коэффициентов разложения позволяем ускорить процесс принятия решения о классификации, что важно при практическом использовании системы идентификации.

*Ключевые слова*: биометрическая идентификация, сетчатка, распознавание, изображение, сегментация, дескрипторы, собственные векторы, линейное преобразование.

## Введение

Индивидуальные биометрические параметры сравнительно давно используются в криминалистике [1] и в системах обеспечения безопасности [2]. Одними из основных требований при проектировании технических аппаратно-программных средства идентификации являются эффективность и надежность этапа распознавания. Точностные характеристики любой системы биометрической идентификации во многом определяются выбором соответствующих признаков (дескрипторов) объекта распознавания. Системы идентификации обладают определенной степенью надежности, если физиологические параметры относительно стабильны. Однако многие эти параметры изменяется с возрастом, существенных патологий. Значения параметров могут подвергаться замене в результате маскирования, имитации, например, изображения радужной оболочки глаза [3]. Современное хирургическое вмешательство позволяет изменить лицо практически до неузнаваемости и пр. Повышенную надежность процесса идентификации можно получить, если в качестве признаков распознавания использовать дескрипторы, характеризующиеся постоянством (стабильностью). В отличие от таких индивидуальных физических характеристик человека как отпечатки пальцев, голосовые особенности, лицо и др. изображение сетчатки практически не изменяется с возрастом. Медицинские и идентификационные [4] исследования на достаточно большом временном интервале показывают, что даже однояйцевые близнецы имеют различия в характерных изображениях кровеносных сосудов глазного дна. При этом подчеркивается даже уникальность изображений отдельных фрагментов кровеносной сосудистой сети. Кроме того, изображение кровеносных сосудов в виде сети не может быть искусственно изменено. В статье предлагается и описывается вычислительный алгоритм получения дескрипторов сетчатки, где используется элементы известных пространственных методов с добавлением эффективного кодирования. По мнению автора, результатом является возможность улучшения точностных и временных характеристик идентификации, что важно, когда предъявляются особые требования по обеспечению безопасности, контролю и управлению доступом на специальные объекты.

## Теоретические принципы

Решение задачи отнесения входных изображений сетчатки к какому-либо из идентифицируемых классов образов основывается на выполнении операций дифференциации существенных признаков образов от фоновых составляющих и от деталей, не относящихся к обрабатываемому процессу. В обобщенном виде, как и для многих приложений, где используются цифровая обработка изображений, алгоритм идентификации по изображению сетчатки отображается схемой, показанной на рис. 1. Этап морфологической обработки реализует утончение изображение дерева кровеносных сосудов, а также фильтрацию мало заметных сосудов с целью уменьшения временных затрат на получение классификационных решений.


Рис. 1. Обобщенная схема идентификации по изображению сетчатки

После процесса бинаризации формируется сегментированное изображение, показанное на рис. 2.

Рис. 2. Сегментированное изображение сетчатки [5]

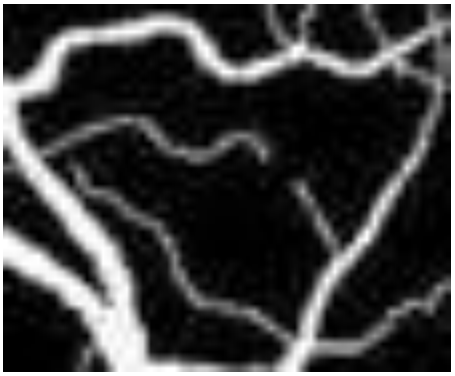


Рис. 3. Фрагмент изображения

В известных и применяемых алгоритмах, взятых их опубликованных работ, извлечение существенных признаков сети сосудов ограничивается только фрагментом изображения, рис. 3. С одной стороны, это связано с временным ограничением процесса идентификации. Если для распознавания используется процесс линейной пространственной фильтрации всего изображения, рис. 2, временные затраты на обработку становятся чрезмерными. С другой стороны, имеются исследования, которые показывают, что увеличение размера входа обработки больше некоторой оптимальной величины, незначительно влияет на точностные характеристики работы классификатора. Один из подходов получения фрагмента базируется на радиальном разделении изображения [6]. Для этого используется маска (окно), выполненная в виде кольца. Внешние границы кольца определяются двумя значениями радиусов $R_1 - R_2 = M$. После совмещения изображения с маской формируется изображение фрагмента, описываемое в полярной системе координат. Используя известные соотношения между представлением данных в полярной и декартовой системах координат, изображение фрагмента будем описывать в декартовом пространстве. После развертки маски-кольца и бинаризации имеем матрицу **G** размером $M \times N$.

Известно, что эффективность обработки изображений как понятие массива случайного процесса, можно повысить, если учитывать его статистические характеристики. Бинарные изображения сетчатки на малых участках напоминают локальные однородные структуры, распределенные по пространству: линии, контуры, разветвления и пр. Все они имеют постоянные значениями яркостей. Такие свойства означают высокую степень коррелированности локальных пространственных признаков изображений, позволяют использовать линейные преобразования коррелированных признаков в набор некоррелированных меньшего размера. Преобразование сравнительно просто реализуется посредством БПФ. Значения дескрипторов Фурье образуют компоненты вектора признаков изображения сетчатки. Вектор хранится в базе данных зарегистрированных пользователей

системы идентификации. Недостатком такого выбора дескрипторов является неполная декорреляция исходных данных, усложнение схемы классификатора. Некоррелированные признаки можно получить из решения задачи на собственные значения [7]. Вычислительно решение этой задачи сравнительно затратно. Отсутствие быстрых вычислительных алгоритмов затрудняет его практическое использование для обработки больших массивов данных. Однако, на специальных объектах имеется ограничение на размер базы данных зарегистрированных пользователей. Кроме того, существует ограничение на размер матрицы $\mathbf{G}$ . По многим научным и техническим источникам размер матрицы $\mathbf{G}$ находится в диапазоне 320–10800 бинарных пикселей. По [8] и другим открытым источникам о системах контроля безопасности, размер вектора дескрипторов Фурье находится в пределах 40–96 байт. Высокая размерность вектора признаков всегда усложняет процесс распознавания. С другой стороны, если выделить главные информационные признаки о объекте, можно уменьшить пространство признаков, и тем самым упростить схему (программу) классификатора. Исходя из этих предпосылок, рассматривается подход выбора (эффективного описания) дескрипторов через переход из декартовой системы координат в систему, базовыми координатами которой, являются собственные векторы ковариационной матрицы изображения сетчатки. В этом случае следует ожидать полной декорреляции данных и повышения эффективности каждого признака с точки зрения представления входного процесса. Рассмотрим основные этапы предлагаемого алгоритма выбора векторов дескрипторов.

1. Определяется ортонормированный базис $\mathbf{T}$ в виде матрицы собственных векторов ковариационной матрицы $\mathrm{cov}(\mathbf{G})$. Матрица $\mathbf{T}$ задает ядро прямого преобразования [9, 10]

$$\hat{\mathbf{G}} = \mathbf{T}(\mathbf{G} - \mathbf{G}_m) \qquad (1)$$

цифрового изображения вида $(\mathbf{G} - \mathbf{G}_m)$, где $\mathbf{G}_m$ – вектор математического ожидания всего фрагмента $\mathbf{G}$ .

Значения коэффициентов матрицы $\hat{\mathbf{G}}$ образуют компоненты векторов $\hat{\mathbf{g}}_i = (\hat{\mathrm{g}}_0, ..., \hat{g}_{N-1})^T$, $i = 0,1,...,M-1$ некоррелиронных признаков. Так как вектор математического ожидания $\hat{\mathbf{G}}_m$ равен нулю, процесс выбора дескрипторов сводится к отбору коэффициентов, имеющих наибольшие значения дисперсий. Таким образом, размер векторов $\hat{\mathbf{g}}_i$ уменьшается при сохранении информации о изображении. Далее векторы $\hat{\mathbf{g}}_i$ преобразуются в двоичный идентификационный код, хранящийся в памяти системы контроля доступа.

2. Для подтверждения правильности идентификации производится дополнительная проверка по усредненному вектору $\mathbf{G}_m = (g_{m,0}, ...g_{m,M-1})$ декартовых данных, описываемых матрицей $\mathbf{G}$. Размерность этого вектора соответствует числу строк $M \le N$ матрицы $\mathbf{G}$. Расстояния между входным образом $\mathbf{G}_m$ и прототипами вычисляются в метрике Хэмминга. Вычисления в этой метрике над двоичным полем Галуа не требуют значительных временных затрат как в аппаратном, так и программном смысле. На этом этапе классификация может осуществляться с помощью простых решающих правил, например, сравнения между множеством допускаемых расстояний внутри класса и расстояниями между классами. Это замечание следует учитывать с учетом того, что при регистрации пользователя в биометрической системе предоставляется несколько образцов биометрического материала.

## Экспериментальные исследования

Идентификационные исследования проводились с использованием изображений сетчатки, взятых из базы данных [5]. В настоящее время продолжается экспериментальная работа с целью получения усредненной оценки минимального размена вектора признаков и, соответственно, длины кода идентификации. Начальное моделирование в среде MALAB решения о подтверждении правильной идентификации личности человека показало, что время обработки не превышало две секунды. Оценка проводилась на 9 различных изображениях, включенных в базу данных созданной для эксперимента. Для более определенной оценки алгоритма предполагается продолжить исследования с использованием базы данных большего размера.

## Заключение

С учетом особенностей статистических характеристик изображения сетчатки рассмотрен алгоритм выбора дескрипторов, позволяющий более эффективно выявлять информационное содержание входного биометрического параметра. Свойство эффективности приводит к преимуществам более быстрой идентификации и аутентификации. Дальнейшие исследования подхода выбора дескрипторов изображения сетчатки связаны с оценкой численности сотрудников специальных объектов, при которой точностные характеристики идентификации должны соответствовать задаваемым техническим требованиям.

# PROTECTION OF INFORMATION BASED ON SPECTRAL-SPATIAL CODING

A.I. MITSIUKHIN

**Abstract.** The paper considers the algorithm for obtaining descriptors of the image of bloody vessels of the fundosal fund (retina). Along with the use of traditional spatial and spectral wavelet or Fourier descriptors, the possibility of using the decomposition of the initial data in the basis of its own functions and effective coding is considered. Using an integrated approach to selecting descriptors improves the accuracy of the identification process for known methods based on performing a spatial comparison operation on the login image and database prototypes. Due to the existing specification limitations on the size of the input data, the stage of effective coding of coefficients of decomposition allows us to speed up the process of making a decision on classification, which is important in the practical use of the identification system.

*Keywords*: biometric identification, retina, recognition, image, segmentation, descriptors, eigenvectors, linear transformation.

## Список литературы

1. American National Standards Institute (ANSI). Biometric Information Management and Security. Technical Report X9.84–2001.
2. Болл Р., Коннел Д., Панканти Ш. [и др.] Руководство по биометрии. Москва, Техносфера, 2007.
3. Старовойтов В.В., Монич Ю.И. // Искусственный интеллект. 2011. № 3. С. 278–284.
4. Ramya M., Sornalatha. M. // IJETCSE. 2014. № 3. С. 164–168.
5. Images Page 1 // [Electronic resource]. URL: https://cecas.clemson.edu/~ahoover/stare/images1.htm.
6. Farzin H., Abrishami H., Shahram M. // EURASIP. 2008. № 5. С. 1–10.
7. Fukunaga K. Introduction to Statistical Pattern Recognition. Academic Press, New York and London, 1972.
8. Behrens M., Roht B. Biometrische Identifikation. Springer Vertrag, 2001.
9. Mitsiukhin A. // Proc. 52. IWK. 2007. Vol. 2. P. 321–325.
10. Гонсалес Р., Вудс Р. Цифровая обработка изображений. М., 2005.

*UDC 004.031.43:004.76*

# IOT COMPONENTS FOR PRODUCTION QUALITY MONITORING

U.A. VISHNYAKOU, S.H. AL-HAJJ, A.H. AL-MASRI, B.H. SHAYA

*Belarusian State University of Informatics and Radioelectronics, Republic of Belarus*

*Submitted 1 November 2021*

**Annotation.** To automate the creation of IoT systems, design tools are used in the form of IoT platforms. The structure of the stack in the IoT network is considered. The connection of sensors with means of primary processing, including protocols and data structure, is described. A generalized algorithm for creating a network using the IoT plat-form Bluemix from IBM is presented. The forms of the developed user interface are described.

*Keywords*: IoT networks, IoT platform components, IoT network modeling.

## Introduction

With the continued development of large and small networks in infocommunication (WAN, LAN) intended for the Internet of People (IoP), a variety of Internet of Things (IoT) networks are becoming more widespread [1].

The structure of the IoT network includes milk analyzers, gateways-converters, a cloud platform, and mobile devices [2]. The cloud platform rents a server that hosts knowledge and data bases, special software (solver) for processing and making decisions on milk quality, and a farm website. The database of the cloud structure server stores milk quality characteristics, and the knowledge base stores the rules for processing them. The solver outputs deviations from the current milk quality indicators from the standards. The site is used for communication of specialists in milk quality control. Monitoring of milk quality characteristics is implemented from mobile devices of specialists with access to the site components.

The 4th generation LTE network using NB-IoT technology was chosen as the network for transmitting information from dairy farms to the cloud. The review of milk analyzers of both domestic and foreign companies is carried out. A gateway solution for querying milk analyzers and transmitting parameters to the cloud infrastructure is presented [3, 4].

## IoT structure

As part of the Internet of Things network, five components can be distinguished [5]: sensors (devices) and their hardware, software for sensor management, communication tools, cloud platform and mobile applications. Let's consider the purpose of each of these components [2].

Devices act as an interface between the physical and digital worlds. They are the first layer of the IoT technology stack. Only one sensor may be needed for simple data collection. For more complex data, collection, it may need a computer that contains many sensors, a processor, local storage, a gateway, etc. At this level of the IoT technology stack, it is important to understand such parameters of equipment as cost, size, ease of deployment, reliability, useful life, service, etc.

Device software is the second layer of the IoT technology stack. It is a component that turns a device's hardware into a «smart device». Device software includes the concept of «software-defined hardware», which means that a particular hardware de-vice can serve multiple applications depending on the firmware it runs on.

The device software allows communication with the cloud or other local devices. You can perform analytics in real time, collect data from device sensors and monitor parameters. The device

software layer consists of two components: the operating sys-tem and the device applications. If the device is simple, the OS may not be used. The application can analyze the data from the sensors, comparing them with the boundary values. If the data exceeds the permissible, it is transmitted to the cloud for monitoring by the operator.

Communications − the third level of the IoT stack, includes both physical net-works and the protocols that will be used. The implementation of the communication layer can be found in the hardware and software of the device. But in terms of the conceptual model, you can keep communication as a separate layer to facilitate discussion during development.

Choosing the right communication mechanisms is an important part of an IoT product strategy. It will determine not only how data is transferred to and from the cloud (using different subnets and protocols: Wi-Fi, 4G, LoRA, etc.), but also how communication with other devices is organized.

The cloud platform (the fourth layer of the IoT stack) is the basis of the IoT network (project), which provides the infrastructure that supports all components: de-vice management, data collection and management, data analytics, cloud interfaces, in-formation security. Smart devices will transmit information to the cloud. You need to be aware of the type and amount of data that will be collected daily, monthly and annually.

Analytics refers to the ability to process data, find patterns, make predictions, integrate machine learning, and so on. The ability to find information from data makes a solution useful. Analytics can be as simple as aggregating and displaying data, or as complex as using machine learning or artificial intelligence. Cloud interfaces allow clients and managers to either interact with devices or exchange data. You may need separate applications for desktops, mobile devices, and for different categories of users.

## Algorithm for connecting sensors with primary processing

For simulated IoT monitoring of parameters, we use a scheme for reading readings of measured physical quantities (indicators of product quality or environmental parameters). Then they are preprocessed and the application is sent to the client via the IoT platform. The final stage is displaying data on the client side. The generalized net-work design algorithm is represented by three steps:

1. Select a sensor or a set of sensors from which we will receive the measured data, and a method for processing the received data.
2. Determining how we will communicate with sensors, determine the amount of data and understand how we will build interaction.
3. Find a suitable client for our network and describe the work with him.

For the sensor and pre-processor, we will choose the SensorTag 2 circuit from Texas Instruments [6]. Another option is Arduino with BLE-shield (Bluetooth low energy, low power) or BLEduino.

Inside the CC2650 chip, the SensorTag 2 core, is a real-time operating system (TI-RTOS), which together with the BLE stack provides reliable control of three different microcontrollers:

1. The core of the first microcontroller is Cortex-M3 (it usually runs the custom application we have written).
2. The core of the second - Cortex-M0 (responsible for the physical layer, radio communication).
3. A separate controller for sensors (helps to quickly receive data from them).

Android phones with BLE stack support are widespread, we will use it as a hub and gateway on the way to the cloud.

Generalized algorithm for creating a network by means of the IoT platform. Consider an IoT network modeling algorithm, which is divided into two parts. First, we organize the transfer of information from the sensors using a smartphone (three levels of the IoT stack), then we connect the cloud platform and implement the remaining two levels of the IoT stack.

To send the data received to the gateway (smartphone) via the BLE protocol to the Internet, we use the MQTT protocol and the JSON data transfer format.

MQTT (Message Queue Telemetry Transport) is a simplified network layer protocol for exchanging messages between devices, it runs on top of the TCP/IP stack and is designed to connect sensors, microcomputers, smartphones, tablets. MQTT is a publisher/subscriber. A publisher (devices of type publishers) sends a message, which is published in a centralized service (a message broker), and a subscriber (devices of type subscriber) receives a message from the broker.

JSON (JavaScript Object Notation) is a textual data interchange format based on JavaScript and used with this particular language. The format is considered language independent and can be used with any programming language. For this, there is a ready-made code for creating and processing data in JSON format.

JSON text is (encoded) one of two structures:

− a set of key-value pairs. In various languages, this is implemented as an object, record, structure, dictionary, hash table, keyed list, or associative array. The key can only be a string (case-sensitive: names with letters in different cases are considered different), the value can be any form.

− an ordered set of values. In many languages, this is implemented as an array, vector, list, or sequence.

These are universal data structures: as a rule, any modern programming language supports them in one form or another. They formed the basis for JSON, as it is used to exchange data between different programming languages.

A common implementation of the MQTT protocol is the Paho MQTT library, which is implemented for common programming languages: C/C++, Java, JavaScript, Python, etc. Let's consider the algorithm of communication between the client and the cloud.

1. Import the Paho MQTT library and the classes we need to work with the MQTT protocol.
2. Indicate the address of the cloud.
3. Set the number of the standard port of the broker of the cloud platform of the MQTT protocol.
4. Send data to the cloud platform.
5. The hub/gateway device (android phone) generates MQTT packets and transmits them to the cloud for storage and processing.
6. From the cloud, the hub can receive commands for device control or for the gateway.

Then we will create our web service to receive and display the readings of our sensors. To do this, we will use the cloud platform from IBM − Bluemix [7], which is needed to implement storage services, analytical processing and visualization of data received from SensorTag and pumped through an android phone. Bluemix is a PaaS (Platform as a Service) open source cloud offering based on the Cloud Foundry open source project. The platform is designed for application development and hosting, and it also simplifies infrastructure management.

**Bluemix platform using**

Building a cloud platform app. In Bluemix terminology, an application is any generated code (source code or executable binaries) that must be run or referenced at runtime. Mobile apps run outside of the Bluemix environment and use the services provided by the apps. In the case of web applications, an application is code uploaded to the Bluemix platform for hosting purposes. In addition, the platform is capable of hosting the application code that we want to run on an internal server in a container-based environment [7].

A service is code that runs on the Bluemix platform and offers specific functionality that applications can use. This can be a ready-made service used directly, such as push notifications for mobile apps or elastic caching for a web app. You can create your own services ranging from simple utility functions to complex business logic.

There are three steps to using services in Bluemix:

1. Tell the Bluemix platform that we need a new instance of the service and specify which particular application will use this new instance.
2. Bluemix automatically initializes a new instance of this service and associates it with the application.
3. The application interacts with the service.

Service bundles are collections of APIs used in specific areas. For example, the Mobile Services package includes MobileData, Cloud Code, Push, and Mobile Application Management services. The available services and runtimes are listed in the Bluemix catalog. In addition, you can register your own services.

In the platform, we will choose Node-RED because of its convenience and ease of configuration. It has a convenient graphical programming interface consisting of JS blocks, which can be described by loading a JSON file. You can also use some Node.js.

The data from the MQTT package is sent to the broker as part of the IoT Foundation service. A data subscriber is a Node-RED application that allows you to manipulate data using simple visual aids. Many primitive processing units (nodes) are JavaScript applications connected to each other by streams of data.

## User interface forms

The authors have developed a number of screen forms for working with users through applications. They can be grouped as follows.

1. Input.
2. Special.
3. Profile.

The user's work begins with the choice of language (forms input, Fig. 1). Then the user is authenticated with the ability to input the login and password (input form, Fig. 2).


Fig. 1. Select language


Fig. 2. Input login, password

In a special mode, the user can view product quality parameters from some farm and for a certain period of time (Fig. 3). In case of the output of some parameter foreign values, the user receives a notification (Fig. 4).


Fig. 3. Input firm for control

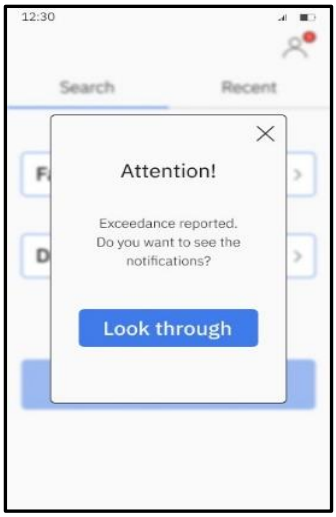



Fig. 4. Some parameter foreign values

Profile forms allow user to change his account and language.

## Conclusion

The article considers the structure of the IoT network for monitoring milk quality includes analyzers, gateways-converters, cloud platform, and mobile devices. The connection of sensors with means of primary processing, including protocols and data structure is described. A generalized algorithm for creating a network using the IoT platform Bluemix from IBM is presented. The authors have developed a number of screen forms for working with users through applications.

## References


1. Roslyakov A.V. Internet of things: textbook manual. Samara: Pgutii, 2015.
2. Visniakou U.A. [et al.] // SA&AI. 2021. № 1. P. 39−44.
3. IoT Platforms. [Electronic resource]. URL: http://www.tadviser.ru/index.php.
4. Rentiuk V. // Control Engineering. Россия. 2018. № 3(75). P. 82−87.
5. Daniel Elizalde. The 5 Layers of the IoT Technology Stack. [Electronic resource]. URL: https://danielelizalde.com/iot-primer/.
6. How to create an IoT for yourself. Learning to do the Internet of things on Android and hardcore hardware. [Electronic resource]. URL: https://xakep.ru/2016/04/28/iot-android-sensortag/.
7. Platform description Bluemix. [Electronic resource]. URL: https://searchcloudcomputing.techtarget.com/definition/IBM-Bluemix.

