ISSN 1727-1239

INTERNATIONAL UNIVERSITY OF RADIO ELECTRONICS

ALMANAC OF MODERN SCIENCE AND APPLIED RESEARCH

APPLIED RADIO ELECTRONICS

Scientific and Technical Journal 2017 Volume 16 № 3, 4

CONTENTS

ЛОКАЦИЯ И НАВИГАЦИЯ

УДК 621.396.965:621.391.26

АДАПТИВНЫЕ СИСТЕМЫ ЗАЩИТЫ РЛС ОТ ШУМОВЫХ ПОМЕХ. 5. ОПЫТНЫЙ ОБРАЗЕЦ СИСТЕМЫ ПОМЕХОЗАЩИТЫ

Д. И. ЛЕХОВИЦКИЙ, В. П. РЯБУХА, А. В. СЕМЕНЯКА, Е. А. КАТЮШИН, В. Н. ГРИЦЕНКО

Пятая статья цикла статей по адаптивным системам защиты РЛС от маскирующих шумовых помех. Описывается опытный образец системы адаптивной цифровой пространственной обработки сигналов на фоне маскирующих шумовых помех на основе адаптивного решетчатого фильтра, выполненный на базе программируемой логической интегральной схемы, приводятся результаты предварительных испытаний.

Ключевые слова: опытный образец, шумовые помехи, программируемая логическая интегральная схема, испытания.

ВВЕДЕНИЕ

Данная статья – пятая в цикле статей по теории и технике адаптивной обработки сигналов на фоне шумовых помех (**ШП**).

В первой статье [1] проанализированы корреляционные автокомпенсаторы помех на основе градиентных алгоритмов адаптации. Их быстродействие сильно зависит от степени сложности помеховой обстановки – числа, расположения и интенсивности источников внешних шумовых помех (разброса собственных чисел пространственной корреляционной матрицы (**КМ**) **ШП**), что приводит к большому времени установления переходных процессов (малому быстродействию), т.е. к необходимости использования большого объема обучающих выборок.

Во второй статье [2] рассмотрены более сложные и быстродействующие квазиньютоновские алгоритмы адаптации на основе оценок максимального правдоподобия пространственных **КМ** гауссовых шумовых помех общего вида, быстродействие которых не зависит от степени сложности помеховой обстановки. Здесь же рассмотрены их регуляризованные разновидности и обоснована целесообразность их практической реализации на основе адаптивных решетчатых фильтров.

В третьей статье [3] описана математическая модель системы пространственной обработки сигналов на фоне собственного шума излучателей и внешних помех от точечных источников независимых шумовых излучений в РЛС с прямоугольной (в частности, квадратной) плоской ФАР.

В четвертой статье [4] на основе математической модели системы пространственной обработки сигналов на фоне шумовых помех обосновано количество, структура и месторасположение системы компенсационных каналов (модулей) в РЛС с плоской ФАР.

В данной статье описывается созданный на современной элементной базе опытный образец адаптивной системы защиты РЛС от маскирующих шумовых помех на основе адаптивного решетчатого фильтра (**АРФ**).

Статья организована следующим образом.

В п. 1 описывается структура и алгоритм адаптивной системы пространственной обработки сигналов на фоне маскирующих шумовых помех на основе **АРФ**, реализованные в опытном образце, в п. 2 описывается аппаратная часть опытного образца адаптивной системы защиты РЛС от маскирующих шумовых помех, а в п. 3 приводятся результаты предварительных испытаний.

1. СТРУКТУРА И АЛГОРИТМ АДАПТИВНОЙ СИСТЕМЫ ПРОСТРАНСТВЕННОЙ ОБРАБОТКИ СИГНАЛОВ НА ФОНЕ МАСКИРУЮЩИХ ШУМОВЫХ ПОМЕХ НА ОСНОВЕ АРФ

Структуру адаптивной системы пространственной обработки сигналов на фоне шумовых помех на основе адаптивного решетчатого фильтра (см. [2], п. 4, [5]) приведем для типичного случая наличия в радиолокаторах систем контроля воздушного пространства трех основных (информационных) каналов (одного суммарного и двух разностных), необходимых для измерения трех координат целей – дальности, азимута и угла места. Эти нерегулируемые основные каналы защищаются от внешних шумовых помех общей системой компенсационных (вспомогательных) модулей плоской ФАР, количество которых определяется количеством внешних источников и дисперсией параметров неидентичности (ширины частотной характеристики, временного сдвига огибающей импульсной характеристики, сдвига центральной частоты фильтра от номинального значения и т.п.) каналов [4]. В опытном образце выбрано $M_{comp} = 12$ компенсационных модулей, которые разнесены в пространстве в горизонтальной и вертикальной плоскостях.

Алгоритм оценивания каждого из трех $13-$мерных $(M = M_{comp} + 1 = 13)$ весовых векторов $\mathbf{r} = \begin{bmatrix} \mathbf{k} \\ 1 \end{bmatrix}$ адаптивной системы пространственной обработки с выделенным основным (13-м) каналом выбран общего вида с диагональной регуляризацией [2], поскольку обеспечение теплицевости или персимметрии корреляционной матрицы (**КМ**) требует строгого расположения фазовых центров приемных элементов эквидистантно или симметрично относительно фазового центра ФАР, что достаточно сложно обеспечить на практике. Объем обучающей выборки помехи K определен равным $K = 60$. Техническая реализация такого алгоритма выбрана на основе многоступенчатого параллельного **АРФ**, который при реально конечной разрядности вычислений обеспечивает более высокую эффективность обработки по сравнению с оценками **КМ** или матриц, обратных к ним, и весовых векторов, которые формируются явным образом.

Таким образом, в адаптивной системе пространственной обработки сигналов на фоне **ШП** в каждом (i-м, $i \in 1, KK$) элементе разрешения по дальности формируются три комплексных числа

$$\begin{aligned}
\varepsilon_\Sigma(i) &= \mathbf{r}_\Sigma^* \cdot \mathbf{u}_i^{(\Sigma)} = u_\Sigma(i) + \mathbf{k}_\Sigma^* \cdot \mathbf{u}_i^{(-)} = \\
&= u_\Sigma(i) + \sum_{j=1}^{12} k_j^{(\Sigma)*} \cdot u_j^{(-)}(i), \\
\varepsilon_{\Delta 1}(i) &= \mathbf{r}_{\Delta 1}^* \cdot \mathbf{u}_i^{(\Delta 1)} = u_{\Delta 1}(i) + \mathbf{k}_{\Delta 1}^* \cdot \mathbf{u}_i^{(-)} = \\
&= u_{\Delta 1}(i) + \sum_{j=1}^{12} k_j^{(\Delta 1)*} \cdot u_j^{(-)}(i), \\
\varepsilon_{\Delta 2}(i) &= \mathbf{r}_{\Delta 2}^* \cdot \mathbf{u}_i^{(\Delta 2)} = u_{\Delta 2}(i) + \mathbf{k}_{\Delta 2}^* \cdot \mathbf{u}_i^{(-)} = \\
&= u_{\Delta 2}(i) + \sum_{j=1}^{12} k_j^{(\Delta 2)*} \cdot u_j^{(-)}(i), \qquad i \in 1, KK.
\end{aligned} \tag{1}$$

Здесь $u_\Sigma(i), u_{\Delta 1}(i), u_{\Delta 2}(i)$ – комплексные отсчеты сигналов i-го $(i \in 1, KK)$ элемента разрешения в суммарном, первом и втором разностных каналах соответственно; $\mathbf{r}_\Sigma = \begin{pmatrix} \mathbf{k}_\Sigma \\ 1 \end{pmatrix}$, $\mathbf{r}_{\Delta 1} = \begin{pmatrix} \mathbf{k}_{\Delta 1} \\ 1 \end{pmatrix}$, $\mathbf{r}_{\Delta 2} = \begin{pmatrix} \mathbf{k}_{\Delta 2} \\ 1 \end{pmatrix}$ – $13-$мерные комплексные весовые векторы для суммарного, первого и второго разностных каналов; $\mathbf{u}_i^{(\Sigma)} = \begin{pmatrix} \mathbf{u}_i^{(-)} \\ u_\Sigma(i) \end{pmatrix}$, $\mathbf{u}_i^{(\Delta 1)} = \begin{pmatrix} \mathbf{u}_i^{(-)} \\ u_{\Delta 1}(i) \end{pmatrix}$, $\mathbf{u}_i^{(\Delta 2)} = \begin{pmatrix} \mathbf{u}_i^{(-)} \\ u_{\Delta 2}(i) \end{pmatrix}$ – $13-$мерные векторы, которые состоят из комплексных отсчетов сигналов $\mathbf{u}^{(-)}$ 12 компенсационных каналов, одинаковых для суммарного, первого и второго разностных каналов, и одного основного (суммарного u_Σ или одного из двух разностных $u_{\Delta 1}$, $u_{\Delta 2}$) в i-м элементе разрешения; звездочка $(*)$ – знак эрмитового сопряжения (транспонирования и комплексного сопряжения).

Указанные комплексные числа ($\varepsilon_\Sigma(i)$, $\varepsilon_{\Delta 1}(i)$, $\varepsilon_{\Delta 2}(i)$) формируются на выходах трех весовых сумматоров, показанных на рис. 1. Развернутое изображение весового сумматора для суммарного канала показано на рис. 2.