*УДК 654.16*

# СРАВНЕНИЕ СОТОВЫХ ТЕРМИНАЛОВ ПО УСТАНАВЛИВАЕМОЙ ДЛЯ ИЗЛУЧЕНИЯ МОЩНОСТИ

В.А. АКСЕНОВ, С.В. СМОЛЯК

*Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь*

*Поступила в редакцию 1 ноября 2021*

**Аннотация.** Предлагается методика экспериментального сравнения сотовых терминалов с точки зрения потенциальной опасности их радиоизлучения для здоровья человека. Для нескольких моделей смартфонов представлены результаты измерений устанавливаемой ими для излучения мощности в условиях реальной сотовой сети.

*Ключевые слова*: SAR, пилотные сигналы, логические каналы, петля регулирования мощности излучения, деградация чувствительность приемника.

## Введение

Повсеместное использование мобильных терминалов сотовой и иной радиосвязи, появлении новых стандартов такой связи, использующих все более высокие частоты для своей работы, вызывает резонную озабоченность общественности степенью опасности этих устройств для здоровья человека. Наиболее популярной численной метрикой для измерения величины вредного воздействия мобильных телефонов на человека, рекомендованной, в частности, Международным союзом электросвязи (ITU), является SAR (англ. Specific Absorption Rate), или удельный коэффициент поглощения. SAR измеряется в ваттах на килограмм, в пересчете на 1 грамм тканей в США, и в пересчете на 10 граммов тканей в Евросоюзе. Как альтернативный вариант, например, в России используется своя система измерения излучаемой мощности в ваттах на квадратный сантиметр.

С самого своего появления научная состоятельность и методика измерения SAR вызывают шквал критики с разных сторон. Показательно, что к этой критике подключился даже ITU. Приведем цитату из рекомендаций [1] этой организации: «Безопаснее ли мобильные телефоны с низким SAR? Нет. Отклонения в максимальном сообщенном SAR отражают различные технические параметры, такие как используемая антенна и ее размещение внутри устройства. Однако эти различия не означают, что существуют различия в безопасности. SAR разработан для демонстрации соблюдения соответствующих национальных или международных ограничений».

После таких комментариев становиться понятным, что вопрос об оценке вредного воздействия мобильных телефонов на человека остается открытым.

## Методики сравнительного анализа терминалов в условиях реальной сети

Важнейший пункт критики методики измерения SAR – оторванность выполняемых в лабораторных условиях измерений от особенностей функционирования терминалов в реальной сотовой (или иной) радиосети. Но возможно-ли какое-либо численное сравнение потенциальной опасности для здоровья человека мобильных терминалов, работающих в реальной сети?

Для выяснения этого были проведены опыты по наблюдению за выбираемой мощностью радиоизлучения, устанавливаемой смартфонами разных моделей при их работе в реальной сети, но при фиксированной геометрии расположения радиосредств. Схема эксперимента показана на рис. 1. Эксперименты были выполнены при технической помощи сотрудников сотового оператора A1. Измерения проводились в центральном офисе компании, где имеется indoor-

покрытие в стандарте сотовой связи 3G UMTS на частоте диапазона 2100 МГц. Для измерений использовался профессиональный аппаратно-программный комплекс семейства TEMS фирмы Erickson.


Рис. 1. Схема эксперимента по наблюдению за устанавливаемой мощностью излучения

Комплекс TEMS позволяет считывать все системные инструкции и измерения, которые смартфон принимает или выполняет. В частности, это величины, используемые при работе так называемой открытой петли регулирования мощности в UL (UL open-loop Power Control). В оригинальном именовании, принятом в стандартах UMTS [2], это измеренный уровень мощности пилотных сигналов базовой станции *CPICH RSCP* ( Common Pilot Channel Received Signal Code Power) и устанавливаемая смартфона начальная мощности на передачу *Initial PRACH Tx power* , или мощности преамбулы логического канала случайного доступа PRACH (Physical Random Access Channel). Алгоритм открытой петли регулирования мощности очень прост: чем меньше будет измеренный *CPICH RSCP* (в дБм с минусом), тем более высокую мощность на передачу *Initial PRACH Tx power* установит смартфон для обращения к базовой станции.

Вычисление начальной мощности осуществляется по формуле

$$Initial\ PRACH\ Tx\ power = Primary\ CPICH\ Tx\ power - CPICH\ RSCP + \\ + Uplink\ Interference + Constant\ value,$$

где *Primary CPICH Tx power* – мощность пилотного сигнала на передаче (на стороне базовой станции); *CPICH RSCP* – измеряемое мобильной станцией значение мощности пилотного сигнала на приеме (на стороне мобильной станции); *Uplink Interference* – интерференция в канале UL, или иначе RTWP (Received Total Wideband Power), которая измеряется базовой станцией; *Constant value* – константа, призванная учесть тот факт, что сигналы базы и мобильной станции передаются в разных частотных полосах (частотный дуплекс).

Величины *Primary CPICH Tx power*, *Uplink Interference* и *Constant value* передаются базовой станцией всем мобильным терминалам в соте по широковещательному логическому каналу BCH (Broadcast Channel). В соответствии со стандартом UMTS [2], эти параметры принимают значения, показанные в табл. 1.

Табл. 1. **Значения параметров для установки начальной мощности**

| Параметр | Диапазон значений, дБм | Точность установки, дБм | Типовое значение на сети, дБм |
|---|---|---|---|
| *Primary CPICH Tx power* | от –10 до +50 | 1 | +19 |
| *Uplink Interference* | от –110 до –70 | 1 | –105 |
| *Constant value* | от –35 до –10 | 1 | –20 |

Изменение текущее значение *CPICH RSCP* в условиях фиксированного расстояния до антенны базовой станции обусловлено следующими причинами. Это влияние работы в открытой сотовой сети, где рядом работают другие соты с такими-же пилотными сигналами и на той-же частоте. Присутствует переменная многолучевость как в данной соте, так и у соседей, вызванная перемещением всевозможных отражателей (люди, машины, иные объекты). Сказывается влияние пульсирующего трафика сот. В результате, эффект изменения уровня принимаемого терминалом *CPICH RSCP* принято называть «зашумлением пилотных сигналов».

Далее для сокращения записей будем использовать обозначения *RSCP* и *Tx*, соответственно, для измеряемой мощности пилотов и устанавливаемой мощности на передачу.

**Результаты измерений устанавливаемой для излучения мощности**

Ниже анализируются результаты опытов для смартфонов Samsung Note4 и Samsung Galaxy S6. В эксперименте проводилась запись *RSCP* и *Tx* один раз в секунду.

В качестве примера на рис. 2 и рис. 3 показаны результаты записи *RSCP* и *Tx* для смартфона Samsung Note4. На графики нанесена линия скользящего среднего по результатам 50-ти измерений (красная сплошная линия) и приведены значения глобального среднего арифметического значения измеряемых величин.

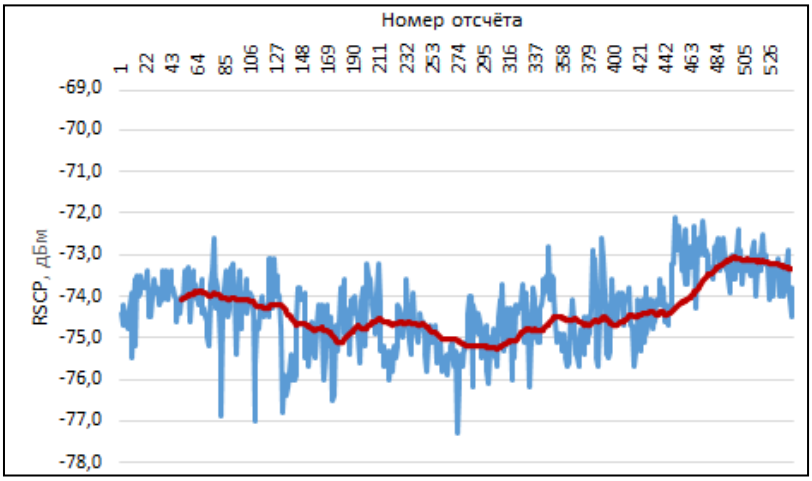



Рис. 2. Результаты измерений *RSCP*
смартфоном Samsung Note4 (среднее значение –74,3 дБм)

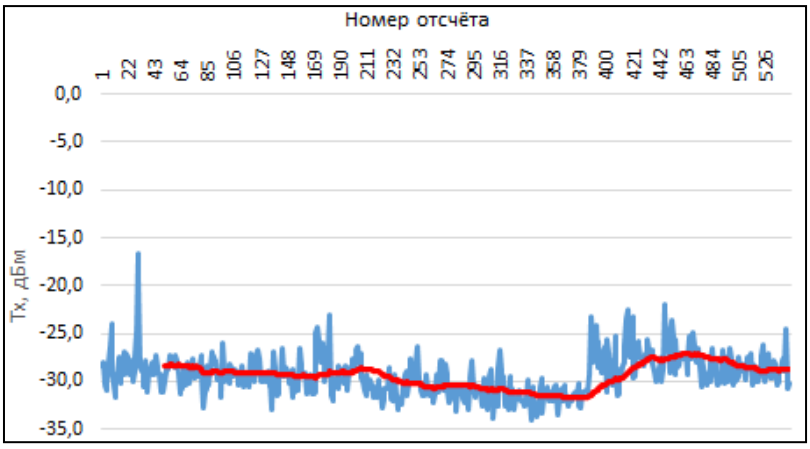



Рис. 3. Установленная мощность на передачу *Tx*
у Samsung Note4 (среднее значение –29,6 дБм)

Для удобства анализа средние значения для двух смартфонов сведены в табл. 2. Находясь в условиях фиксированной дальности до антенны базовой станции, смартфоны уверенно измерили и установили на передачу существенно разные уровни.

Табл. 2. **Сравнение результатов измерений**

| Модель смартфона | Среднее *RSCP* | Среднее *Tx* |
|---|---|---|
| Samsung Note4 | –74,3 дБм | –29,6 дБм |
| Samsung Galaxy S6 | –80,9 дБм | –16,8 дБм |
| Разница в значении | 6,6 дБ | 12,8 дБ |

Бросается в глаза, что разница в значении *Tx* практически равна удвоенному значению разницы в *RSCP*. Можно утверждать, что смартфон Samsung Galaxy S6 имеет устойчивую деградацию чувствительности своей антенны (и приемника в целом) приблизительно на 6 дБ в сравнении с Samsung Note4. Другими словами, этот аппарат сначала на 6 дБ «ошибается» в вычислении уровня пилотных сигналов, а затем еще раз добавляет эту ошибку в устанавливаемое значение для мощности передачи. Уместна жизненная аналогия: глухой человек старается громче разговаривать. В результате, можно с большой долей достоверности утверждать, что смартфон Samsung Galaxy S6 всегда будет пытаться излучать большую мощность, чем сравниваемый с ним Samsung Note4. Соответственно, он будет потенциально более опасен для здоровья пользователя.

С причинами деградации эффективности антенн и чувствительности приемников смартфонов можно ознакомиться, например, в [3, 4].

## Заключение

Таким образом, показана работоспособность методика оценки степени опасности мобильных терминалов здоровью человека, основанная на накоплении и усреднении значений *RSCP* и *Tx* в условиях фиксированного месторасположения этих терминалов в реальной сети.

Отметим, что в других стандартах сотовой и иной цифровой беспроводной связи, терминалами также используется алгоритм «меряю тестовый сигнал – устанавливаю мощность». Поэтому и для них предлагаемая методика будет продуктивной.

## COMPARISON OF CELLULAR TERMINALS IN POWER INSTALLED FOR RADIATION

V.A. AKSYONOV, S.V. SMOLYAK

**Abstract.** A method is proposed for the experimental comparison of cellular terminals from the point of view of the potential danger of their radio emission for human health. For several models of smartphones, the results of measurements of the power set by them to radiate under the conditions of a real cellular network are presented.

*Keywords*: SAR, pilot signals, logical channels, power control loop, receiver sensitivity degradation.

## Список литературы

1. K series – Supplement 1 (05/2020) to ITU-T K-series Recommendations. ITU-T K.91 – Guide on electromagnetic fields and health. Page 17. [Электронный ресурс]. URL: https://www.itu.int/rec/T-REC-K.Sup1-202005-S/en.
2. 3GPP Technical Report TR 25.951 V11.0.0 (2012-09) [Электронный ресурс]. URL: http://www.arib.or.jp/english/html/overview/doc/STD-T63v10_60/5_Appendix/Rel11/25/25951-b00.pdf.
3. Pedersen G.F. Mobile Phone Antenna Performance 2018. Institut for Elektroniske Systemer, Aalborg Universitet. [Электронный ресурс]. URL: https://vbn.aau.dk/ws/portalfiles/portal/292015653 MobilephoneTest2018Dec19.pdf.
4. Khan R. [et al.] User Influence on Mobile Terminal Antennas: A Review of Challenges and Potential Solution for 5G Antennas. [Электронный ресурс]. URL: https://core.ac.uk/download/pdf/188365752.pdf.

*УДК 061.68*

# ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ ФРАГМЕНТА СЕТИ ЭЛЕКТРОСВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ С ТЕХНОЛОГИЕЙ IPSEC В СЕТЕВОМ СИМУЛЯТОРЕ NS-3

С.С. ВРУБЛЕВСКИЙ, Е.В. МАШКИН

*Военная академия Республики Беларусь, Республика Беларусь*

*Поступила в редакцию 31 октября 2021*

**Аннотация.** Разработан класс для сетевого симулятора Network Simulator 3, имитирующий работу VPN-шлюза. Показано, что разработанный класс работает имитирует основные процессы протокола IPSec.

*Ключевые слова*: имитационное моделирование, стек протоколов IPSec, Network Simulator 3.

## Введение

Виртуальная частная сеть (Virtual Private Network – VPN) – представляет собой выделенную сеть передачи данных, построенную на инфраструктуре телекоммуникационной сети общего пользования, в которой конфиденциальность и защищенность информации пользователя обеспечивается механизмами шифрования и разграничения трафика (рис. 1) [1].

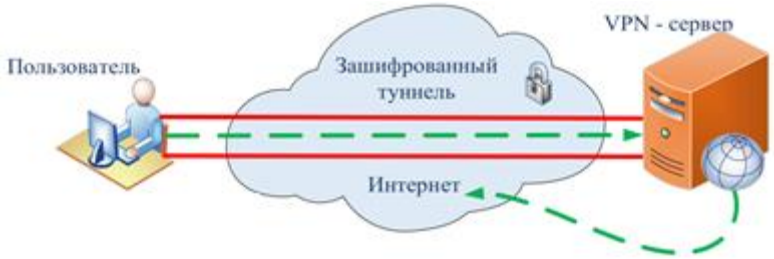



Рис. 1. Виртуальная частная сеть

Виртуальные частные сети подразделяются на:

– сети, построенные на оборудовании, которое устанавливается на стороне клиента и служит для его подключения к сети провайдера;

– сети, построенные на оборудовании, которое устанавливается на стороне провайдера.

И те, и другие подразделяются на три класса в зависимости от принципа организации связи пользователей сети:

– ведомственные (внутрикорпоративные) сети VPN – как правило, строятся на собственной сетевой инфраструктуре без использования ресурсов сети связи общего пользования;

– межведомственные (межкорпоративные) сети VPN – используют как собственную сетевую инфраструктуру, так и инфраструктуру сети провайдера;

– сети VPN удаленного доступа – данный класс сетей VPN предполагает подключение пользователя к сети VPN при помощи специального аппаратного (криптомаршрутизаторы) и программного (Cisco AnyConnect Secure Mobility Client, Avast SecureLine VPN) обеспечения.

Виртуальные частные сети могут быть реализованы на базе протоколов модели OSI на следующих уровнях:

– канальный – L2VPN (L2TP, PPTP, VPLS, VPWS);

– сетевой – L3VPN (IPSec, GRE, BGP/MPLS, VPRN);

– сеансовый – L5VPN [2].

Создание ведомственных (замкнутых) сетей VPN оправдано при использовании аппаратуры IP-шифрования с целью разграничения общего и зашифрованного трафика. Примером ведомственных сетей VPN могут служить сети электросвязи специального назначения (СЭСН), банковские сети и др. На сегодняшний день в СЭСН для создания сетей VPN используется стек протоколов IPSec.

## Стек протоколов IPSec и его особенности

Стек протоколов IPSec обеспечивает аутентификацию, целостность и конфиденциальность при помощи алгоритмов шифрования, хеширования, открытых ключей и цифровых сертификатов, стандартизованного консорциум Internet Engineering Task Force (IETF). Стек протоколов IPSec включает в себя протоколы:

– аутентификации – Authentication Header (AH);

– шифрования – Encapsulated Security Payload (ESP);

– обмена ключами – Internet Key Exchange (IKE).

Протоколы AH и ESP могут передавать данные в двух режимах:

– туннельном (IP-пакеты защищаются целиком, включая их заголовки);

– транспортном (защищается только содержимое IP-пакетов).

Широкое распространение нашел туннельный режим работы данных протоколов. В данном режиме исходный пакет инкапсулируется в новый IP-пакет, и передача данных по сети выполняется на основании заголовка нового IP-пакета.

Основным достоинством протокола IPSec является то, что данный протокол поддерживает все виды приложений (видеоконференцсвязь, VoIP, передача данных и т.д.) и может шифровать или аутентифицировать весь трафик на сетевом уровне. Но в тоже время использование данного протокола уменьшает скорость передачи информационных потоков, а также увеличивает время доставки пакета данных в сети.

## Имитационная модель фрагмента сети с технологией IPSec в сетевом симуляторе Network Simulator 3

Для создания надежно функционирующей СЭСН необходимо еще на этапе проектирования знать возможные характеристики узлов сети, ввиду того что современный мультисервисный трафик, циркулирующий в сети обладает свойствами самоподобия, который не поддается строгому математическому анализу. Основным инструментом анализа может являться имитационное моделирование без использования реального сетевого оборудования.

Одним из средств имитационного моделирования компьютерных сетей является сетевой симулятор Network Simulator 3 (NS-3). Данная среда моделирования представляет собой симулятор сети связи с дискретными событиями, предназначенный для исследований и использования в образовательных целях. Поддерживает большой стек протоколов и позволяет моделировать компьютерные сети с различными топологиями. Является бесплатным программным обеспечением с открытым исходным кодом (C++ / Python), а также работает с внешними инструментами анимации, анализа данных (создает файлы формата .pcap для работы с Wireshark, а также трейс-файлы в формате ASCII) и визуализации (NetAnim) [3].

Для имитации VPN-туннеля на основе технологии IPsec была создана модель фрагмента СЭСН (рис. 2) с помощью симулятора NS-3, которая состоит из трех оконечных устройств и одного маршрутизатора [4].


*а* *б*

Рис. 2. Фрагмент СЭСН с VPN-туннелем: *а* – схема сети; *б* – схема сети в NetAnim

Для проведения имитационного моделирования необходимо пройти четыре этапа (рис. 3):

– создание C++ – скрипта, описывающего модель сети;
– получение результатов;
– анализ результатов с помощью трейс- и .pcap файлов;
– визуализация процессов в сети.


Рис. 3. Этапы моделирования фрагмента СЭСН с помощью NS-3

Каждое из сетевых устройств имеет свой IP-адрес. Но при создании туннеля им присваивается виртуальные адреса. Для этого был разработан класс Tunnel, в котором реализуется данная функция. Для проверки функционирования имитационной модели поток UDP-трафика от host_3 передается с виртуального адреса 11.0.0.1 на host_1 с виртуальным адресом 11.0.0.254, что видно из рис. 4. На котором изображено событие моделирования, показывающее передачу потока трафика между виртуальными адресами, а также видно, как пакет с данными (в синей рамке) инкапсулируется в пакет IPSec (в желтой рамке).

```
+ 1.00914 /NodeList/0/DeviceList/1/$ns3::PointToPointNetDevice/TxQueue/Enqueue
ns3::PppHeader (Point-to-Point Protocol: IP (0x0021)) ns3::Ipv4Header (tos 0x0
DSCP Default ECN Not-ECT ttl 64 id 0 protocol 17 offset (bytes) 0 flags [none]
length: 568 10.1.1.1 > 10.1.3.1) ns3::UdpHeader (length: 548 667 > 667)
ns3::Ipv4Header (tos 0x0 DSCP Default ECN Not-ECT ttl 64 id 0 protocol 17
offset (bytes) 0 flags [none] length: 540 11.0.0.1 > 11.0.0.254)
ns3::UdpHeader (length: 520 49153 > 9) Payload (size=512)
```

Рис. 4. Событие моделирования, показывающее передачу потока трафика между виртуальными адресами

В таблице показано влияние процедур функционирования VPN-шлюза на параметры передаваемого UDP-трафика: пиковую ($p$) и среднюю ($r$) скорость передачи информационных потоков, длину генерируемых пакетов ($L$).

**Значение параметров трафика на входе и на выходе VPN-шлюза**

| Место измерения параметров трафика | Значения параметров трафика | | |
|---|---|---|---|
| | $p$, Мбит/с | $r$, Мбит/с | $L$, Байт |
| На входе VPN-шлюза | 2,3 | 0,91 | 1482 |
| На выходе VPN-шлюза | 1,80 | 1,23 | 1530 |

Исходя из выходных данных моделирования можно сделать вывод, что каждый пакет передается с одного виртуального интерфейса на другой, использование VPN-шлюза влияет на параметры передаваемого трафика, уменьшая скорость передачи информационных потоков и увеличивая длину IP-пакета.

## Заключение

Таким образом разработанный класс Tunnel для фрагмента сети полностью имитирует применение технологии IPSec, что видно из проведенных испытаний данного класса. Данный класс позволит создать модель полной СЭСН с VPN. Что и является дальнейшим направлением исследования.

# SIMULATION OF A SPECIAL PURPOSE TELECOMMUNICATION NETWORK FRAGMENT WITH IPSEC TECHNOLOGY IN THE NS-3 NETWORK SIMULATOR

S.S. VRUBLEVSKY, E.V. MASHKIN

**Abstract.** A class for the network simulator Network Simulator 3 has been developed to simulate the operation of a VPN gateway. It is shown that the developed class works by simulating the basic processes of the IPSec protocol.

*Keywords:* simulation, IPSec protocol stack, Network Simulator 3.

## Список литературы

1. Mitra D., Morrison J.A., Ramakrishnan K.G. Proc. of the 18th Annual Joint Conference of the IEEE Computer and Communications Societies, 1999. 490 p.
2. Сапрыкин А.В. Исследование и разработка методов анализа вероятностно-временных характеристик узлов сетей связи специального назначения: автореф. дис. канд. тех. наук: 05.12.13 / А.В. Сапрыкин; Поволжский гос. ун-т телекоммуникаций и информатики. Самара, 2018. 16 с.
3. NS-3 Model Library [Electronic resource]. URL: https://www.nsnam.org/docs/models/ns-3-model-library.
4. NS-3 Manual [Electronic resource]. URL: https://www.nsnam.org/docs/manual/ns-3-manual.pdf.

*УДК 004.052.32*

# ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ СИСТЕМЫ АВТОМАТИЗИРОВАННОГО ТЕСТИРОВАНИЯ УСТРОЙСТВ ИНТЕГРИРОВАННОГО ДОСТУПА

А.А. ИПАТОВИЧ

*Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь*

*Поступила в редакцию 31 октября 2021*

**Аннотация.** Разработана программа автоматизированного тестирования устройств интегрированного доступа, работающих по технологии ADSL. Представлены структурная схема программы и функциональный алгоритм тестирования устройств интегрированного доступа. Описаны этапы тестирования функциональных узлов устройств интегрированного доступа, приведены используемые программные инструменты.

*Ключевые слова:* автоматизированное тестирование, устройство интегрированного доступа, ADSL.

## Введение

Процесс ремонта абонентских устройств интегрированного доступа (IAD) включает в себя следующие этапы: диагностика, устранения неисправностей и тестирование, при котором производится проверка работоспособности всех узлов и контроль основных параметров. С течением времени растет как количество выходящих из строя устройств, так и разнообразие возникающих неисправностей. Некоторые из таких неисправностей проявляются лишь при длительной эксплуатации абонентских устройств, что значительно усложняет процессы диагностики и тестирования на рабочем месте по ремонту. Достижения высокого результата при тестировании устройств интегрированного доступа возможно лишь при достаточно большой длительности теста и высокой степени автоматизации.

Разработана система автоматизированного тестирования устройств интегрированного доступа, которая представляет собой аппаратно-программный комплекс, обеспечивающий полный автоматический цикл тестирования всех функциональных узлов IAD. Система поддерживает распространенные модели IAD производителей ZTE и Huawei, а также предусматривает возможность расширения списка поддерживаемых устройств [1].

В статье представлено программное обеспечение системы автоматизированного тестирования устройств интегрированного доступа и дано описание работы основных ее функциональных компонентов.

## Структура программы автоматизированного тестирования IAD

Структура программы системы автоматизированного тестирования устройств интегрированного доступа обусловлена составом аппаратной части и способами взаимодействием ее элементов. Исходя из решаемых задач и архитектуры тестируемых устройств определены основные функциональные возможности программы:

– автоматическая конфигурация тестируемых устройств с использованием их веб-интерфейса;

– контроль параметров ADSL соединения путем взаимодействия с терминалом мультисервисного модуля доступа DSLAM;

– тестирование IP-телефонии: контроль статуса VoIP регистрации на сервере, совершение автоматических вызовов на тестируемое устройство, контроль определителя номера и качества канала тональной частоты;

– контроль сетевого соединения устройства;

– мониторинг уровня сигнала Wi-Fi;

– нагрузочное тестирование: пропускание трафика, симулирующего работу IPTV, через абонентское устройство и контроль потери пакетов;

– графический пользовательский интерфейс.

Структура разработанной программы автоматизированного тестирования IAD представлена на рис. 1. Функциональный алгоритм тестирования IAD отображен на рис. 2.

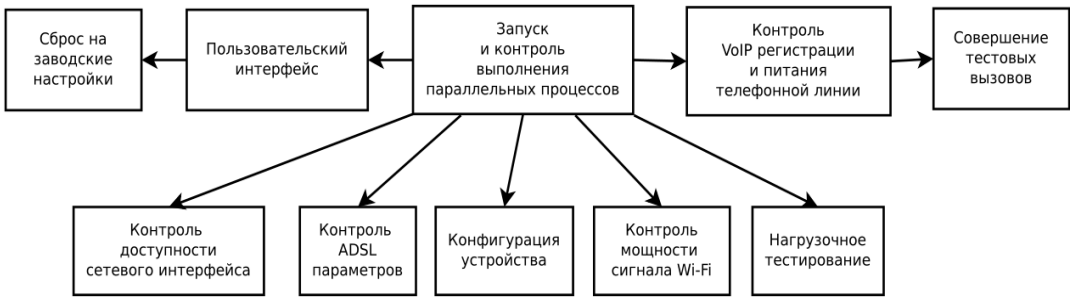



Рис. 1. Структурная схема программы

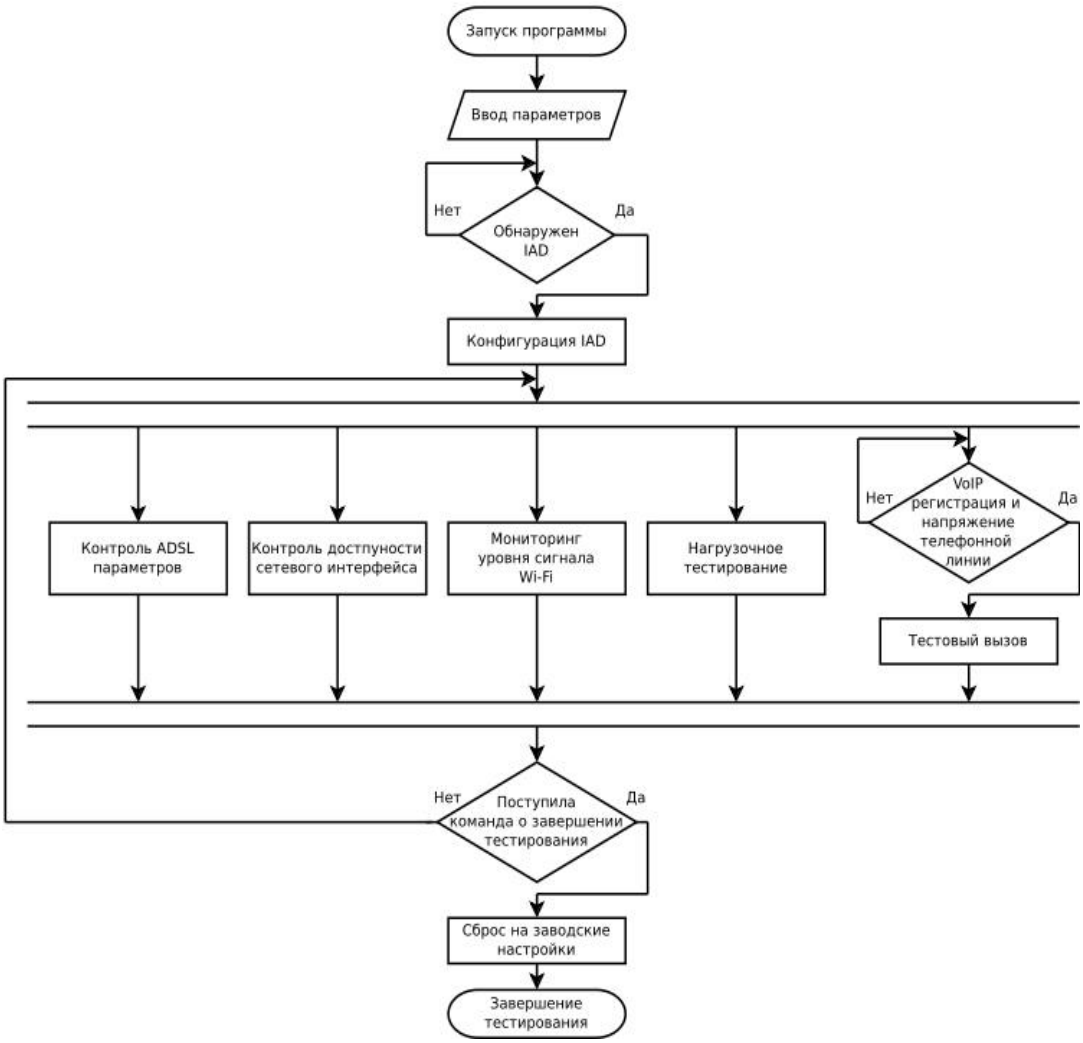



Рис. 2. Функциональный алгоритм тестирования IAD

При выборе языка программирования для написания кода программы системы были определены следующие критерии.

1. Наличие библиотек для реализации функций IP-телефонии.
2. Наличие инструментов для автоматизированного взаимодействия с веб-интерфейсом тестируемых устройств для их конфигурации.
3. Поддержка работы с протоколами SSH, Telnet для взаимодействия с сервером телефонии, мультисервисным модулем доступа DSLAM, а также сетевым коммутатором.
4. Поддержка работы с интерфейсом RS-232 для управления коммутатором телефонных каналов и dial-up модемом;
5. Работа с базами данных.
6. Наличие библиотек для разработки пользовательского графического интерфейса, поддерживающего построение графиков и работу с файлами.
7. Работа системы предусматривается в среде операционной системы семейства Linux.

В качестве основного языка программирования был выбран Python. Данный язык имеет широкий спектр библиотек для работы с сетевыми протоколами, управления базами данных, автоматизации процессов, создания графического интерфейса и организации IP-телефонии [2].

Для одновременного тестирования всех функциональных узлов устройств интегрированного доступа программа должна работать в асинхронном режиме. Для реализации асинхронности при написании программы была использована библиотека Subprocess, позволяющая запускать отдельные скрипты, написанные на языке Python, параллельно, без ожидания их завершения [3]. Так как все контролируемые параметры тестируемого устройства записываются в базу данных и обрабатываются независимо друг от друга, то для этого необходима система управления базами данных, поддерживающая работу с несколькими одновременными подключениями. В качестве такой системы была выбрана MySQL [4], а также библиотека драйвера подключений PyMySQL [5].

Главное окно программы представлено на рис. 3.

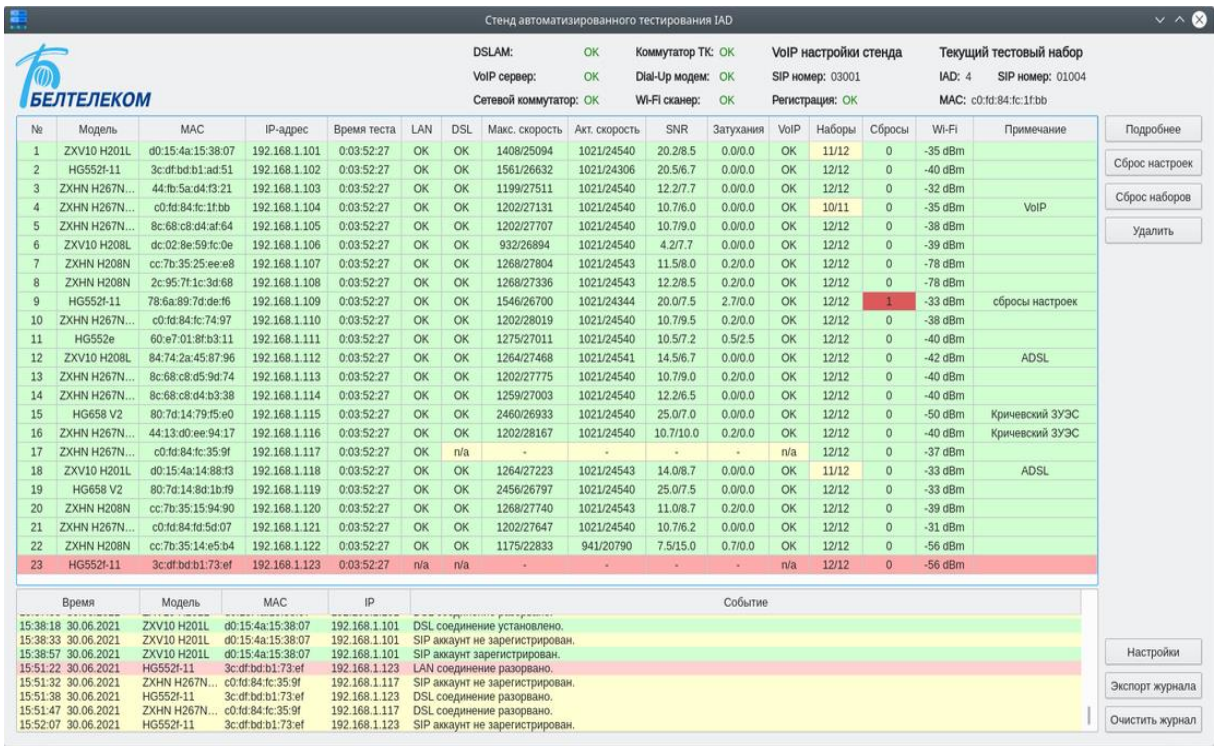



Рис. 3. Главное окно программы

Пользовательский интерфейс был разработан с использованием библиотеки PyQT5 [6]. В главном окне программы в виде таблицы отображаются все тестируемые устройства и их основные параметры. В нижней части главного окна программы отображается общий журнал событий системы. Пользовательским интерфейсом предусмотрена возможность сброса настроек устройства до заводских по окончании тестирования одним нажатием кнопки. Также

реализована возможность экспорта журнала событий в текстовый файл. При выборе одного устройства будут отображены его подробные характеристики, отдельный журнал событий, графики его ADSL параметров. Окно для отображения информации по тестируемому устройству приведено на рис. 4.

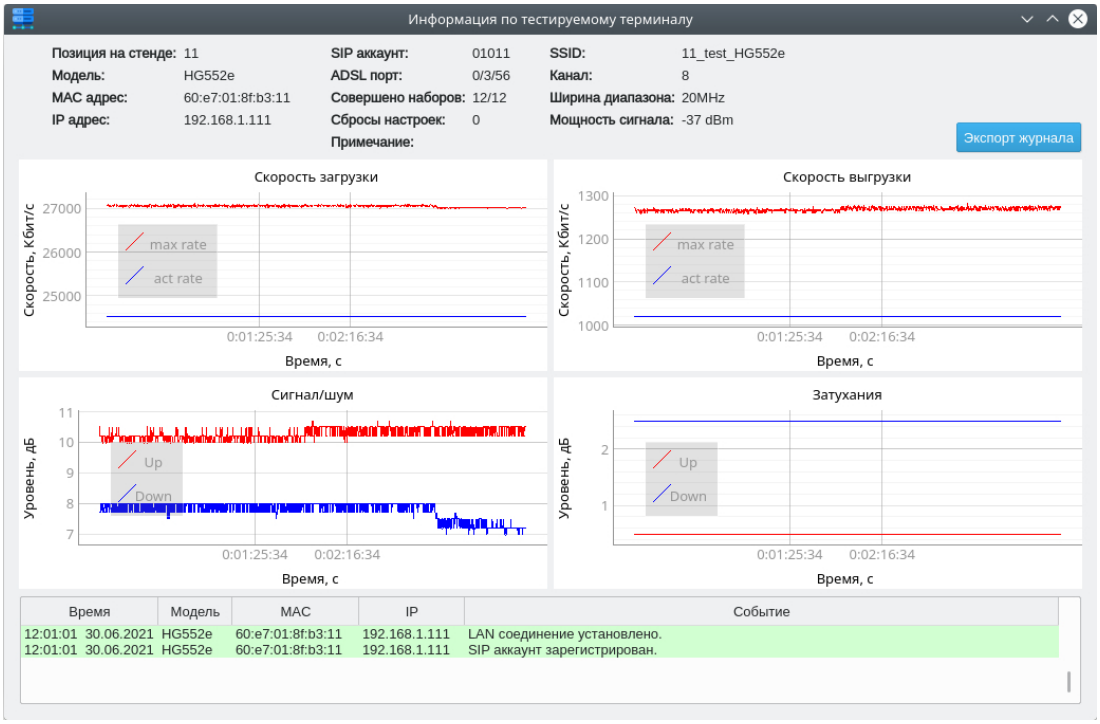



Рис. 4. Окно программы для отображения информации по тестируемому устройству

Изменение настроек абонентских устройств доступно только с использованием веб-интерфейса, так как протоколы Telnet и SSH в различных моделях устройств либо не поддерживаются, либо запрещены настройками безопасности по умолчанию. Для работы с веб-интерфейсом была выбрана библиотека Python Selenium, представляющая собой мощный инструмент автоматизации и поддерживающий множество параметров распространенных браузеров [7]. Для разработанной системы был использован браузер с открытым исходным кодом Chromium, а также драйвер chromedriver для автоматизированного взаимодействия с ним [8]. Для оптимизации работы программы браузер запускается в режиме headless (фоновый режим без графического отображения).

Автоматическая конфигурация абонентского устройства начинается сразу после его подключения к стенду и загрузки. Для обнаружения нового устройства система посылает ICMP запросы на IP адрес по умолчанию 192.168.1.1. После получения ответа на ICMP запрос запускается браузер и происходит направление на стартовую страницу настроек абонентского устройства. По анализу отображаемых элементов веб-страницы определяется производитель и модель устройства, автоматически вводится логин и пароль по умолчанию для входа в меню конфигурации. Далее программа производит поиск определенных HTML элементов веб-страницы, происходит взаимодействие с ними: нажатие на кнопки и пункты меню, ввод текста в определенные поля, чтение необходимых параметров. Таким образом происходит настройка VoIP, Wi-Fi, локального IP адреса устройства.

Также программой предусмотрено выявление случаев самопроизвольного сброса настроек тестируемых устройств. Для этого, при каждом обнаружении нового устройства происходит чтение его MAC адреса и поиск этого адреса в базе данных. Найденное совпадение говорит о том, что данное устройство уже находится в длительном тестировании, необходимо возобновление его конфигурации и фиксация факта произвольного сброса настроек в журнале событий.

Для более глубокой проверки отказоустойчивости отремонтированных абонентских устройств при длительном тестировании система позволяет обеспечить искусственную нагрузку. В качестве нагрузки выступает модель IP-TV трафика. Пакеты размером 1348 байт пропускаются

через тестируемое устройство по протоколу UDP со скоростью 8,5 Мбит/с, это соответствует IP-TV трафику при воспроизведении видео формата HD. Для передачи пакетов и контроля надежности их доставки создается сокет соединение. Каждый пакет нумеруется при генерации и отправке, порядковый номер записывается в полезной нагрузке. Также ведется счет общего количества принятых пакетов, которое каждый раз сравнивается с номером из полезной нагрузки. Разность данных величин и показывает количество не дошедших пакетов и представляет собой коэффициент потери пакетов IP (IPLR). Для мультисервисных систем этот параметр должен находится в пределах $10^{-3}$–$10^{-5}$ в зависимости от класса трафика в сети [9]. Более длительное тестирование под нагрузкой даст более объективный анализ качества передачи трафика. Потери пакетов могут происходить по разным причинам: неисправность узла ADSL и ухудшение параметров соединения, неисправность узла сетевых интерфейсов, повреждение микросхемы процессора и другие.

Контроль мощности сигнала Wi-Fi осуществляется с помощью отдельного устройства, выступающего в роли сканера сетей. Программа производит периодическое подключение к нему по протоколу Telnet с использованием библиотеки Telnetlib, выполняет сканирование и вывод результатов в терминал с помощью встроенных команд «wl scan» и «wl scanresult». Результаты в текстовом формате анализируются программой и заносятся в базу данных. На основании обновляемых данных о каждом тестируемом устройстве строятся графики изменения уровня мощности сигнала Wi-Fi во времени.

Для контроля параметров ADSL соединения каждого тестируемого устройства производится подключение к мультисервисному модулю доступа DSLAM Huawei SmartAX MA5600 по протоколу Telnet. В терминале модуля DSLAM циклически выполняются следующие команды [10].

1. «display mac-address vlan 116» – вывод таблицы MAC адресов всех активных устройств, установивших ADSL соединение с DSLAM (vlan 116 – предварительно настроенная виртуальная локальная сеть для IP-телефонии).

2. «display line operation board» – вывод параметров всех активных ADSL соединений выбранной сервисной платы.

Полученные данные в результате выполнения команд обрабатываются и заносятся в базу данных. По каждому тестируемому устройству строятся графики изменения основных параметров: уровень сигнал/шум, скорость соединения, исходящего и нисходящего потоков, затухания линии.

Для контроля доступности сетевого интерфейса абонентских устройств на каждое из них автоматически посылаются ICMP запросы (ping). В случае отсутствия ответа производится соответствующая запись в журнале событий.

Тестирование функций IP-телефонии производится после проверки регистрации IAD на сервере телефонии. С помощью библиотеки Python PJSUA2 совершаются автоматические вызовы на тестируемое устройство с контролем определителя номера [11]. После установления соединения программа воспроизводит аудио файл формата .wav, содержащий последовательность импульсов различной частоты, соответствующую DTMF комбинации «0123456789». Принятая на стороне IAD комбинация сравнивается с исходной. Искажение DTMF комбинации говорит о низком качестве канала тональной частоты. В этом случае производится соответствующая запись в журнале событий.

## Заключение

В статье описана работа программы для системы автоматизированного тестирования устройств интегрированного доступа, работающих по технологии ADSL. Приведена структурная схема и алгоритм программы, описаны методы автоматического тестирования функциональных узлов устройств. Разработанная система обладает высоким уровнем автоматизации и обладает свойствами масштабируемости.

# SOFTWARE OF THE SYSTEM OF AUTOMATED TESTING OF INTEGRATED ACCESS DEVICES

A.A. IPATOVICH

**Abstract.** The developed system of automated testing of integrated access devices operating on ADSL technology is considered. Methods of automated testing of functional units if device are described, software tools are given.

*Keywords*: automated testing, integrated access device, ADSL.

**Список литературы**

1. Ипатович А.А. // Инфокоммуникации: 57-я научная конференция аспирантов, магистрантов и студентов. Минск. БУГИР, 2021. С. 86–88.
2. Lutz M. Learning Python: Powerful Object-Oriented Programming. Sebastopol, 2013.
3. Бизли Д. Python. Подробный справочник. Санкт-Петербург, 2010.
4. Гольцман В. MySQL 5.0. Библиотека программиста. Санкт-Петербург, 2010.
5. PyMySQL Documentation. Release 0.7.2. [Электронный ресурс]. URL: https://readthedocs.org/projects/trio-mysql/downloads/pdf/stable/.
6. PyQT Python Binding. Tutorials point. [Электронный ресурс]. URL: https://www.tutorialspoint.com/pyqt/pyqt_tutorial.pdf.
7. Mathukadan B. Selenium with Python. [Электронный ресурс]. URL: https://selenium-python.readthedocs.io/.
8. ChromeDriver Documentation. [Электронный ресурс]. URL: https://chromedriver.chromium.org/.
9. Средства электросвязи мультисервисных сетей. Основные параметры и характеристики. СТБ 2156–2020. Минск, 2020.
10. SmartAX MA5600 Configuration Information. [Электронный ресурс]. URL: https://support.huawei.com/enterprise/en/access-network/smartax-ma5600-pid-17957
11. PJSUA2 Documentation. [Электронный ресурс]. URL: https://www.pjsip.org/docs/book-latest/html/.

*УДК 621.391.13*

# РАСЧЕТНЫЕ МОДЕЛИ ДЛЯ ОПРЕДЕЛЕНИЯ ПОМЕХОУСТОЙЧИВОСТИ И ЭФФЕКТИВНОСТИ СИСТЕМ СВЯЗИ С МНОГОПОЗИЦИОННОЙ МОДУЛЯЦИЕЙ КОМБИНИРОВАННЫМ КАСКАДНЫМ КОДИРОВАНИЕМ

Э.Б. ЛИПКОВИЧ, Е.А. БЕЛОКОНЬ

*Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь*

*Поступило в редакцию 1 ноября 2021*

**Аннотация**. Предложены математические модели расчета помехоустойчивости и эффективности систем связи с многопозиционными видами модуляции и комбинированным каскадным кодированием на базе несистематических сверточных кодов и недвоичных блочных кодов Рида-Соломона без необходимости привлечения в расчетах сложных процедур компьютерного моделирования и графических построений кривых помехоустойчивости.

*Ключевые слова*: помехоустойчивость, многокаскадное комбинированное кодирование, энергетическая и информационная эффективность, достоверность приема.

## Введение

В работе [1] представлены расчетные соотношения для прямого определения помехоустойчивости и энергетической эффективности систем связи с многопозиционной модуляцией и каскадным сверточным кодированием в зависимости от параметров кодов, характеристик модуляции и требуемой достоверности приема. Показано, что при использовании двух и более каскадов кодирования представляется возможным снизить отношение сигнал/шум (ОСШ) за счет выбора параметров режимов работы первой ступени декодирования и обеспечить требуемую достоверность приема за счет исправления ошибок принятым во внимание последующими ступенями.

В данной статье предложены расчетные модели для определения помехоустойчивости, энергетического выигрыша от кодирования (ЭВК) и информационной эффективности систем связи, использующих многопозиционные виды модуляции и каскадное комбинированное кодирование на базе несистематических сверточных кодов и блочных кодов Рида-Соломона (РС). Во внимание принято, что для борьбы с образованием блочных ошибок используется перемежение/деперемежение символов.

## Расчетные модели

Основываюсь на работах [1, 2], общее уравнение, увязывающее вероятность ошибки в информационном бите $P_{bN}$ на выходе приемной системы с многокаскадным декодированием и многопозиционной модуляцией с величиной отношения ОСШ $h_k^{'}$ на ее входе, представляется в следующем виде:

$$P_{bN} = \frac{C_i \cdot \mu_{ipN}}{q_i \cdot R_{pN}} \cdot \operatorname{erfc}\left(\sqrt{\mu_{ipN} \cdot h_k^{'}}\right); \quad (1)$$

$$\mu_{ipN} = \prod_{j=1}^{N} \mu_{ijN} = \mu_{i1N} \cdot \mu_{i2N} \cdot \mu_{i3N} \cdot \ldots \cdot \mu_{iNN}, \quad (2)$$

где $C_i$ – параметр, зависящий от вида и порядка модуляции; $\mu_{ipN}$ – результирующий показатель эффективности *N*-ступенчатого декодирования; $\mu_{ijN}$ – показатель эффективности декодирования *j*-й ступени; $R_{pN}$ – результирующая кодовая скорость *N*-каскадного кодирования; $q_i = d_0 / 4E_0$ – квадрат коэффициента помехоустойчивости; $d_0$ – минимальное расстояние между символами сигнального созвездия; $E_0$ – средняя энергия, переносимая битом информации; $h_k^{'} = E_0 / N_0$ – отношение энергии $E_0$ к спектральной плотности мощности шума $N_0$ ; $N$ – число ступеней кодирования; $j$ – номер ступени декодирования; $i$ – индекс, указывающий на принятый формат модуляции; $\mathrm{erfc}(Z)$ – функция определяемая выражением:

$$\mathrm{erfc}(Z) = \frac{2}{\sqrt{\pi}} \int_Z^{\infty} \exp\left(-u^2\right) du \cong \frac{1}{Z\sqrt{\pi}} \cdot 10^{-Z^2/2,3}. \qquad (3)$$

С учетом (3) уравнение (1) приводится к виду:

$$P_{bN} = \frac{C_i \sqrt{\mu_{ipN}}}{q_i \cdot R_{pN} \sqrt{\pi \cdot h_k^{'}}} \cdot 10^{-\mu_{ipN} \cdot h_k^{'} / 2,3} . \qquad (4)$$

Расчетные формулы для определения значений $C_i$ и $q_i$ при использовании М-позиционных сигналов с квадратурной амплитудой (КАМ-М), фазовой (ФМ-М), частотной (ЧМ-М), амплитудной (АМ-М) и относительной фазовой (ОФМ-М) модуляцией приведены в работе [1].

Согласно [1] для систем связи с многопозиционной модуляцией и $N$ – каскадным сверточным кодированием результирующий показатель эффективности $N$ – ступенчатого декодирования определяется следующим образом:

$$\mu_{ipN}^{(\mathrm{CK})} = q_i \prod_{j=1}^{N} d_{cj} \cdot \beta_{ijN}^{(CK)} \cdot R_{jN}^{(\mathrm{CK})} = \left(q_i \cdot d_{c1} \cdot \beta_{i1N}^{(\mathrm{CK})} \cdot R_{1N}^{(\mathrm{CK})}\right) \cdot \left(d_{c2} \cdot \beta_{i2N}^{(\mathrm{CK})} \cdot R_{2N}^{(\mathrm{CK})}\right) \cdot \ldots \cdot \left(d_{cN} \cdot \beta_{iNN}^{(\mathrm{CK})} \cdot R_{NN}^{(\mathrm{CK})}\right); \qquad (5)$$

$$R_{jN}^{(\mathrm{CK})} = \prod_{j=1}^{N} R_j^{(\mathrm{CK})};\ R_{1N}^{(\mathrm{CK})} = R_{pN}^{(\mathrm{CK})} = R_1 \cdot R_2 \cdot \ldots \cdot R_N; R_{2N}^{(\mathrm{CK})} = R_2 \cdot R_3 \cdot \ldots \cdot R_N, \qquad (6)$$

где $d_{cj}$ – свободное расстояние СК *j*-й ступени декодирования; $\beta_{ijN}^{(\mathrm{CK})}$ – функция взаимосвязи между параметрами *j*-й ступени декодирования; $R_{jN}^{(\mathrm{CK})}$ – кодовая скорость, учитываемая при оценке эффективности *j*-й ступени декодирования; $R_j = k_j / n_j$ – кодовая скорость *j*-го каскада на стороне передачи, номер которого отсчитывается от внутреннего каскада кодирования в сторону источника сигнала; $k_j$, $n_j$ – число символов на входе и выходе *j*-го каскада кодирования.

Входящая в (5), функция взаимосвязи между параметрами *j*-й ступени декодирования при *N*-каскадном сверточном кодировании рассчитывается по формуле:

$$\beta_{ijN}^{(\mathrm{CK})} = \left(1 - \frac{\lg\left(R_{jN}^{(\mathrm{CK})} \cdot d_{cj}\right)}{\left(n_j - k_j\right) \cdot \left(-\lg P_{bj}\right)}\right) \Big/ \left[1 + \frac{R_{jN}^{(\mathrm{CK})} \cdot \sqrt{P_{bj}}}{1 - R_{jN}^{(\mathrm{CK})}}\right], \qquad (7)$$

где $P_{bj}$ – вероятность ошибки на выходе *j*-й ступени декодирования.

**Значения свободного расстояния кода $d_{cj}$**

| $K_j$ | Значения $d_{cj}$ при кодовой скорости $R_j^{(\mathrm{CK})}$ | | | | | | |
|---|---|---|---|---|---|---|---|
| | 1/4 | 1/3 | 1/2 | 2/3 | 3/4 | 5/6 | 7/8 |
| 5 | 16 | 12 | 8 | 5 | 4 | 3 | 2 |
| 7 | 20 | 15 | 10 | 7 | 5 | 4 | 3 |
| 9 | 24 | 18 | 12 | 8 | 6 | 5 | 4 |

В таблице приведены значения $d_{cj}$ для избыточных сверточных кодов с $R_j^{(\text{СК})} = 1/n_j$ и перфорированных кодов с $R_j^{(\text{СК})} = (n_j - 1)/n_j$ в зависимости от $K_j$ при использовании оптимальных порождающих полиномов.

Из анализа (7) следует, что величина $\beta_{ijN}^{(\text{СК})}$ зависит не только от параметров соответствующей ступени декодирования, но и значения вероятности ошибки $P_{bj}$ на ее выходе. Диапазон изменения $\beta_{ijN}^{(\text{СК})}$ составляет от величин, близких к нулю при $P_{bj} \geq 5 \cdot 10^{-2}$, до единицы при $P_{bj} \to 0$. Чем меньше $\beta_{ijN}^{(\text{СК})}$, тем ниже эффективность декодирования $\mu_{ijN}$ рассматриваемой ступени.

Если каскадная кодовая конструкция строится на базе блочных недвоичных кодов РС, то результирующий показатель эффективности декодирования $\mu_{ipN}^{(\text{РС})}$ определяется следующим образом:

$$\mu_{ipN}^{(\text{РС})} = q_i \prod_{j=1}^{N} \beta_{ijN}^{(\text{РС})} \cdot (t_j + 1) \cdot R_{jN}^{(\text{РС})} = \\ = \left(q_i \cdot \beta_{i1N}^{(\text{РС})} (t_1 + 1) \cdot R_{1N}^{(\text{РС})}\right) \cdot \left(\beta_{i2N}^{(\text{РС})} (t_2 + 1) \cdot R_{2N}^{(\text{РС})}\right) \cdot \ldots \cdot \left(\beta_{iNN}^{(\text{РС})} (t_N + 1) \cdot R_{NN}^{(\text{РС})}\right); \quad (8)$$

$$R_{jN}^{(\text{РС})} = \prod_{j=1}^{N} R_j^{(\text{РС})}, \quad (9)$$

где $t_j = (n_j - k_j)/2$ – количество гарантированно исправляемых символов $j$-й ступени декодирования; $n_j = (2^l - 1)$ – общее число символов в кодовом слове; $l = log_2(n_j + 1)$ – число бит в символе; $k_j$ – число информационных символов в кодовом слове.

Минимальное кодовое расстояние для кодов РС:

$$d_{mj} = \left[2t_j + 1\right] = \left[n_j - k_j + 1\right]. \quad (10)$$

Расчетная формула для определения функции взаимосвязи между параметрами $j$-й ступени декодирования кодов РС следующая:

$$\beta_{ijN}^{(\text{РС})} = \left(1 - \frac{1{,}6 \lg\left(R_{jN}^{(\text{РС})} \cdot d_{mj}\right)}{\left(-\lg P_{bj}\right) + t_j \sqrt{P_{bj}}}\right) \Big/ \left[1 + \lg \frac{\left(t_j + 1\right)}{\left(1 - R_{jN}^{(PC)}\right) \cdot \left(-\lg P_{bj}\right)}\right]. \quad (11)$$

Исследование поведения функции $\beta_{ijN}^{(\text{РС})}$ показывает, что ее величина в области Заметных ошибок ($P_{bj} \geq 10^{-3}$) при условии $R_{jN}^{(\text{СК})} \cdot d_{cj} = R_{jN}^{(\text{РС})} \cdot (t_j + 1)$ существенно ниже значения $\beta_{ijN}^{(\text{РС})}$ сверхточных кодов, поскольку в выражении (11) с ростом ошибок увеличивается вес его знаменателя, снижающего $\beta_{ijN}^{(\text{СК})}$ и, соответственно, – значение эффективности декодирования $\mu_{ijN}^{(\text{РС})}$. Поэтому в первых каскадах декодирования, работающих в режиме с умеренным и большим уровнем ошибок, предпочтительно использовать сверхточные коды, позволяющие обеспечить лучшую компенсацию ошибок и рост $\mu_{ijN}$.

При расчете характеристик систем с комбинированным кодированием на базе сверхточных и блочных кодов РС вычисление осуществляется с использованием формул (5) – (7) или (8) – (11) в зависимости от рассматриваемого типа кода в соответствующих ступенях.

Базируясь на уравнении (4) представляется возможным выразить значение $h_k^{'}$ в зависимости от вероятности ошибки $P_{bj}$ на выходе заданной ступени декодирования $N$-

каскадного кодирования и получить расчетные формулы для прямого определения энергетической эффективности систем с многопозиционной модуляцией и каскадным однотипным или комбинированным кодированием:

$$h_k^{'} = \frac{2,3}{\mu_{ipj}}\left( D_{ij} - 0,5\lg\frac{2,3\left(D_{ij} - V_{ij}\right)}{\mu_{ipj}}\right); \quad (12)$$

$$D_{ij} = -\lg P_{bj} + \lg(\sqrt{\mu_{ipN}} \cdot \mathrm{x}_i);\ V_{ij} = 0,5 \cdot \lg\left(2,3 D_{ij} / \mu_{ipj}\right); \quad (13)$$

$$x_i = C_i / R_{pN} \cdot q_i \cdot \sqrt{\pi}, \quad (14)$$

где $\mu_{ijN}$ – результирующий показатель эффективности для учитываемых $j$-ступеней декодирования при использовании $N$-каскадного кодирования.

При незначительных и умеренных ошибках ($P_{bj} \le 10^{-4}$) на выходах рассматриваемых ступеней декодирования выражения (12) могут упростить и записать в виде:

$$h_k^{'} = \frac{2,3}{\mu_{ipj}}\left[ D_{ij} - 0,5 \cdot \lg\left(2,2 \cdot D_{ij} / \mu_{ipj}\right)\right]. \quad (15)$$

Из анализа соотношений (12) – (15) можно сделать следующие выводы:

– приведенные соотношения являются достаточно общими для определения ОСШ системы в зависимости от числа и параметров каскадных кодов, их результирующей эффективности декодирования $\mu_{ipj}$, заданных значений $P_{bj}$ на выходах учитываемых ступеней, характеристик модуляции $(q_i, C_i)$ и кодовой скорости $R_{pN}$;

– для минимизации значений ОСШ, при которых требуется помехоустойчивость необходимо повышать эффективность $\mu_{i1N} = \mu_{ip1}$ первой ступени декодирования, выбирать режим ее работы в области относительно больших уровней ошибок ($P_{b1} = 10^{-2} \ldots 10^{-3}$) и возлагать их исправление на следующие за ней ступени;

– для рационального построения многокаскадных кодовых конструкций необходимо, чтобы эффективность декодирования $\mu_{i1N}$ первый ступени превышала значения $\mu_{ijN}$ следующих ступеней в предположении их работы на месте предыдущей;

– число каскадов в кодовой конструкции ограничивается компромиссом между ее сложностью и величиной приращения энергетической эффективности от их использования, поскольку с увеличением числа каскадов растет избыточность на стороне передачи и снижается эффективность декодирования $\mu_{ijN}$ каждой из ступеней.

– при одноступенчатом декодировании каскадного кода значение ОСШ однозначно связано с величиной $P_{b1}$ на выходе первой ступени;

– с увеличением числа ступеней декодирования величина $h_k^{'}$ при фиксированном значении $P_{bj} = P_{b1}$ снижается за счет роста эффективности декодирования $\mu_{ipj}$, а при фиксированном значении $h_k^{'}$ снижаются значения $P_{bj}$ на выходах учитываемых ступеней декодирования за счет исправления ошибок каждой из них.

Если в (12) – (15) принять $\mu_{ipj} = q_i$ и, следовательно исключить параметры, связанные с кодированием, то получим соотношения для определения ОСШ без кодирования

$$h_0^{'} = \frac{2,3}{q_i}\left( A_i - \lg\sqrt{2,3\left(A_i - V_{i0}\right) / q_i}\right); \quad (16)$$

$$A_i = -\lg P_{b0} + \lg\frac{C_i}{\sqrt{\pi \cdot q_i}};\ V_{i0} = 0,5 \cdot \lg\left(2,3 \cdot A_i / q_i\right), \quad (17)$$

где $P_{b0}$ – вероятность ошибки на выходе устройства при отсутствии кодирования.

Различие между уровнями ОСШ при отсутствии и наличии кодирования для ровных параметров модуляций и значений ошибок ($P_{b0} = P_{bj}$) на выходах сравниваемых устройств определяет энергетический выигрыш от кодирования

$$\Delta G_{(0-j)} = 10\lg\left(h_0^{'} / h_{kj}^{'}\right) = h_0 - h_{kj} = 10\lg(\mu_{ipj} \cdot \varepsilon_{oj} / q_i)\text{, дБ.;} \quad (18)$$

$$\varepsilon_{oj} = \left(A_i - \lg\sqrt{2{,}3\left(A_i - V_{i0}\right)/q_i}\right) / \left(D_{ij} - \lg\sqrt{2{,}3\left(D_{ij} - V_{ij}\right)/\mu_{ipj}}\right), \quad (19)$$

где $h_0 = 10\lg h_0^{'}$, $h_{kj} = 10\lg h_{kj}^{'}$ – уровни ОСШ на входе приемной системы при отсутствии и наличии кодирования с учетом *j*-й ступени декодирования, дБ.

Из (18) – (19) видно, что величина ЭВК в основном зависит от отношения $\mu_{ipj} / q_i$ растет, согласно (2), с ростом числа и эффективности декодирования отдельных ступеней. При $P_{bi} \to 0$ значения $\varepsilon_{0j} \to 1$ , $\beta_{ijN} \to 1$ и асимптотическая величина ЭВК в случае использования трехкаскадного комбинированного кодирования по схеме СК+РС+СК с учетом (5) – (6) и (8) – (9) определяется следующим образом:

$$\Delta G_{(0-3)}^{(\max)} = 10\lg\left[dc_1\left(t_2+1\right)\cdot dc_3 \cdot R_1 \cdot R_2^2 \cdot R_3^3\right]\text{, дБ.} \quad (20)$$

Например, при $dc_1 = 5$ , $t_2 = 8$ , $dc_3 = 8$ , $R_1 = 3/4$ , $R_2 = 239/255$ , $R_3 = 7/8$ значение $\Delta G_{(0-3)}^{(\max)} = 17{,}75$ дБ.

Основываясь на полученных соотношениях (12) – (15) несложно определить рост ЭВК от наращивания ступеней декодирования, при условии равенства вероятностей ошибок на их выходах. Выполнив сравнение уровней ОСШ в системах с *j* и *N*-ступеней декодирования, получим:

$$\Delta G_{(j-N)} = 10\lg(h_{kj}^{'} / h_{kN}^{'}) = h_{kj} - h_{kN} = 10\lg(\mu_{ipN} \cdot \varepsilon_{iN} / \mu_{ipj})\text{, дБ;} \quad (21)$$

$$\varepsilon_{jN} = \left(D_{ij} - \lg\sqrt{2{,}3\left(D_{ij} - V_{ij}\right)/\mu_{ipj}}\right) / \left(D_{iN} - \lg\sqrt{2{,}3\left(D_{iN} - V_{iN}\right)/\mu_{ipN}}\right), \quad (22)$$

где $h_{kj}$, $h_{kN}$ – уровни ОСШ при использовании *j* и *N*-ступеней декодирования, дБ.

Из (21) – (22) видно, что величина $\Delta G_{(j-N)}$ в основном определяется отношением результирующих эффективностей декодирования при использовании *N* и *j*-ступеней. Значения $\mu_{ipN}$ и $\mu_{ipj}$ для сверточного и блочного декодирования рассчитываются на основании формул (5) – (6) и (8) – (9).

При использовании многокаскадного кодирования из-за вносимой на стороне передачи избыточности увеличивается по сравнению с режимом без кодирования величина $P_{b.\text{вх}}$ на входе первой ступени декодирования, значение которой согласно (4) при $\mu_{ipN} = q_i R_{pN}$ определяется по формуле:

$$P_{b.\text{вх}} = \frac{C_i}{\sqrt{q_i \cdot R_{pN} \cdot \pi \cdot h_k^{'}}} \cdot 10^{-q_i \cdot R_{pN} \cdot h_k^{'}/2{,}3}. \quad (23)$$

Рост $P_{b.\text{вх}}$ на входе первой ступени декодирования увеличивает $P_{b.1}$ на ее выходе и сокращает исправляющую способность $H_1$ определяется следующим образом:

$$H_1 = P_{b.\text{вх}} / P_{b1} = \left(\sqrt{q_i \cdot R_{pN} / \mu_{i1N}}\right) \cdot 10^{-q_i \cdot R_{pN} \cdot h_k^{'}/2{,}3}. \quad (24)$$

Анализ выражения (24) показывает, что при условиях $d_{c1} \cdot \beta_{ijN}^{(CK)} \le 1$ для СК и $(t_1+1)\beta_{ijN}^{(PC)} \le 1$ для РС величина $H_1 \le 1$ и исправление ошибок первой ступенью декодирования отсутствует. Выполнение этих условий возможно в режиме с достаточно большим уровнем ошибок ($p_{b1} \ge 10^{-2}$), когда $\beta_{ijN} \to 0$.

Исправляющая способность каждой последующей ступени декодирования; $\mu_{ip(j-1)}$ – результирующая эффективность декодирования от использования $(j-1)$ -ступеней.

$$H_i = P_{(j-1)} / P_{bj} = \left(\sqrt{1/\mu_{i1N}}\right) \cdot 10^{h_k^{'} \cdot \mu_{ip(j-1)}\left(\mu_{ijN}-1\right)/2,3}. \quad (25)$$

Взаимосвязь между значениями вероятностей ошибок на выходах *N*-й и *j*-й ступеней декодирования при известном значении ОСШ определяется согласно отношения

$$P_{bN} = P_{bj}\left(\sqrt{\mu_{ipN}/\mu_{ipj}}\right) \cdot 10^{-h_k^{'}\left(\mu_{ijN}-\mu_{ipj}\right)/2,3}. \quad (26)$$

Основываясь на полученных расчетных выражениях, представляется возможным определить информационную эффективность каналов связи, использующих многопозиционную модуляцию и комбинированное составное кодирование с одной или группой ступеней декодирования.

$$\eta_{\text{инф}} = B_0 / C = 0,3\gamma_0 / \lg\left(1 + h_k^{'} \cdot \gamma_0\right), \quad (27)$$

где $\gamma_0 = m \cdot R_{pN}$ – удельная скорость передачи данных, бит/симв.; $C$ – пропускная способность канала связи по Шеннону.

### Заключение

Предложенные математические модели расчета помехоустойчивости, энергетического выигрыша от кодирования и исправляющей способности отдельных ступеней декодирования систем связи, использующих многопозиционные виды модуляции и комбинированное каскадное кодирование на базе сверточных и блочных кодов РС. Базируясь на расчетных моделях возможных расширенные исследования по обеспечению высокой достоверности приема и низких значений ОСШ за счет вариации числа каскадов и параметров кодирования, структуры кодовой конструкции и режима работы использующих ступеней кодирования.

## CALCULATION MODELS FOR DETERMINING THE IMMUNITY AND EFFICIENCY OF COMMUNICATION SYSTEMS WITH MULTIPOSITIONAL MODULATION BY COMBINED CASCADE CODING

E.B. LIPKOVICH, E.A. BELAKON

**Abstract.** Mathematical models are proposed for calculating the noise immunity and efficiency of communication systems with multi-position modes of modulation and combined concatenated coding based on unsystematic convolutional codes and non-binary block Reed-Solomon codes without the need to involve complex computer modeling procedures and graphical constructions of noise immunity curves in the calculations.

*Keywords*: noise immunity, multistage combined coding, energy and information efficiency, reception reliability.

## Список литературы

1. Липкович Э.Б., Белоконь Е.А. // Кодирование и цифровая обработка сигналов в инфокоммуникациях: материалы международной научно-практической конференции (Республика Беларусь, Минск, 19 апреля 2021 года). Минск: БГУИР, 2021. С. 47–51.
2. Липкович Э.Б., Серченя А.А. // Электросвязь. 2020. № 10, С.62–66.

*УДК 004.85*

# МОДУЛЬ РАСПОЗНАВАНИЯ СЕТЕВОЙ РАЗВЕДКИ

Н.П. ШАРАЕВ, С.Н. ПЕТРОВ

*Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь*

*Поступила в редакцию 18 ноября 2021*

**Аннотация.** Изучена эффективность метода дерева решений в задачах обнаружения сетевой разведки. Приведены блок-схемы обученного дерева решений и работы модуля обнаружения признаков сетевой разведки.

*Ключевые слова*: сетевая разведка, аномалии сетевого трафика, метрики признаков сетевой разведки, датасеты.

## Введение

В последнее время наблюдается тенденция перехода от массовых кибератак отдельных злоумышленников к масштабным атакам киберпреступных группировок на конкретные организации (таргетированные атаки). Данные атаки в значительной мере опасны для организаций, в связи с созданием злоумышленниками вредоносного программного обеспечения с учетом специфики сетевой инфраструктуры организации.

В мировой практике задача обнаружения признаков сетевой разведки сводится к задаче обнаружения аномалий сетевого трафика, так как в обоих случаях наблюдается большое количество подозрительного трафика, преимущественно на третьем и четвертом уровнях модели OSI. Существуют датасеты для обучения моделей обнаружению аномалий сетевого трафика: Network Intrusion Detection [1]; UNSW_NB15 [2]; 2019 Trendmicro CTF Wildcard 400 [3]; Kitsune Network Attack [4]; NSL-KDD [5]; Network Traffic with Port Scanning Attack [6]. Путем анализа открытых источников были выбраны наиболее актуальные метрики и разработан датасет для обнаружения сетевой разведки [7].

Таким образом, актуальным является вопрос разработки модуля обнаружения признаков сетевой разведки и оценка эффективности его работы на созданном датасете.

## Метод дерева принятия решений в решении задач обнаружения сетевой разведки

Созданный JSON-датасет конвертируется в двумерную матрицу признаков. На данном этапе множество ответов представлено в формате строки («good», «bad») и для дальнейшей работы требуется перевести их в бинарный формат (0, 1). Указанное реализуется использованием класса LabelEncoder и перекодирует ответы следующим образом: «good» – 1, «bad» – 0. Матрица признаков, содержащая перекодированные ответы, с помощью класса train_test_split разделяется на обучающее (80 %, или 800 событий) и тестовое (20 %, или 200 событий) множества с помощью функции псевдослучайных чисел. Анализ созданных множеств показал наличие 201 события сетевой разведки в обучающей выборке (25 %) и 49 событий в тестовом множестве (25 %), что позволяет судить о сбалансированности выборок.

В результате исследования эффективности методов машинного обучения [8], наиболее быстрым методом, верно классифицирующим признаки сетевой разведки, признан метод дерева принятия решения (Decision Tree) с параметрами criterion = «gini» и splitter = «random», обучающимся за 0,000912 секунды.

Блок-схема обученного алгоритма дерева принятия решений представлена на рис. 1.

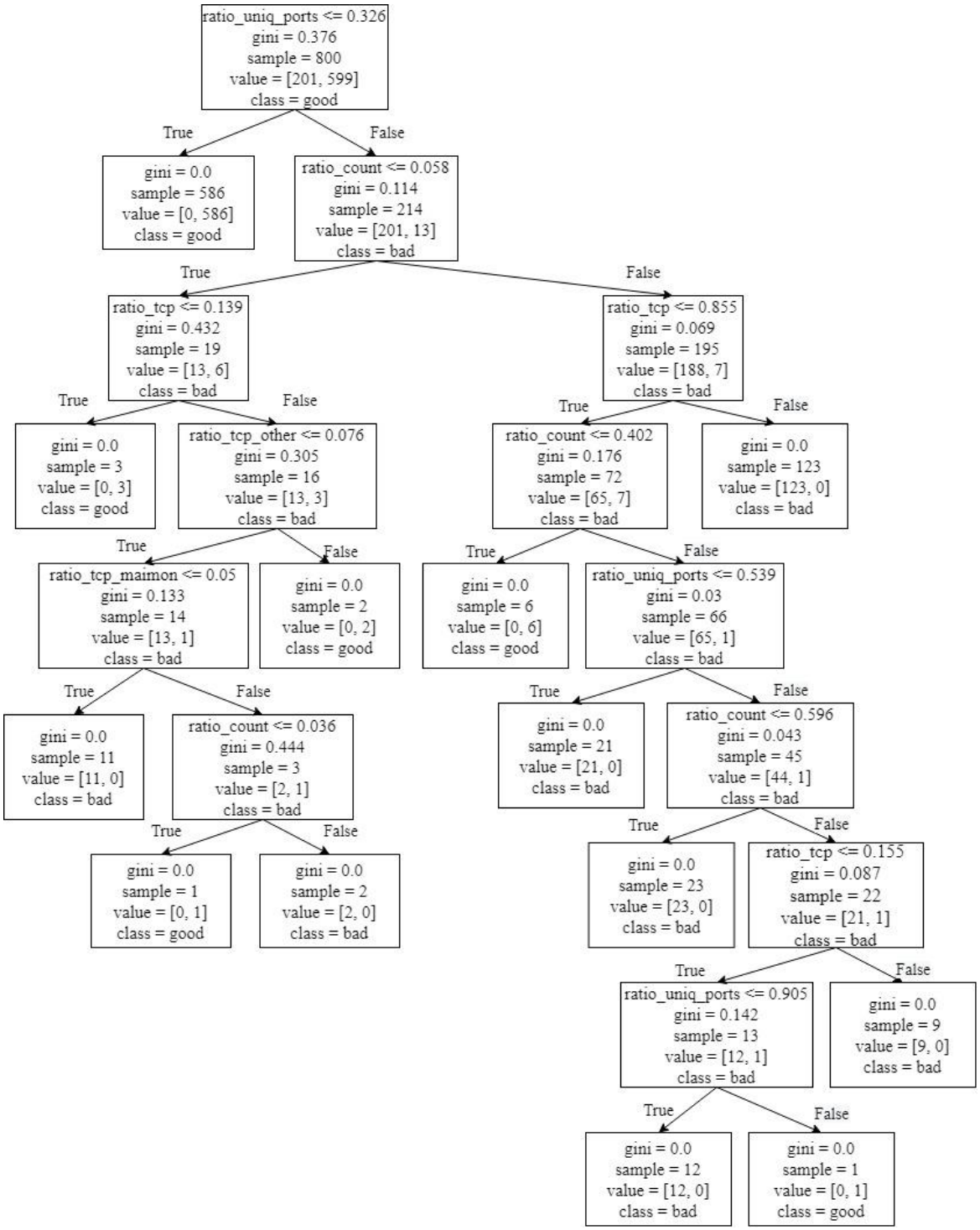



Рис. 1. Блок-схема обученного дерева принятия решений

Дополнительным плюсом применения указанного метода на практике является возможность описать его работу программным языком вместо применения обученной модели, что положительно скажется на производительности и объеме программного кода.

### Принцип работы модуля обнаружения признаков сетевой разведки

При запуске модуль обнаружения признаков сетевой разведки импортирует базовые и расширенные библиотеки для работы программы. При разделении программы на множество файлов создавался один основной файл (main.py), в котором инициализировались библиотеки threading, json и logging. Далее импортируются основные модули: Sniffer, DataStore, Analyitcs и

Model. Модули представляют собой отдельные интерпретируемые файлы (*.py), содержащие в себе программный код и предназначенные для логического разделения программы. После создается объект библиотеки logging, предназначенный для создания журнала событий, определяется формат записи события, путь к лог-файлу, а также уровень информирования в журнале событий. Далее загружается файл конфигурации. Если данный файл отсутствует, происходит преднамеренное завершение программы и информирование об отсутствии файла. Из файла конфигурации импортируются следующие параметры: количество событий в анализируемой выборке (по умолчанию 30 событий), время жизни одного события (по умолчанию 5 мин), переключатель создания модели (по умолчанию модель создается), путь к датасету (по умолчанию «module/data/dataset.json»), путь к модели (по умолчанию «module/data/model.pkl»), анализируемый интерфейс (по умолчанию «eth0»), массив исключенных из мониторинга IP-адресов (по умолчанию только loopback). На основе представленных параметров создаются объекты DataStore(), Sniffer(), Analytics() и Model(). При этом объекты Sniffer() и Analytics() создаются в новых потоках библиотеки threading (sniffer и analytics соответственно) и выполняются параллельно основному потоку ввода-вывода Python, а объект Model() передается объекту Analytics(). Потоки запускаются и проверяются на наличие ошибок при выполнении. В случае наличия ошибок основной поток ввода-вывода досрочно завершается и останавливает созданные потоки библиотеки threading.

Внутри потока sniffer после записи параметров конфигурации в поля класса происходит выполнение двух команд операционной системы для получения списка прослушиваемых портов и IP-адресов интерфейса. После получения указанной информации создается и запускается объект асинхронного сниффера класса scapy. При получении пакета данный сниффер проверяет, является ли данный пакет из стека TCP/IP, направлен ли он на закрытые порты транспортного уровня и не находится ли IP-адрес, на который он отправлен в списке исключение. Если на все вопросы ответ «правда» (true), то пакет нормализуется и записывается (метод запись события) в созданный объект DataStore(). Если нет – пакет не обрабатывается и считается легитимным. Дополнительно в классе есть методы запуска и остановки асинхронного снифера, что связано с отладкой приложения.

В классе DataStore() реализованы два метода: запись события и чтение всех событий. При записи события происходит извлечение из тела события IP-адреса источника. Базируясь на данной информации создается новый словарь, содержащий в себе в качестве ключа IP-адрес источника, а в качестве значения – словарь, состоящий из времени получения первого пакета с указанным IP и массива событий. В случае, если IP-адрес нового пакета уже существует в словаре, событие заносится в массив событий. Метод чтения всех событий возвращает словарь всех событий, хранящихся в поле объекта DataStore().

Внутри потока analytics происходит чтение событий из объекта DataStore(), инициализация объекта Model() и запуск метода проверки события. Метод проверки события запущен в бесконечном цикле и для этого и запущен в отдельном потоке. В данном цикле проверяется наличие в базе данных не более 100 различных исходящих IP-адресов. Это применяется для защиты от DDoS атак, в целях защиты от неограниченного потребления оперативной памяти. Если количество исходящих IP-адресов превышает параметр, происходит очистка базы данных объекта DataStore(). Далее для каждого исходящего IP-адреса формируется выборка из 30 событий (настраивается в конфигурационном файле). В случае, если данное число событий за 5 минут (настраивается в конфигурационном файле) не набралось, создается множество из не менее чем половины исходного параметра (в данном случае 15 событий). Если же и половины выборки не набралось – выборка удаляется. Представленный механизм экономит оперативную память и позволит выявлять сетевую разведку, проводимую за значительный промежуток времени. Выбор параметра в 5 минут основан на желании злоумышленника провести анализ запущенных в информационной системе служб в обозримый промежуток времени. Так, для набора минимального количества событий для анализа достаточно отправлять одно событие в 20 секунд, что для анализа 1000 популярных портов составляет 5,5 часа, на что вполне может пойти злоумышленник. После, базируясь на сформированной выборке, происходит расчет метрик и создается полностью нормализованное событие, предназначенное для анализа методами машинного обучения. Данное событие передается объекту Model(). В случае, если полученный результат анализа относится к классу сетевой разведки, данное событие логируется и содержит

время получения первого пакета, исходящий IP-адрес и все параметры нормализованного события. Таким образом, можно назначить автоматическую блокировку подозрительно IP-адреса на 5 минут с помощью утилиты fail2ban.

Блок-схема работы модуля обнаружения признаков сетевой разведки представлен на рис. 2.

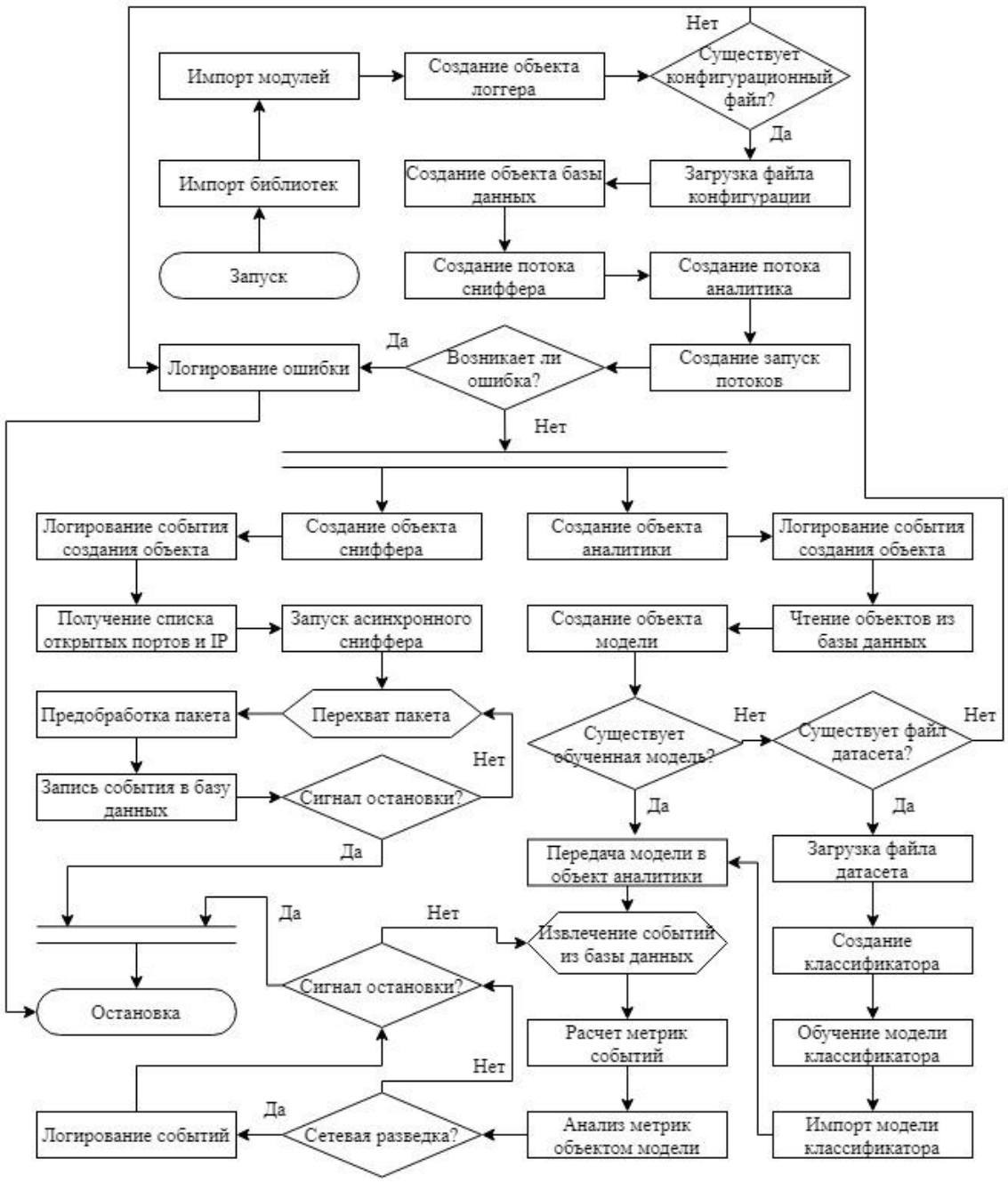



Рис. 2. Блок-схема работы модуля обнаружения признаков сетевой разведки

На момент создания объекта Model() происходит поиск существующей обученной модели машинного обучения. При ее наличии происходит загрузка в оперативную память. В случае ее отсутствия происходит создание новой модели, если этому не противоречит параметр конфигурационного файла (create_model). Когда параметр «create_model» переведен в состояние «false» или отсутствует файл датасета, выполнение программы завершается, журналируется событие ошибки и останавливаются все потоки. При создании новой модели происходит загрузка файла датасета, создание необходимого классификатора (в данном случае Decision Tree с параметрами criterion = «gini» и splitter = «random»), обучение классификатора и экспорт созданной модели классификатора для ускорения последующих загрузок программы. При

передаче в указанный объект события происходит его анализ классификатором и возврат результата проверки в объект Analytics().

Описанное программное обеспечение позволяет добиться значительной скорости работы в потоке, небольшого потребления оперативной и энергонезависимой памяти, качественного обнаружения признаков сетевой разведки и возможность интегрирования базовыми сторонними утилитами (типа fail2ban).

### Заключение

Разработана блок-схема работы модуля обнаружения признаков сетевой разведки. Описаны необходимые компоненты и зависимости модуля. Проведен анализ работы модуля, показавший 100 % обнаружения попыток проведения сетевой разведки. Наилучшие результаты показал метод дерева принятия решений с параметрами criterion = «gini» и splitter = «random», с точностью 100 % и скоростью работы 0,912 мс. Дополнительно проведено представление алгоритма с наилучшими параметрами в виде программного кода, что позволило увеличить скорость работы приблизительно в 2 раза.

## NETWORK INTELLIGENCE RECOGNITION MODULE

N.P. SHARAEV, S.N. PETROV

**Abstract.** The effectiveness of the decision tree method in network intelligence detection tasks has been studied. The flowcharts of the trained decision tree and the operation of the network intelligence feature detection module are given.

*Keywords*: network intelligence, network traffic anomalies, metrics of network intelligence features, datasets.

### Список литературы

1. Network Intrusion Detection – Kaggle. [Electronic resource]. URL: https://www.kaggle.com/sampadab17/network-intrusion-detection/.
2. UNSW_NB15 – Kaggle. [Electronic resource]. URL: https://www.kaggle.com/mrwellsdavid/unsw-nb15/.
3. 2019 Trendmicro CTF Wildcard 400 – Kaggle. [Electronic resource]. URL: Режим доступа: https://www.kaggle.com/hawkcurry/2019-trendmicro-ctf-wildcard-400/.
4. Kitsune Network Attack Dataset – Kaggle. [Electronic resource]. URL: https://www.kaggle.com/ymirsky/network-attack-dataset-kitsune/.
5. NSL-KDD dataset – Canadian Institute for Cybersecurity. [Electronic resource]. URL: https://www.unb.ca/cic/datasets/ nsl.html.
6. NTwPSA – Loughborough University Network Traffic with Port Scanning Attack. [Electronic resource]. URL: https://figshare.com/articles/dataset/Loughborough_University_-_Network_Traffic_with_Port_Scanning_Attack/4630282/3
7. Шараев Н.П., Петров С.Н. // Управление информационными ресурсами: материалы XVII Междунар. науч.-практ. конф., 12 мар. 2021 года. Минск. 2021. С. 238–240.
8. Sharaev N. // Education & applications on design and engineering during pandemic 2021: 7th Maltepe University International Student Congress (MUISC), 5–7 May 2021, Istanbul, Turkey, 2021. P. 47.

*UDC C 620.9:.658.26*

# IOT NETWORK: MODELS, STRUCTURE, COMMUNICATIONS, PROBLEMS

U.A. VISHNIAKOU, DU ZONGQI, LIU ZHENHUA, HU JIFENG, YU CHUNYU

*Belarusian State University of Informatics and Radioelectronics, Republic of Belarus*

*Submitted 8 November 2021*

**Annotation.** A brief analysis of the concepts and applications of IoT networks is carried out. Four models of building these networks as variants of component interaction are given: terminal, gateway, cloud, application. Variants of IoT network architectures are presented. Seven variants of interaction in Yota networks are considered. The analysis of problems in these networks and the direction of their solution are carried out.

*Keywords*: IoT networks, models, architectures, interaction, problems.

## Introduction

The concept of Internet of Things (IoT) originated from the network Radio Frequency Identification (RFID) system proposed by the Massachusetts Institute of Technology in the USA in the automatic identification laboratories, created in 1999 [1]. This system can connect all items to the Internet via radio frequency identification (RFID) and other equipment to read information and implement intelligent identification and management.

The Internet of Things is a technology that automates input, processing and optimization based on the obtained values of process characteristics reflected in the indicators of industrial and home sensors. The IoT technology allows the user to receive data and report on the status of equipment or processes in real time, monitor the work of industrial and agricultural enterprises [2]. The IoT has found its application in many areas [3]: smart car, smart home, smart city, smart agriculture, healthcare, etc.

Structurally IoT consists of four main components, which are: IoT devices; communication technologies; platforms for data storage and processing, applications [3]. IoT in a narrow sense refers to a network that connects objects with objects for the implementation of intellectual identification and management of objects. IoT in a broad sense can be considered as the integration of information space and physical space, digitization and integration of everything into a network. To achieve effective information interaction between objects, objects and people, as well as between people and the real environment and communication.

## IoT network models

From hardware to software, the IoT system includes a lot of content, but conceptually it is a hierarchical structure. From the bottom up, the IoT system can be divided into three levels: the perception level, the network level and the application level. This three-layer conceptual model of IoT has a great impact, but from a physical point of view, it is possible to imagine four varieties of physical models of IoT systems [3, 4].

The first model: «Cloud Terminal-Cloud» refers to all applications in the IoT system that will be deployed in the cloud; terminal refers to IoT objects, including hardware and software deployed on them. This model refers to the IoT system, divided into two parts: a cloud platform and a terminal. The cloud platform needs to implement a website so that people can manage it through a web page. The cloud platform should also implement a communication interface for interacting with things. The terminal contains sensors, devices, memory, etc. For performing local business functions, as well as for connecting to the Internet using wired and wireless means, this model can meet the requirements of most

IoT systems. The advantages of the model are simple structure, proven technology and relatively simple implementation of the system. However, its disadvantage is that the cost of the terminal is high and it is difficult to achieve large-scale deployment, and when using a wireless connection, high operating costs are required.

The second model: «Cloud-Terminal application». In this model, mobility has become an element that must be taken into account when designing application systems. To implement this model, the cloud platform needs to organize interaction with the application.

Application development is carried out on iOS, Android and Windows platforms, the background is connected to the cloud platform of IoT, and the application runs on a smartphone, computer and tablet. The model can accommodate complex functions that require significant system resources.

The disadvantage of this model is the increased complexity of the system, the need to provide real-time communication between the application and the client, security requirements and the need to establish various methods of interaction between the application and the terminal, for example, QR code, RFID, Bluetooth communication.

The third model: «Terminal-Gateway-Cloud-Application». Technical means require the endpoint to be connected to the Internet via a network port or via 2G/3G/4G means. But the first option has low mobility, the second has higher operating and maintenance costs, which does not contribute to the promotion of the system.

The gateway of the IoT is usually designed as an «Intermediate Software» for connecting the terminal to the Internet, up, it can be accessed via fiber, Ethernet, Wi-Fi or 2G/3G/4G, and down – via Wi-Fi, Bluetooth, ZigBee and other means of communication. The addition of a gateway allows the terminal to connect to the IoT using some short-range communication protocols, especially short-range wireless protocols such as Bluetooth, Wi-Fi, etc. This can reduce the cost of the terminal while improving usability. In addition, the gateway implements a small local network and various local terminals in this network can work together, which expands the application functions of the IB. But adding a gateway improves the overall performance of the system.

Fourth model: «Sensor-Networks». A sensor network is a network consisting of sensor nodes. Wireless sensor network is the main focus of this model development. In order to save energy, wireless sensor networks are usually designed with a low transmission rate, and it is difficult to provide real-time downlink control. From the point of view of communication, the wireless protocol network for sensors is basically not based on IP, so it is connected during the operation of the platform, the work on converting the existing protocol is also difficult to apply.

Because of these two limitations, wireless sensor networks are more commonly used in monitoring systems. For example, in agriculture and forestry, WSN (Wireless Sensor Network) can be used to monitor the growth environment, temperature, humidity, etc. The WSN can monitor various parameters of rivers and oceans; in the field of intelligent transport, the WSN can control street lights, etc.

With the development of technology, the ZigBee protocol has begun to fully support IPv6, and the development of low-power chips, security technologies, energy and other technologies will continue to contribute to the wider application of wireless sensor networks in more application areas [5].

## Architecture of IoT network

There are various models of the IoT architecture [6]: the reference architecture of the Industrial Internet of Things (IIRA), the reference model of the Industry 4.0 architecture (RAMI 4.0) and the reference model of the IoT Cisco. IoT architectures, such as P2413 (standard for the architecture of the IoT), the reference architecture of the Internet of Things (IoT RA), the Telecommunication standardization sector of the International Telecommunication Union (ITU-T), etc. However, no standard reference architecture has been widely adopted, because some IoT architectures are outdated, they do not define new technologies, such as cloud and fog computing, big data. The simplified IoT architecture is shown in Fig. 1.

It is necessary to classify the universal and simple architecture of the Internet of Things – a five-level model. This architecture includes the perception layer, network layer, platforms, application layer and business layer. Different levels include different technologies, depend on different areas and scenarios, and also include different technologies.

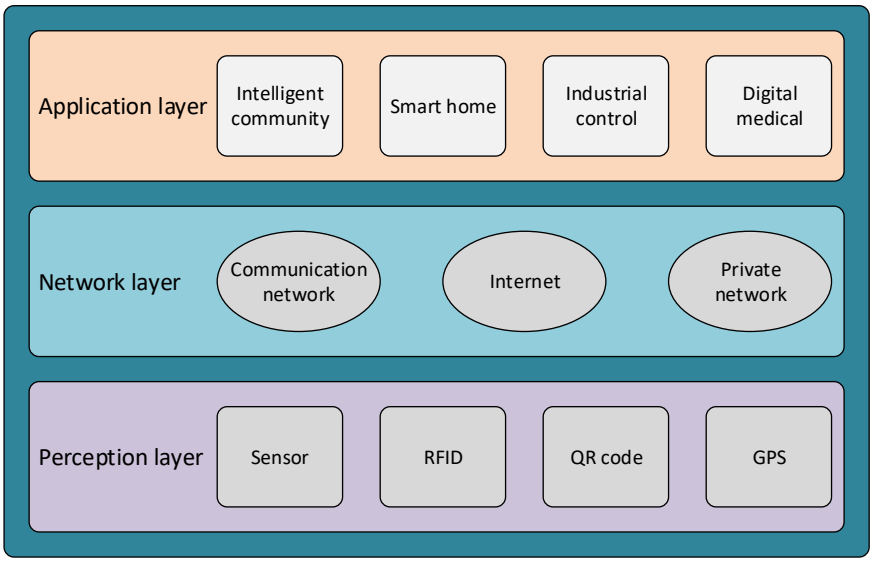



Fig. 1. IoT architecture

For the perception level, the main function is to collect and identify data, as well as transfer the necessary data to the network layer. For the network layer – identification, communication, security and routing are the four main functions. For the identification function at this level, the technology of a single resource identifier (URI), the electronic product code standard (EPC), the ubiquitous code system (UCODE) and IPv6 addressing protocols can be implied. To communicate with other nodes or server servers, it is necessary to use protocols such as power line communication (PLC), near field communication (NFC), ANT+, DASH7 Alliance Protocol (D7A). Standards such as X10, IEEE 802.15.4, Bluetooth with low power consumption, and technologies such as ultra-broadband (UWB), Wi-Fi, long-range broadband network (LORA WAN), 5G and Light Fidelity (Li-Fi), etc. for IoT are used.

There are many nodes with limited capabilities to ensure security, so this is a big problem, in addition, different communication technologies require different security technologies, so at this level, lightweight security technologies can be used, for example, Internet Protocol security (IPsec), transport layer security (TLS), TLS datagram (DTLS), IEEE 1888, etc. For routing, it is very important to find the optimal route for each node.

For the platform layer, also called the service management layer, which is the core of the IoT environment, data modification, processing, and the service discovery function should be taken into account. At this level, technologies such as, CoAP, MQTT, foggy, cloud should be used. At the application level, the main function is to provide services for Internet of Things users. At this level, the services provided are usually divided into four categories according to different application scenarios: identity-related services, information aggregation services, collaboration services, and ubiquitous services.

Two technologies are recommended for the IoT business level: semantics and big data analysis. To achieve semantics, the sensor model language (sensor ML), media types for the sensor markup language (SENML), the Internet of Things database (IOTDB), the RESTful API modeling language (RAML) and Wolfram data removal technologies will be used. To analyze big data, you can use Apache Spark, a distributed processing technology that includes caching, and to improve performance, it uses Apache Apex, Apache Flink and Apache Kafka technologies.

## Ways to interact with the IoT

Interaction in IoT networks faces some difficulties: how to make the IoT system distinguish between service objects and avoid the impact of non-service objects; the complexity of the environment, since the environment will not always be stable; hardware failure, it is very important for IoT devices to avoid failures depending on the actual state of the device. There are the following ways of interaction [4].

1. Touch screen interaction. The interactive method is widely used in the field of mobile phones and touch-screen devices, traditional and easy to use, it is not easy to make a mistake.

2. Voice interaction. By recognizing voice prints or initiating a command to interact, this interactive method is commonly used in voice assistants, voice speakers, and other areas. Based on energy consumption and privacy considerations, active voice activation is required.

3. Virtual Reality. This is a new visual perception technology, the technology is interactive, technological and more exciting for a real virtual experience.

4. Biometrics. This technology uses the unique information of a biological individual as a key and information transmission. Unique information usually refers to fingerprints, palm prints, voice prints, facial and iris recognition, etc. This type of interaction is very secure and unique.

5. Somatosensory technology. This type of interaction mainly includes gesture recognition, face recognition, body movement recognition, etc.

6. Information recognition technology. This type of interaction includes image recognition, text recognition, and object recognition. Simple processing and evaluation of information using intelligent recognition. This type of interaction can recognize a wide range of categories, but has limited processing complexity.

7. Traditional buttons. Control the user using physical buttons that directly provide the corresponding functions.

## Using the IoT in production quality control

The IoT is a technology that automates input, processing and optimization based on the obtained values of process characteristics reflected in the indicators of industrial and home sensors. The IoT technology allows some user to receive data and report on the status of equipment or processes in real time, monitor the work of industrial and agricultural enterprises [3].

Due to the advantages of the Internet of Things, the Internet of Things technology has a wide range of applications for product quality control. K. Rajalashmi [7] et al. sensors are used to monitor the pH and oxygen content in the water, the purity of the water can be easily calculated using sensors.

In [8], the architecture of the Internet of Things and network protocols for product quality control in the aerospace industry are proposed, and in [9], the model and structure of the Internet of Things network for milk quality control is proposed.

## Problems in networks

In real IoT networks, the placement and number of components can also cause some problems when connecting various components to the network [3, 4].

Overload: when the gateway location is placed unreasonably, it will lead to insufficient use of resources, that is, some gateways are overloaded, and some gateway resources are not fully used. This will not only lead to a significant reduction in the use of resources in the border network, but will also cause serious network congestion, which directly affects the quality of service for mobile users. Therefore, when deploying a gateway, it must be placed in a suitable location to achieve load balancing, improve the use of network resources and reduce network congestion, thereby ensuring the quality of user service.

Coverage: each gateway has its own coverage area. If the distance between the terminal device and the gateway is too large, this will lead to a decrease in the reception signal level. Therefore, we need to make sure that all terminal devices are in the gateway's coverage area, but at the same time it is necessary to minimize overlapping coverage and cover most devices with the least number of gateways, thereby ensuring network performance while increasing resource utilization and minimizing gateway deployment costs.

Interference: the location and number of gateways have a big impact on network performance. If the location of the gateways is unreasonable or the density of the gateway deployment is too high, there will be serious interference problems that will affect the SINR received by the terminal equipment., which will lead to a decrease in throughput, as well as an increase in construction costs, so optimizing the location and number of gateways is very important to reduce interference when deploying gateways.

All these problems require the use of system analysis and various optimization methods. Optimization models in infocommunication systems are considered in [10].

## Conclusion

1. A brief analysis of the concepts and applications of IoT networks is carried out. Four models of building these networks as variants of component interaction are given: terminal, gateway, cloud, application.

2. Variants of IoT network architectures are presented, including the perception level, network level, platform, application levels and business level. For each level the functions and technologies and protocols used are considered.

3. Seven variants of interaction in IoT networks are considered. The analysis of problems in these networks, such as overload, limited coverage, overload is carried out. To overcome them, it is proposed to use methods and technologies of system analysis and optimization.

## References


1. AutoID Labs homepage. [Electronic resource]. URL: https://www.autoidlabs.org.
2. International Telecommunication Union, Internet Reports 2005: The Internet of things[R]. Geneva: ITU, 2005.
3. Roslyakov A.V. Internet of things: textbook manual. Samara: Pgutii, 2015.
4. IoT Platforms. [Electronic resource]. URL: http://www.tadviser.ru/index.php.
5. Four models of IoT systems. [Electronic resource]. URL: https://blog.csdn.net/lihongzhai/article/%20details/80370369.
6. Sun QiBo, IoT: Architecture and key technology research review [J]. Journal of BeiJing University of Posts and Telecommunication, 2010,33(03):1–9.
7. Rajalashmi K. [et al.] IoT based water quality management system [J]. Materials Today: Proceedings, 2020.
8. Visniakou U.A. [et al.] // Siberian Journal of Science and Technology. 2020. № 4. P. 478-482.
9. Visniakou U.A. [et al.] // SA&AI. 2021. № 1. P. 39-44.
10. Nikulshin B.V. [et al.]. System analysis and decision-making in project and management activities: an educational and methodological manual on the academic discipline «Theory of system analysis and decision-making in infocommunications» for students of the II stage of the specialty «Systems and networks of infocommunications» of all forms of education. Minsk: BGUIR, 2021.

*УДК 004.627*

# ИССЛЕДОВАНИЕ СОКРАЩЕНИЯ ПСИХОФИЗИЧЕСКОЙ ИЗБЫТОЧНОСТИ В АЛГОРИТМЕ JPEG

Д.П. ГОРБУКОВА, Ю.М. БАКИМОВ, Т.М. ПЕЧЕНЬ

*Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь*

*Поступила в редакцию 15 ноября 2021*

**Аннотация.** Проведено исследование сокращения психофизической избыточности в алгоритме JPEG. В результате установлено, что с увеличением размера блока дискретно-косинусного преобразования (DCT) качество кодирования ухудшается. Установлено, что постоянное снижение величины коэффициента компрессии изображений соответствует обратно пропорциональному числу кодируемых коэффициентов DCT.

*Ключевые слова*: алгоритм JPEG, дискретно-косинусное преобразование, коэффициент компрессии, качество кодирования, психофизическая избыточность.

## Введение

Одним из наиболее часто применяемых преобразований двумерных изображений является DCT. Оно лежит в основе почти всех стандартов сжатия, которые используются в видеонаблюдении, за исключением Wavelet и JPEG-2000. Сокращение психофизической избыточности в алгоритме JPEG происходит в результате выполнения нескольких различных алгоритмов обработки данных. Этот метод сжатия применим для непрерывно-тоновых изображений. Таким образом, все стандарты JPEG, MPEG и семейство H.26x используют DCT в той или иной форме [1].

Уменьшить количество информации о каждом отдельном пикселе, определенным образом описывая контуры объекта и указывая средние значения яркости и цвета в пределах этого контура, можно путем сокращения избыточности. Крупные объекты соответствуют низким пространственным частотам, а мелкие объекты – высоким. На верхнем уровне эти частоты одновременно не присутствуют. В цифровом видеосигнале может быть передан весь спектр пространственных частот, однако если провести частотный анализ изображения, то возможно оставить в сигнале лишь те частоты, что действительно в нем присутствуют. Следовательно, в процессе сжатия изображений необходимо провести анализ пространственных частот.

Основным этапом процедуры сжатия цифровых изображений является преобразование небольших блоков изображения при помощи двумерного DCT. Обработка ведется блоками 8×8 пикселов. В результате выполнения DCT формируется 64 коэффициента. Исходный фрагмент изображения представляется в области пространственных частот. Этот шаг еще не приводит к сжатию изображения. Однако при его выполнении полагается, что в подавляющем большинстве изображений близкие по своим координатам пиксели имеют и близкие значения. Поэтому, при переходе от фрагмента к его частотному представлению большая часть энергии сигнала сосредотачивается в области низких частот, т.е. компоненты с меньшим значением индекса имеют большие значения [2].

При выполнении этой операции 64 исходных пикселей преобразуются в матрицу из 64 коэффициентов, которые характеризуют «энергию» исходных пикселей. Важнейшей особенностью этой матрицы коэффициентов является то, что первый коэффициент передает подавляющую часть «энергии», а количество «энергии», передаваемой остальными коэффициентами, очень быстро убывает. Таким образом, большая часть информации исходной

матрицы 8×8 пикселей представляется первым элементом матрицы, преобразованной по способу DCT.

## Методика исследования сокращения психофизической избыточности в алгоритме JPEG

Для исследования сокращения психофизической избыточности в алгоритме JPEG необходимо выполнить кодирование по отдельным блокам изображения с возможностью просмотра коэффициентов DCT, коэффициентов масштабирования, результатов применения DCT к изображению, в укрупненном виде одного блока изображения [3].

С учетом особенностей человеческого глаза, который практически не чувствителен к ошибкам передачи цветности, выполняем архивирование данных для $C_r$ и $C_b$ с большим сжатием по следующему алгоритму:

$$\begin{vmatrix} Y \\ C_r \\ C_b \end{vmatrix} = \begin{vmatrix} 0,299 & 0,587 & 0,144 \\ 0,5 & -0,4187 & -0,0813 \\ -0,1687 & -0,3313 & 0,5 \end{vmatrix} \times \begin{vmatrix} R \\ G \\ B \end{vmatrix} + \begin{vmatrix} 0 \\ 128 \\ 128 \end{vmatrix}. \quad (1)$$

Для $N$ равного восьми DCT, можно представить

$$D[i,j] = C(i) \times C(j) \times \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} S(x,y) \times \cos\left( \frac{(2 \times x + 1) \times j \times \pi}{2 \times N} \right) \times \cos\left( \frac{(2 \times y + 1) \times j \times \pi}{2 \times N} \right), \quad (2)$$

где $S(x,y)$ – исходное значение амплитуды пикселя с координатами $x$ и $y$ внутри блока; $D[i,j]$ – значение элемента $(i, j)$ матрицы коэффициентов преобразования $0 \le i, j \le N-1$, а значение $C(i)$ и $C(j)$ рассчитывается по формуле:

$$C(t) = \begin{cases} \frac{1}{\sqrt{N}}, & t = 0; \\ \sqrt{\frac{2}{N}}, & 1 \le t \le N-1. \end{cases}$$

Умножение $Y$, $C_r$ и $C_b$ на обратную матрицу есть обратное преобразование выполним по алгоритму:

$$Y_q = [u, v] = IntegerRaund \times \left( \frac{Y[u,v]}{q[u,v]} \right). \quad (3)$$

Исследования проводились для случая, когда пиксели цветовой компоненты разбиваются на матрицы по восемь на восемь пикселей. Для каждой компоненты формируется три рабочие матрицы DCT по восемь бит для каждой компоненты. Если $N$ равно восьми, то обратное DCT можно записать

$$S(x,y) = \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} C(i) \times C(j) \times D(i,j) \times \cos\left( \frac{(2 \times x + 1) \times j \times \pi}{2 \times N} \right) \times \cos\left( \frac{(2 \times y + 1) \times j \times \pi}{2 \times N} \right). \quad (4)$$

Применение алгоритма DCT к каждой рабочей матрице приводит к результирующей матрице, где коэффициенты в левом верхнем углу есть низкочастотная составляющая изображения, а в правом – высокочастотная.

Необходимо выполнить квантование как деление рабочей матрицы на матрицу квантования поэлементно. Формирование матрицы квантования происходит следующим образом: каждое из 64 компонент делится на число – коэффициент квантования [2].

**Разложение изображений по базисному алгоритму дискретно-косинусного преобразования**

Выполним разложение изображения по базисному алгоритму DCT в программе «VCDemo». Исходные изображения (рис. 1, *а* и 2, *а*) загружаются в формате .bmp в программу «VCDemo» (рис. 1, *б* и 2, *б*). На рис. 1, *в* и 2, *в* показан результат разложения выбранных изображений по базисному DCT размером восемь на восемь.

*а* *б* *в*

Рис. 1. Изображение «Подсолнух»: *а* – исходное; *б* – в программе «VCDemo» в формате .bmp; *в* – разложение изображения по базисному DCT 8×8

*а* *б* *в*

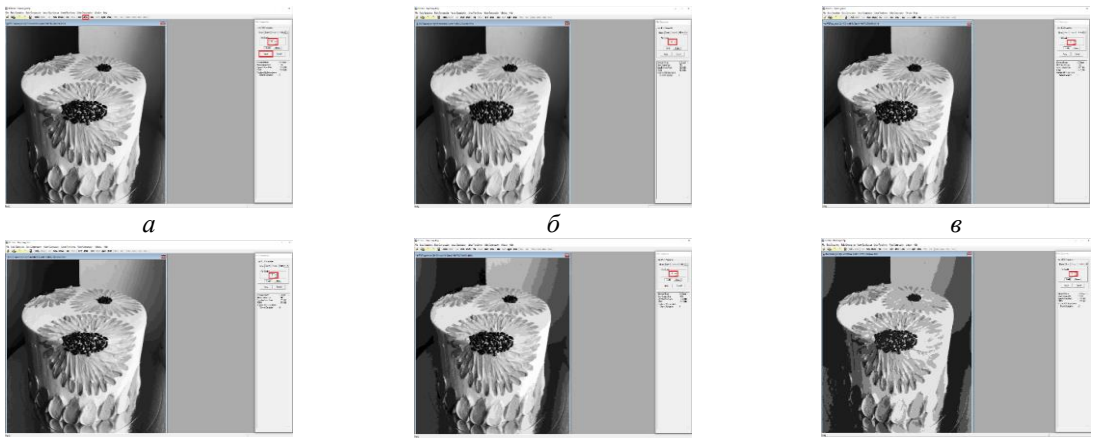
Рис. 2. Изображение «Шары»: *а* – исходное; *б* – в программе «VCDemo» в формате .bmp; *в* – разложение изображения по базисному DCT 8×8

Для того, чтобы оценить влияние параметров качества при сжатии изображений необходимо выполнить следующие шаги в программе «VCDemo».

Шаг 1. Включить на панели управления режим исследования JPEG.

Шаг 2. В подменю «Bitrate» выбрать параметр качества «Set Quality» и изменять его значение от 75 до 2, отмечая изменения качества обработки изображений.

На рис. 3 представлены результаты исследования влияния в контрольных точках, соответствующих значениям параметра качества 2, 4, 9, 16, 36, 75, как изменение параметра качества влияет на изображения «Подсолнух» и «Шары».



*а* *б* *в*

*г* *д* *е*

Рис. 3. Фрагмент рабочей области программы «VCDemo» при исследовании влияния параметра качества на сжатие изображения «Подсолнух»: *а* – равного 75; *б* – равного 36; *в* – равного 16; *г* – равного 9; *д* – равного 4; *е* – равного 2

*а* *б* *в*

*г* *д* *е*

Рис. 4. Фрагмент рабочей области программы «VCDemo» при исследовании влияния параметра качества на сжатие изображения «Шары»: *а* – равного 75; *б* – равного 36; *в* – равного 16; *г* – равного 9; *д* – равного 4; *е* – равного 2

В табл. 1 приведены значения соотношения сигнал-шум (SNR) и пикового соотношения сигнал-шум (PSNR) в зависимости от параметров качества для изображений «Подсолнух» и «Шары».

Табл. 1. **Значения SNR и PSNR в зависимости от параметров качества для изображений «Подсолнух» и «Шары»**

| Параметр качества | SNR, дБ | | PSNR, дБ | |
|---|---|---|---|---|
| | Изображение «Подсолнух» | Изображение «Шары» | Изображение «Подсолнух» | Изображение «Шары» |
| 75 | 39,7 | 43,3 | 50,5 | 52,0 |
| 36 | 30,0 | 33,6 | 40,8 | 42,2 |
| 16 | 25,7 | 29,0 | 36,5 | 37,6 |
| 9 | 22,5 | 26,0 | 33,3 | 34,6 |
| 4 | 17,4 | 20,6 | 28,2 | 29,3 |
| 2 | 13,0 | 15,2 | 23,8 | 23,9 |

Для установления характера зависимости изменения качества сжатых изображений «Подсолнух» и изображений «Шары» при наличии в канале связи ошибок, значение которых варьируется от 0,001 до 0,00005, нужно выполнить следующие шаги.

Шаг 1. На панели управления включить режим исследования JPEG.

Шаг 2. Выбрать в подменю «Errors», далее в графе «Set Channel Error Probability» указать количество ошибок от 0,001 до 0,00005.

При квантовании происходит существенная потеря информации об изображении. Задавая матрицу квантования с большими коэффициентами, мы можем получить большую степень сжатия. Квантованные коэффициенты DCT после округления преобразуем в линейный так, чтобы в начале вектора мы получали коэффициенты матрицы, соответствующие низким частотам, а в конце – высоким.

Далее показано какое влияние оказывают ошибки на изображения «Подсолнух» и «Шары» с различными значениями вероятности (рис. 5, 6).

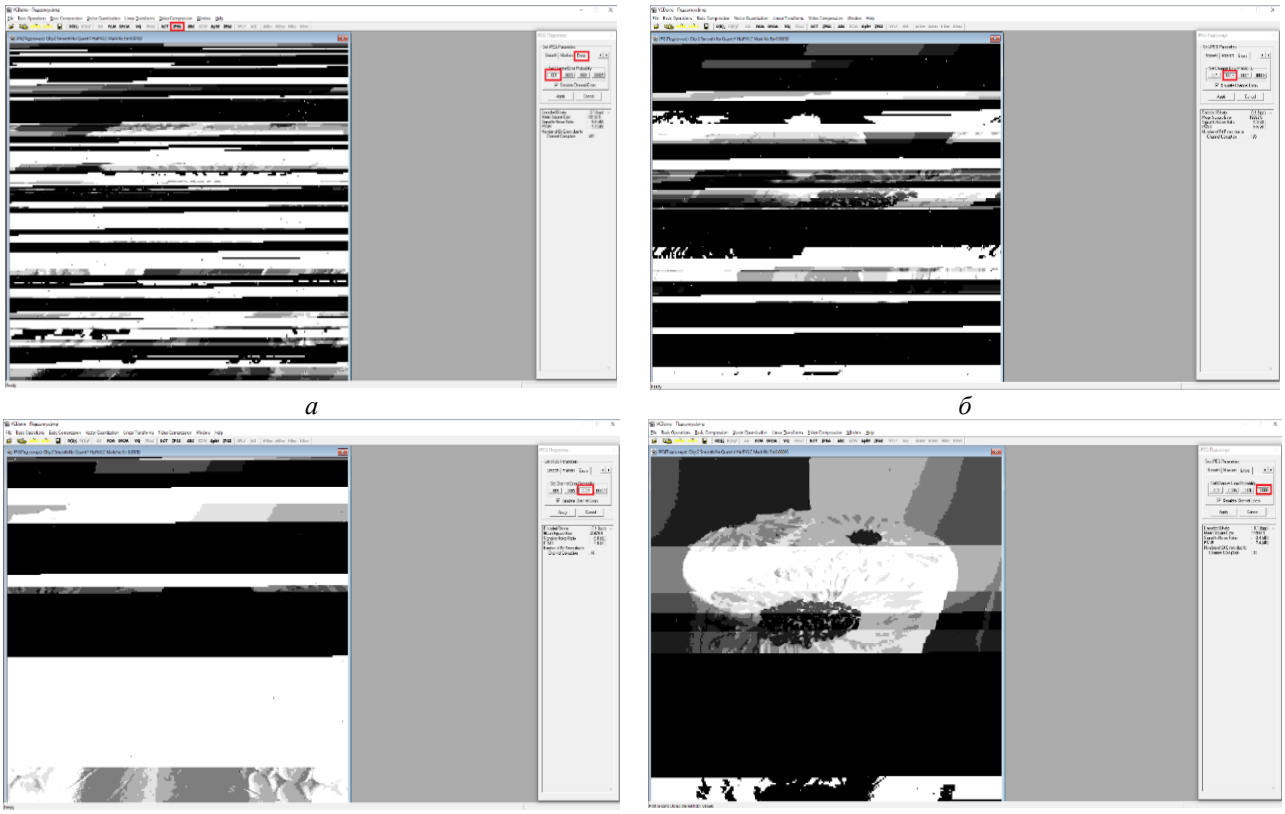
Для расчета коэффициентов DCT и оценки влияния параметров преобразования на качество сжатых изображений необходимо выполнить следующие шаги.

Шаг 1. Открыть изображение bmp-формата.

Шаг 2. На панели управления включить режим исследования DCT.

Шаг 3. В подменю выбрать размер блока DCT.

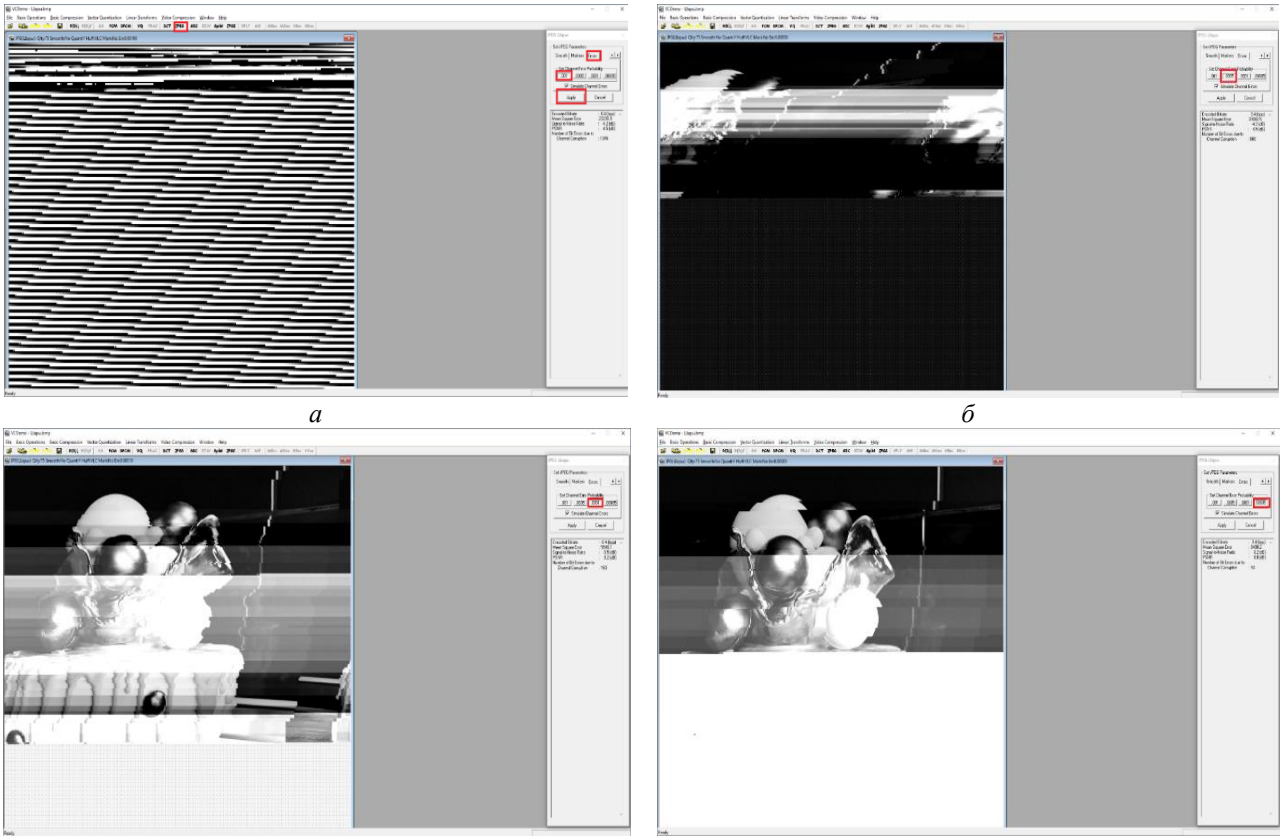
Результаты измерений субъективного качества, SNR и PSNR преобразованных изображений представлены в табл. 2 [5].



*а* *б*

*в* *г*

Рис. 5. Влияние ошибок на преобразованное изображение «Подсолнух «
со значением вероятности равной: *а* – 0,001; *б* – 0,0005; *в* – 0,0001; *г* – 0,00005



*а* *б*

*в* *г*

Рис. 6. Влияние ошибок на преобразованное изображение «Шары»
со значением вероятности равной: *а* – 0,001; *б* – 0,0005; *в* – 0,0001; *г* – 0,00005

Табл. 2. **Результаты измерений субъективного качества, PSNR и SNR**

| Размер блока | Число бит/отсчет | Субъективное качество изображения по 5-бальной шкале | | PSNR, дБ | | SNR, дБ | |
|---|---|---|---|---|---|---|---|
| | | «Подсолнух» | «Шары» | «Подсолнух» | «Шары» | «Подсолнух» | «Шары» |
| 2×2 | 0,25 | 2 | 2 | 25,9 | 26,1 | 13,5 | 13,5 |
| | 0,5 | 3 | 3 | 29,1 | 29,3 | 16,6 | 16,8 |
| | 0,75 | 4 | 3 | 32,5 | 32 | 20 | 19,4 |
| | 1 | 4 | 4 | 32,5 | 32 | 20 | 19,4 |
| | 2 | 5 | 4 | 36,5 | 35,4 | 24,1 | 22,9 |
| 4×4 | 0,25 | 2 | 2 | 28,8 | 27,6 | 16,4 | 15 |
| | 0,5 | 3 | 2 | 31,3 | 30,8 | 18,8 | 18,3 |
| | 0,75 | 4 | 3 | 33,6 | 33 | 21,2 | 20,4 |
| | 1 | 4 | 4 | 34,7 | 34,2 | 22,3 | 21,7 |
| | 2 | 5 | 5 | 39,7 | 38,8 | 27,2 | 26,3 |
| 8×8 | 0,25 | 2 | 2 | 30,4 | 30,1 | 17,9 | 17,5 |
| | 0,5 | 3 | 3 | 33 | 32,9 | 20,6 | 20,3 |
| | 0,75 | 3 | 3 | 34,9 | 34,6 | 22,4 | 22.1 |
| | 1 | 4 | 4 | 36,4 | 36 | 23,9 | 23,5 |
| | 2 | 5 | 4 | 41,2 | 40,5 | 28,7 | 28 |
| 16×16 | 0,25 | 2 | 2 | 31 | 31,2 | 18,5 | 18,6 |
| | 0,5 | 3 | 3 | 33,7 | 33,7 | 21,3 | 21,2 |
| | 0,75 | 3 | 3 | 35,6 | 35,4 | 23,2 | 22,9 |
| | 1 | 4 | 4 | 37,1 | 36,7 | 24,6 | 24,2 |
| | 2 | 5 | 4 | 41,4 | 40,7 | 28,9 | 28,1 |

Как видно из табл. 2, для одинаковых значений числа бит/отсчет, значения PSNR и SNR увеличивается при увеличении размера блока. Следует отметить, что «хороший» PSNR не всегда гарантирует хорошее качество изображения, из-за того, что зрительная система человека обладает нелинейным поведением.

Оценка качества производилась согласно [6]. В табл. 3 приведено соответствие количественной (балльной) и качественной оценок.

Табл. 3. **Оценка качества изображения**

| Оценка (балл) | Качество | Ухудшение |
|---|---|---|
| 5 | Отличное | Незаметное |
| 4 | Хорошее | Заметное, но не мешающее |
| 3 | Удовлетворительное | Слегка мешающее |
| 2 | Плохое | Мешающее |
| 1 | Очень плохое | Очень мешающее |

## Заключение

При исследовании сжатия изображений «Подсолнух» и «Шары», на основе разработанного алгоритма, было оценено влияние их параметров на качество преобразованных изображений. Параметр PSNR показывает расхождение между оригинальным и восстановленным после кодирования изображений. Чем выше PSNR, тем лучше качество изображения. Обычное значения PSNR для сжатия с потерями составляет от 30 до 50 дБ. Для исследуемых изображений «Подсолнух» и «Шары» PSNR составляет в зависимости от параметра качества от 50,5 до 23,8 дБ и от 52 до 23,9 дБ. Это означает, что качество изображений при обработке изменялось почти равномерно.

В программе «VCDemo» выполнено разложение изображений по базисному алгоритму DCT. Проведено исследование влияния параметра качества на изображение.

# INVESTIGATION OF REDUCTION OF PSYCHOPHYSICAL EXCESSIVENESS IN JPEG ALGORITHM

D.P. GORBUKOVA, Yu.M. BAKIMOV, T.M. PECHAN

**Abstract.** A study of the reduction of psychophysical redundancy in the JPEG algorithm was carried out. It is shown that with an increase in the size of a discrete-cosine transform (DCT) block, the coding quality deteriorates. It was found that a constant decrease in the value of the compression ratio of images corresponds to inversely proportional to the number of encoded DCT coefficients.

*Keywords*: JPEG algorithm, discrete cosine transform, compression ratio, coding quality, psychophysical excessiveness.

## Список литературы

1. Tran H.T., Tran S.M. // Электроника и связь. 2010. № 2(55). С. 74–81.
2. Дружинин Д.В. // Вычислительные методы и программирование. 2008, Т.9. С. 72–80.
3. Chien S-Y., Huang Y-W. // IEEE Communications Magazine. 2005. P. 123–131.
4. August N.J., Ha D.S. // IEEE Transactions on Multimedia. 2004.Vol. 6, P. 414–422.
5. Heyne B., Götze J. // Adv. Radio Sci. 2007. Vol. 5, P. 305–311.
6. Поляков Д.Б. // Труды Московского технического университета связи и информатики. 2008. № 1. С. 463–466.

*UDC 339.138*

# DESIGN OF SCHOOL BELL AUTOMATIC CONTROL SYSTEM BASED ON SINGLE-CHIP MICROCOMPUTER

YU CHUYUE, XIA YIWEI, DU ZONGQI, LIU ZHENGHUA

*Belarusian State University of Informatics and Radioelectronics, Republic of Belarus*

*Submitted 22 November 2021*

**Abstract.** This article introduces the basic components of the school's automatic control system, and makes a detailed introduction and comparison of the functions, application scenarios, and advantages of each part. The hardware design of the automatic control system is based on the STC89C52 single-chip control circuit as the core, supplemented by sensor circuits, clock circuits, bell circuits and human-computer interaction circuits to complete various functions. The human-computer interaction circuits include keyboard input circuits and liquid crystal display circuits. The software design of this system mainly includes sensor detection, button setting, and bell output part. The sensor detection part is composed of a temperature detection subprogram, the key setting part is composed of an independent key subprogram and a liquid crystal display subprogram, and the bell output part is composed of a voice recording and playback subprogram. The program and clock subroutine constitute.

*Keywords*: STC89C52 single chip microcomputer, sensor, electric bell automatic.

## Introduction

Before the 21st century, the maintenance of school discipline was ensured by manual ringing by manpower or the teacher’s dismissal of the get out of class. However, it was inefficient and poor. Students’ learning effects are weakened and their enthusiasm for class is not high. In order to further guarantee and improve the teacher’s teaching effect, it can be used for more complex control applications [1].

In recent years, intelligence has become more and more popular, because manual represents unstable production capacity and difficulty in unified management of quality control. Behind the popularization of intelligent speed of light in daily life is the innovation and progress of single-chip microcomputers. It has the characteristics of high cost performance, small size, high reliability, and strong control power, which are widely used in various fields of automatic control [2]. Nowadays, the campus bell system has become the standard configuration of major colleges and universities, and it has very broad development prospects and room for improvement. At the same time, compared with the high labor costs, the advantages of low electricity cost and precise bell ringing efficiency also promote The reason why the ringing system is adopted efficiently.

This subject is an efficient bell system based on STC89C52 single-chip microcomputer, supplemented by temperature sensors, liquid crystal display, clock and other modules. It is suitable for various working environments and supports users' operations such as time adjustment, time adjustment, and bell time adjustment. It can be realized Real-time display of temperature and clock, operation of the bell system.

## Overview of development at home and abroad

Through reviewing and summarizing the literature of relevant scholars at home and abroad in recent years, it is found that the ringing system is currently mainly optimized in three areas with a high degree of optimization and more optimization schemes: improving the accuracy of the system ringing, and optimizing the human nature of the ringing system Degree of integration and improve the flexibility of the system.

In the direction of improving the accuracy of the system's ringing, scholars advocate the use of external storage chips [3], broadcast [4], GPS [5] to improve the ability to self-calibrate the bell for a long time. Up to now, the bell system is extremely large. Part of the time calibration is still done by manpower. First, if the self-calibration ability of the electric bell system is increased, the cost of the electric bell system will increase. The second is that the mature electric bell system on the market has a certain self-calibration ability and temperature resistance. Humidity guarantees that in a short period of time, the accuracy of the electric bell system will not drop a lot, so the high-efficiency tends to manually adjust the time of the electric bell system. In the direction of optimizing the degree of humanization of the bell system, scholars advocate that the traditional electric bells that are widely used at present have large noise and harsh sound, which does not meet the requirements of people pursuing «green environmental protection» living environment. Soft, humanistic and pleasant music ringtones can be used [6], MP3 output [7], beating the bell [8] and other methods instead, aiming to create a better learning atmosphere and campus culture. In the direction of improving the flexibility of the system, scholars have proposed that the bell system is widely wired on each floor of the teaching building, and the wiring is messy, making it inconvenient to move and causing a lot of waste of raw materials. The control of the electric bell system can make the electric bell system no longer need to be an exception for special wiring, saving costs and improving the overall aesthetics of the campus. At the same time, there is still a lot of room for optimization of the system, using a high-precision clock chip or a special computer ringing system are both methods.

## The overall hardware design of the school bell automatic control system

The hardware part of the school bell automatic control system is based on the smallest system of STC89C52, which is composed of expanded voice recording and playback, liquid crystal display, human-computer interaction, real-time clock, and temperature sensor modules to coordinate work. The hardware block diagram is shown in Fig. 1 below.

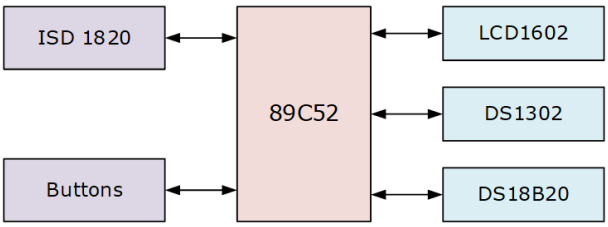



Fig. 1. Hardware block diagram of automatic control ringing system

The power supply of the system adopts 5V, which effectively guarantees the stable and normal operation of each module of the system. The main controller of the automatic control ringing system is the STC89C52 single-chip microcomputer. This single-chip microcomputer takes advantage of its own classic design and has a variety of ports. After proper programming, various modules can work together and achieve multiple functions. This design will pass The algorithm makes the control program concise; moreover, it seeks convenience and efficiency in defining the serial port, so that the legibility of the code drives the modification of the code accurately and concisely. The human-computer interaction module is convenient for users to complete computer-related operations and get the next operation instructions from the computer's feedback. The display module selects the lcd1602 liquid crystal demonstration screen, which completes the real-time display of temperature, the display of time, the instructions to the user's operation and the feedback of the current state of the computer. The electric bell circuit completes the realization of the upper and lower get out of class bells, and selects the voice recording and playback ISD1820 module, which supports high-quality and natural restoration of the voice, which is triggered by the rising edge. The temperature sensor completes the real-time monitoring of the temperature and transmits the data to the single-chip microcomputer. The EEPROM storage circuit enables the system to store clock information related to the accuracy of the bell in a timely manner even if the system is subjected to unexpected situations such as power outages. The switch module makes the system more environmentally friendly and economical. When not in use, it is turned off and enters the dormant state, and the battery can be updated and charged during this period; when it is turned on and enters the running state, it can work better due to the update of the dormant state.

This automatic ringing system has three working modes, detection mode, setting mode, and ringing mode, corresponding to three operation pages. In detection mode, use DS1302 module and DS18B20 temperature sensor and display data. In setting mode, press independent button 1 or independent button 4 to enter the operation page, press independent button 1 to increase or decrease the clock data, press Independent button 4 can read the ringing time for setting and modification. Ringing mode When the set clock data is the same as the clock read data, it will trigger the ISD1820 to work and produce a slow and pleasant music sound to remind teachers and students to go to and from get out of class.

### The overall design of the school electric bell automatic control system software

The program design adopts a modular design idea. Each chip driver function is written into different header files, and then these header files are referenced and called in the main function. This can reduce the complexity of the program and facilitate the modification of the program.

Program programming uses Keil5 development software and uses C language to write program statements. Compared with assembly language, C language is more readable and transplantable.

The program executes the main function in an endless loop during the running process, and the keyboard scan function is called once in each loop to detect whether a key is pressed and whether the pressed key is a set key. If a key is pressed and the key is a setting key, the corresponding program is executed in the corresponding sentence; if no key is pressed, LCD1602 displays clock and temperature information.

## Conclusion

The school bell automatic control system is designed to work together by multiple modules, coordinated and commanded by the STC89C52 single-chip microcomputer, through the single-chip microcomputer programming to enable the system to run in the direction you want, achieve, complete and improve the design functions of the system, forming a good closed-loop system , Human-computer interaction is carried out only by pressing the keys to guide and complete the operations performed by the users on the system. This design integrates the most mature modules at the moment, and the finished product has high efficiency and stability, and has good anti-interference ability. The related technologies include control theory, liquid crystal display, temperature sensing, etc.

## References

1. Yongxian Song [et al.] // Journal of Computers. 2011. Vol. 6. P. 718–724.
2. Wu Gang // Electronic Component & Device Applications. 2008. Vol. 10 (12). P. 23–24.
3. Yang Fan // Computer Knowledge and Technology. 2013. Vol. 32. P. 7236–723.
4. Lai Yihan [et al.] // Journal of Longyan University. 2017.
5. Bai Xinran // Electroacoustic Technology. 2016. Vol. 11.
6. Li Cailong [et al.] // Digital Technology and Application. 2016. Vol. 08.
7. Tang Yu, Sun Hui // Mathematical Techniques and Applications. 2016. Vol. 09.
8. Ramesh Harajibhai Chaudhari [et al.] // International Journal of Current Microbiology and Applied Sciences. 2019. Vol. 8, № 4. P. 1326–1333.

*UDC 339.138*

# DESIGN OF SMART CODE LOCK

YU CHUYUE, XIA YIWEI, ZHAO DI, HU ZHIFENG

*Belarusian State University of informatics and Radioelectronics, Republic of Belarus*

*Submitted 22 November 2021*

**Abstract.** This design uses MCS-51 single-chip microcomputer and the corresponding interface chip to complete the design of a smart password lock. The matrix key input module is used as the input channel for passwords and related information, and the display screen LCD1602 is used to display the prompt words through a stepping motor. The rotation of the door lock can be opened and closed, and the buzzer and LED are used to realize the sound and light alarm when the password is wrong. In addition, the uniqueness of this design is that the proximity switch is used to detect whether the door is closed or not, which is more intelligent.

*Keywords*: Password lock, Stepper motor, Human machine interface, Proximity switch.

## Introduction

The development of electronic technology, especially with the emergence of large-scale integrated circuits, has brought fundamental changes to people's lives. In modern society, with the general improvement of people's security awareness, code locks are not only used in daily life, but their functions are also reflected in all aspects [1]. And this design uses MCS-51 series single-chip microcomputer as the control core to realize the design function of smart code lock.

The main function of this product is to ensure the safety of the door. After the main program is used to execute the initialization, the while statement is entered. When no key is pressed or the key is a non-function key, 1602 displays a statement to prompt the user to select a function, and when there is a function key After pressing the programming idea of selectively entering the subroutine, the following operations are realized: manually set the password, manually modify the password, automatically open the door after verifying the password, realize the waiting at a fixed time and intelligently identify whether the door is closed, if it is not closed, it will be realized Automatically alarm and automatically stop and wait. It has certain reference significance for the further design of various types of smart locks.

## System composition

The intelligent password lock system consists of a single-chip microcomputer system module, a keyboard input module, a display module, an alarm module, an EEPROM storage module, and an unlocking module. The display module is LCD Lcd1602, which is used to display various prompts and step instructions. The keyboard input module is used to operate the display content of the LCD. Different keys have corresponding functions, which can realize the functions of setting passwords, changing passwords, confirming current operations, deleting specific characters and verifying passwords [2]. The stepper motor is mainly operated after verifying the correct password. Its main function is to control the opening and closing of the door lock, which are respectively forward 360° unlocking and reverse 360° unlocking. The function of the proximity switch LP-18Y8C is to be able to judge whether the door is closed normally. The system structure diagram is shown in Fig. 1.

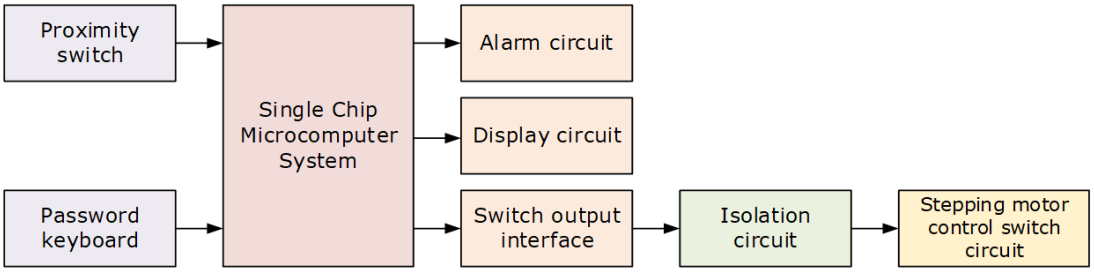



Fig. 1. System structure block diagram

## The working principle of the system hardware module

The smart password lock is mainly connected with the AT89C52 chip and the liquid crystal display, and is connected with the 4×4 matrix keyboard. The matrix keyboard has the function of selection. The optional functions include but not limited to setting passwords, changing passwords, typing and verifying passwords. AT24C02 chip is the core component of the data storage part.

When the password verification is successful, the single-chip microcomputer outputs the high and low levels of the specific step sequence to the output interface part through the P port [3]. UIN2003 and its peripheral circuits act as isolation and amplifying current, and the stepping motor is controlled by the P port output voltage to achieve unlocking function. The matrix keyboard part is equipped with 15 keys including number keys and function keys to control the display content, namely: number keys 0–9, set password, delete, confirm, modify password, and enter password. The data access part stores the unlock password when setting the password on the keyboard, and calls the password when the password is entered to verify the entered password to confirm whether to unlock. The 24C02 chip is an EEPROM device with IIC interface. The so-called EEPROM is electrically erasable programmable read-only memory, which is a type of ROM. It is a read-only memory, that is, it can continue to store the program when power is off, and at the same time it can be erased and rewritten under the action of higher than normal voltage, which greatly facilitates the development of the single-chip microcomputer, and realizes the power-down storage function and update password settings.

## The working principle of the system software module

The software part is mainly composed of the following modules: keyboard scanning module, liquid crystal display module, storage module, stepper motor rotation module, timing interrupt module, alarm module, proximity switch module.

In the main program, the program cyclically executes the judgment keyboard scan. If no key is pressed or the pressed key is a non-function key, the LCD will continue to display «select function:». If it is detected that a key is pressed, the corresponding subroutine is executed. After the subroutine is exited, the main program continues to be executed: the keyboard scanning program detects which key is pressed, and then enters the corresponding judgment statement to execute according to the demand, it can Set the password, you can also change the password, and update the changed password to the IIC; the external interrupt service program is used for the timing opening after unlocking [4]. After the unlocking is successful, a part of the time is reserved for the unlocker to enter, and then timing, timing ends, the door Close again. The alarm module is used to control the sound and light alarm when the password is detected incorrectly. The proximity switch module is used to judge whether the door is closed or not. Because the proximity switch is an NPN Hall element, it only corresponds to two different states when a fixed object is detected, so only the single-chip microcomputer needs to read the pin state of the pin. However, if the pin status is high, it means that the door is not detected and an alarm is issued. If the pin status is low, it means the door has been detected. The single-chip microcomputer controls the stepper motor to turn the lock cylinder back to achieve intelligent lock closure [5].

## Conclusion

In this work, the development of an electronic combination lock, designed to be installed on the outer door of a residential building, was carried out. A feature of this lock is the presence of an audible alarm that notifies the owner of an attempt to select a code.

In the course of the work, the analysis of the task was carried out, on the basis of which the requirements for the final system were formulated. Based on the requirements, a structural diagram was built. Based on the structural diagram, appropriate devices were selected to implement the functions assigned to the system elements. Further, using the selected devices, a functional diagram was built. The development was completed by drawing up a block diagram of the algorithm and writing the source code of the program for the microcontroller.

Thus, during the implementation of this project, a digital password locking control system was developed with a single-chip microcomputer as the core and password input through the panel keyboard. This system includes a single-chip microcomputer system module, keyboard input module, display module, alarm module, and so on.

## References

1. Zhang Yigang. Newly edited MCS-51 Application Design. Harbin: Harbin Institute of Technology Press, 2003.
2. Lu Xiaoxuan // Journal of Qingdao University of Science and Technology. 2006. P. 268–271.
3. Li Xin // Microcomputer Information. 2006. P. 32–37.
4. Yang Meixian // Scientific Information. 2007. P. 35–39.
5. Zhang Youde, Zhao Zhiying, Tu Shiliang. Principle, Application and Experimental Design of Single Chip Microcomputer. Shanghai: Fudan University Press, 2008.

*UDC C 620.9:.658.30*

# MODEL, STRUCTURE AND ALGORITHM OF THE INTERNET OF THINGS FOR THE MANAGEMENT OF PRODUCTION QUALITY CONTROL

U.A. VISHNYAKOU, HU ZHIFENG

*Belarusian State University of Informatics and Radioelectronics, Republic of Belarus*

*Submitted 23 November 2021*

**Abstract.** The multi-agent model for the dairy farm is constructed, described the four-layer Internet of Things (IoT) structure, algorithm on the dairy farm control is work out. Proposed the use of digital software and federated learning to solve the problem of the lack of effective data on the dairy farm and the security of data sharing.

*Keywords*: IoT networks, model, structure, algorithm.

## Introduction

Actually, for diary form management, there are mainly two types of management involved. The first one is production management. Another is process management. In production management, milking management is the most important, this part involves the management of processing equipment, milking preservation and automatic milking, and in milk preservation, it involves the management of smart sterilization and milk cooling. In the process of management of the dairy farm, in mainly involves intelligent monitoring, dairy cow observation, feeding and reproductive management. Intelligent monitor is mainly aimed at location analysis of dairy cows' position status. The observation of the cow mainly includes the observation of the of the cow observation of the activity, behavior and physical health of the dairy cow. The feeding and reproductive management mainly involve the nutritional management and physical state management. For this two types management of dairy farm, obviously, the IoT can be an effective tool that can be applied to the management.

For this two types management of dairy farm, obviously, the IoT can be an effective tool that can be applied to the management. Some researchers have already implied IoT into this field [1–3]. Therefore, effective use of the Internet of Things technology will improve the management efficiency of the dairy farm, thereby increasing the economic efficiency and productivity of the dairy farm.

## IoT Model for Dairy Farm Management

According to different types of dairy farms (different size, different numbers of cows, or different regions, urban or rural), the IoT can play a different role and solve different problems. Therefore, how to effectively use IoT technology in dairy farms is one of the current researcher issues. The first thing need to be known is the communication standards in IoT networks. At a short distance, IoT networks use such communication standards as Bluetooth, ZigBee, and less popular protocols: Thread, WirelessHART, MiWi, SNAP, and others [4]. All these communication standards use non-licensing bands of the radio frequency spectrum from the so-called ISM band (Industrial, Science, Medical), allocated for the needs of industry, medical equipment and scientific equipment. In practice, this frequency range, taking into account the restrictions adopted for it, is also used for organizing communication channels within cells and clusters of IoT cellular networks. Wi-max and LTE protocols are used for long distance. Some communication protocols used in IoT networks can be seen at table 1.

Most standards for short-range wireless communication systems sometimes called personal area network (PAN). Typically, such networks have a coverage radius of 10 to 30 meters. This kind of network can be used to connects personal electronic device of one user (phones, computers, monitors,

laptops). Sometimes a short-range personal network can be optimized for certain applications called «application profiles». A Low-power Wide-area Network-energy-efficient long-range network (LPWAN) can be used for requiring long distances from monitoring objects to processing services [5]. Therefore, this kind of IoT network can be applied in a large size dairy farm to transfer the data of cows. This network uses radio frequencies in the non-licensing range (30–300 MHz), (300 MHz–3 GHz) and 800–930 MHz.

Table 1. **Communication protocols used in IoT networks**

| Name of protocols | Transmission rate | Frequency band | Communication range |
|---|---|---|---|
| RFID | 424 Kb/s | 135 KHz | >50 cm |
| | | 13,56 MHz | >50 cm |
| | | 866–960 MHz | >3 m |
| | | 2,4 GHz | >1,5 m |
| NFC | 424 Kb/s | 2,45 GHz | <2 m |
| ZigBee | 20/10 Kb/s–10 Mb 256 Kb/s | 900 MHz/ 2,4 GHz | 10 m |
| Bluetooth | 1 Mb/s | 2,4 GHz | 10 m |
| BLE | 10 Mb/s | 2,4 GHz | >10 m |
| UWB | 50 Mb/s | broadband | 30 m |
| Wi-Fi (IEEE 802/11ac) | <6,77 Gb/s | 2,4/5 GHz | 100 m |
| Mobile networks 3G/4G (LTE) | <150 Mb/s | 800/900/1800/2400 MHz | >10 km |

A multi-agent approach can be created to create a model of IoT network for monitoring production quality for dairy farm management [6]. In this multi-agent structure, we will distinguish a set of agents for production quality sensors, agents for converters, agents for storing quality production indicators, agents for processing production quality indicators to obtain conclusions, agents for monitoring these indicators and conclusions. This multi-agent model is represented by the set:

$$\text{IoTccm} = \{\text{RAM, Ac, Amq, Apmq, Admq, Aimq, MAi}\},$$

where IoTccm – the IoT network model, RAM – a set of sensor agents (from portable analyzers of milk quality, and dairy cow health monitoring), Ac – the set of agent converters, (gateways), Amq – agents' storage of quality indicators, Apmq – agents of their processing, Admq – agents to make decisions about the quality of production, Aimq – agents interface to display indicators, MAi – monitoring agents (mobile devices to monitor production quality indices and the dairy cow). This multi-agent model can realize the information flow needed in the production management and process management of the dairy farm. Therefore, the management of dairy farms will more effective.

## The structure of IoT for dairy farm management

For a comprehensive describe IoT that its architecture includes perception layer, network layer, middleware layer, application layer and business layer. But as conceptually, the IoT can belongs to the next generation of networks (NGN), so its structure is similar to the four layer of NGN, which includes smart sensors, transport environment, services and application [7].

The lowest level of the IoT structure consists of the smart objects integrated with sensors. The sensors can be used to digitize various indicators of the dairy farm, such as the location, physical condition and nutritional indicators of the dairy cow, as well as the weather, temperature, humidity of the dairy farm. The sensors digitize the physical information of the dairy farm.

The larger amount of data (temperature, location, caw's body temperature, milk quality's indicator) collected by sensors, and these data should rely on reliable and high-performance wired and wireless network infrastructure for transmission. A network layer can be constructed.

The service layer usually contains a set of information services: for example, some automate technological and business operations may will be used in IoT, supporting for operational and business activities (OSS/BSS-Operation Support System/Business Support System), some information processing method (statistical, data preprocessing, feature extraction and predictive analytics, etc.), data storage, information security, the business rule of cow dairy farm management, the business process of cow dairy farm management.

At the fourth layer named application layer, there are different types of applications in different industry, and even in an IoT system about dairy farm, for different subsystems, there are different types of application for cow dairy farm sectors.

Based on the above description, the structure of the IoT for dairy farm management can be seen in the Fig. 1.

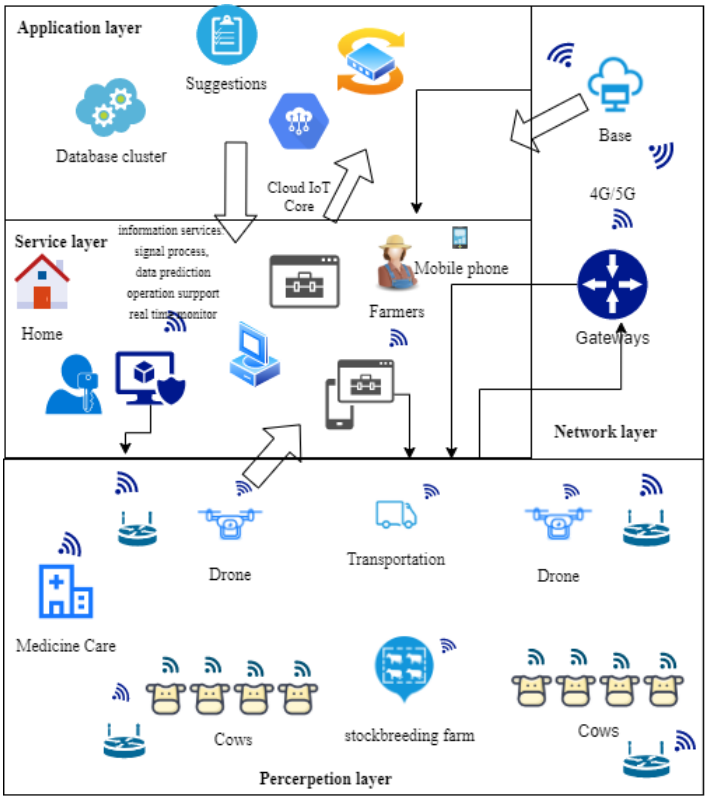



Fig. 1. The structure of the IoT for dairy farm management

## Algorithms of the IoT for managing a dairy farm

It is worth noting that machine leaning (ML) algorithm usually depends on large, high-quality datasets, the data availability is poor, for reasons such as commercial competition or confidential information, some dairy farmers are generally unwilling to share relevant data, it is hard to integrate with the data sources for the ML algorithm. Digital twin (DT) [8] may a good idea to solve this problem. DT is a reliable strategy to migrate knowledge from the virtual space to physical space. This kind of DT algorithm have already implemented in crop farms [9]. A literature review of digital twin in smart farming had discussed in [10], this reference presented DT have massive scope for success in the field of sustainable agriculture, but the number of works in this field is relatively less than other domains like Manufacturing, Healthcare, Autonomous Vehicles, and Aviation, and explored the possibilities in Hydroponics.

Therefore, in response to the lack of valid data in the dairy farms, DT will be an effective technology to deal with this kind of problem.

Moreover, in response to the lack of security and privacy constraints on dairy farm data, Federated Learning (FL) [10] can be applied to dairy farm data management due to its advantages in ensuring information security during big data exchange and protection the privacy of terminal data and personal data. In work [11] discussed alternative solutions to the problem based on privacy-preserving collaborative learning, and provide a set of scenarios to show their benefits for both farmers and businesses. Therefore, FL is a suitable algorithm to tackle the lack of security and privacy constraints on dairy farm data.

Moreover, specific management issues for dairy farms, such as milk quality control, there are some indicators (lactose, fat, Chlorides, Protein) need to be detected. Table 2 is intended to describe the values of milk quality indicators for normal and mastitis.

Table 2. **The values of milk quality indicators for normal and mastitis**

| Indicators | Normal milk | Mastitis milk |
|---|---|---|
| Lactose, % | 4,7 | 3,9–4,5 |
| Fat, % | 3,8 | 2,2 (1,5–3,5) |
| Chlorides, % | 0,091–0,1 | 0,147–0,15 |
| Protein, % | 3,3 | <6,1 |

The milk quality control generalized algorithm consists of the following steps:

1. The portable analyzers for milk quality of the dairy farm are applied as sensors to collect the indicators of milk, these indicators of the milk will be transformed into sensor data.

2. Before the sensor data sent to IoT network, the device of portable analyzers need to be verified by the IoT platform (the service authorization). If the verification is not successful, then the verification request will be sent manager until the devices IDs corrected.

3. Data analyzers output the results to a gateways-converters, (instead of a computer or printer via a serial port in previous). The gateways-converters can convert and transmit the captured milk quality indicators to the cloud platform (CP). In this process, various network protocols are applied.

4. In the CP the database usually stores kinds of indicator data that received from different dairy. The database stores data received from dairy farms, taken quality characteristics by time (number, time of day, checked parameters and etc.), from different dairy farms. The knowledge base contains rules for evaluating the quality of milk.

5. Data are sent to the solver, which based on the accepted indicators and rules for processing quality indicators from the knowledge base, issues solutions for certain quality parameters. These decisions are also recorded in the database.

6. According to the different types of received data, rule handler perform action: classification data, save data into database, send data to Analytics system, send preprocessing commands and so on.

7. Mobile devices be installed an application that allows the farmer or the user to check the information that they interested from the cloud database through the site.

8. The site serves as a means of displaying obtained results on the quality of milk for manager.

## Conclusion

A multi-agent model is presented for monitoring production quality for dairy farm management. Based on the multi-agent model, the four layers' structure of the Internet of Things for dairy farm management is proposed.

In response to the lack of high-quality and reliable data resources on dairy farm, a DT algorithm is proposed to applied to tackle this problem. To tackle the lack of security and privacy constraints on dairy farm data, FL as a suitable method is proposed. Moreover, for specific management issues for dairy farms, such as milk quality control, the milk quality control generalized algorithm is proposed.

## Reference


1. Vate-U-Lan P. [et al.] // Smart dairy farming through the Internet of Things (IoT). 2016. P. 23–36.
2. Treiber M, Höhendinger M. // Connectivity for IoT Solutions in Integrated Dairy Farming in Germany. 2019.
3. Muhammad O. [et al.] // IoT for Development of Smart Dairy Farming. Journal of Food Qualit, 2020.
4. Rentyuk V. // Brief guide to wireless technologies of the Internet of things. Part 2. Short range. 2018. Vol. 1. P. 51–57.
5. Rentyuk V. // Brief guide to wireless technologies of the Internet of things. Part 4. Long range. 2018. Vol. 3. P. 82–87.
6. Shoham Y, Leyton-Brown K. Multiagent systems: algorithmic, game-theoretic, and logical foundations. Cambridge University Press, 2008.
7. Visniakou U.A. [et al.] // Siberian Journal of Science and Technology. 2020. № 4. P. 478–482.
8. Xu Y. [et al.] // A digital-twin-assisted fault diagnosis using deep transfer learning. 2019. Vol. 7. P. 1990–1999.
9. Van Evert. F. [et al.] // A digital twin for arable and dairy farming. 2021. P. 364–377.
10. Gengler N. // Symposium review: Challenges and opportunities for evaluating and using the genetic potential of dairy cattle in the new era of sensor data from automation. 2019. Vol. 102. P. 5756–5763.
11. Papst F. [et al.] // Proceedings of the 9-th International Conference on the Internet of Things. 2019. P. 1–4.

## СВЕДЕНИЯ ОБ АВТОРАХ


| | | |
|---|---|---|
| 1. | Аксенов Вячеслав Анатольевич | – старший преподаватель кафедры инфокоммуникационных технологий БГУИР |
| 2. | Бакимов Юрий Мухамеджанович | – студент кафедры инфокоммуникационных технологий БГУИР |
| 3. | Белоконь Евгений Олегович | – магистрант кафедры инфокоммуникационных технологий БГУИР |
| 4. | Вишняков Владимир Анатольевич | – д.т.н., профессор кафедры инфокоммуникационных технологий БГУИР |
| 5. | Врублевский Сергей Сергеевич | – адъюнкт кафедры связи Военной академии Республики Беларусь |
| 6. | Горбукова Динара Павловна | – студентка кафедры инфокоммуникационных технологий БГУИР |
| 7. | Ду Цзунци | – магистрант кафедры инфокоммуникационных технологий БГУИР |
| 8. | Липкович Эдуард Борисович | – доцент кафедры инфокоммуникационных технологий БГУИР |
| 9. | Лю Чжэнхуа | – магистрант кафедры инфокоммуникационных технологий БГУИР |
| 10. | Машкин Евгений Вячеславович | – к.т.н., заместитель директора по развитию – первый заместитель директора ОАО «АГАТ-СИСТЕМ» |
| 11. | Митюхин Анатолий Иванович | – доцент кафедры инфокоммуникационных технологий БГУИР |
| 12. | Нгуен Ань Туан | – аспирант кафедры инфокоммуникационных технологий БГУИР |
| 13. | Панькова Вероника Витальевна | – старший преподаватель кафедры инфокоммуникационных радиотехнологий БГУИР |
| 14. | Петров Сергей Николаевич | – к.т.н., доцент кафедры защиты информации БГУИР |

| | | |
|---|---|---|
| 15. | Печень Татьяна Михайловна | – старший преподаватель кафедры инфокоммуникационных технологий БГУИР |
| 16. | Рудиков Станислав Игоревич | – магистр технических наук, заместитель директора по информационным технологиям Унитарного предприятия «НТЦ «ЛЭМТ» БелОМО» |
| 17. | Саломатин Сергей Борисович | – к.т.н., доцент кафедры инфокоммуникационных технологий БГУИР |
| 18. | Смоляк Сергей Владимирович | – руководитель группы оптимизации радио и опорной сети УП «А1» |
| 19. | Ся Ивэй | – магистрант кафедры инфокоммуникационных технологий БГУИР |
| 20. | Ху Чжифэн | – магистрант кафедры инфокоммуникационных технологий БГУИР |
| 21. | Цветков Виктор Юрьевич | – д.т.н., заведующий кафедрой инфокоммуникационных технологий БГУИР |
| 22. | Чжао Ди | – магистрант кафедры инфокоммуникационных технологий БГУИР |
| 23. | Шайа Бахаа Хикмат | – аспирант кафедры инфокоммуникационных технологий БГУИР |
| 24. | Шараев Никита Петрович | – системный инженер ИООО «ЭПАМ СИСТЕМЗ» |
| 25. | Шкадаревич Алексей Петрович | – д.ф-м.н., профессор, академик НАН РБ, директор Унитарного предприятия «НТЦ «ЛЭМТ» БелОМО» |
| 26. | Эль Масри Абдель Хуссейн Али | – аспирант кафедры инфокоммуникационных технологий БГУИР |
| 27. | Эль Хаджи Слейман Кхалед Кхалиль | – аспирант кафедры инфокоммуникационных технологий БГУИР |
| 28. | Юй Чуюэ | – магистрант кафедры инфокоммуникационных технологий БГУИР |