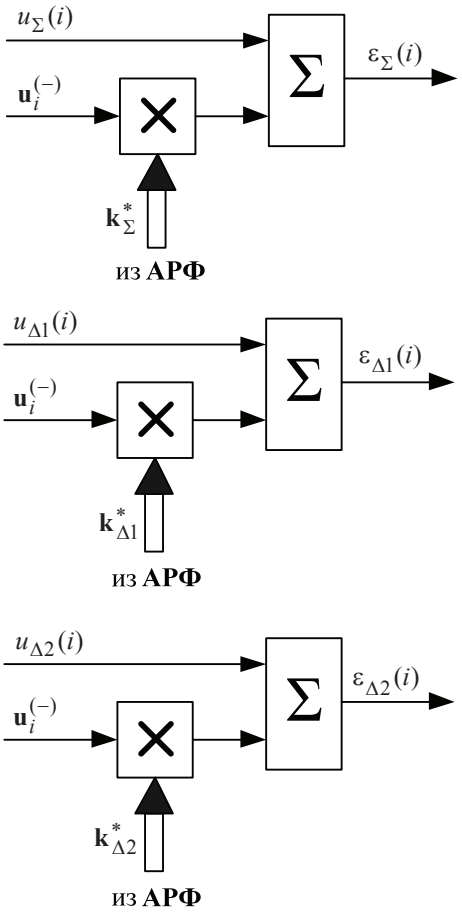


Рис. 1. Весовые сумматоры

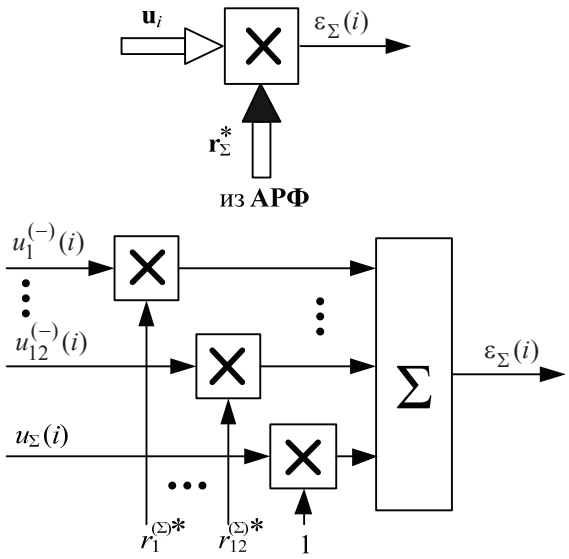


Рис. 2. Весовой сумматор

Весовые сумматоры других информационных каналов имеют ту же структуру и отличаются только значениями отсчетов на основном входе и весовыми векторами, сформированными **АРФ**.

Начальными данными для расчета 3×13 матрицы

$$\mathbf{R}_{(3\times13)}=\begin{pmatrix}\mathbf{r}_{\Sigma}^{(13)*}\\ \mathbf{r}_{\Delta1}^{(13)*}\\ \mathbf{r}_{\Delta2}^{(13)*}\end{pmatrix} \qquad (2)$$

из трех $13-$мерных комплексных весовых векторов $\mathbf{r}_{\Sigma}^{(13)*}$, $\mathbf{r}_{\Delta1}^{(13)*}$, $\mathbf{r}_{\Delta2}^{(13)*}$ служит 15×60 матрица (обучающая выборка) $\mathbf{YY}_{(15\times60)}=\begin{pmatrix}\mathbf{Y}_{(12\times60)}\\ \mathbf{G}_{(3\times60)}\end{pmatrix}$, составленная из матрицы $\mathbf{Y}_{(12\times60)}$ $12-$мерных комплексных векторов отсчетов сигналов 12 компенсационных каналов приема в 60 сопредельных интервалах разрешения ($K=60$), набранных на этапе настройки, и 3×60 матрицы $\mathbf{G}_{(3\times60)}=\left(\mathbf{y}_{\Sigma}^{(60)},\ \mathbf{y}_{\Delta1}^{(60)},\ \mathbf{y}_{\Delta2}^{(60)}\right)^{*}$, образованной $60-$мерными вектор-строками отсчетов сигналов в суммарном ($\mathbf{y}_{\Sigma}^{(60)}$) и двух разностных ($\mathbf{y}_{\Delta1}^{(60)}$ и $\mathbf{y}_{\Delta2}^{(60)}$) каналах строго в тех же 60 интервалах разрешения, из которых сформирована обучающая выборка вспомогательных каналов приема.

Каждый из трех весовых векторов вычисляется по алгоритму

$$\mathbf{r}^{*}=\frac{1}{h_{13,13}}\cdot\left[\mathbf{e}_{13}^{*},\ \mathbf{0}_{13}^{*}\right]\cdot\begin{bmatrix}\mathbf{H}_{(13\times13)}\\ \mathbf{N}_{(13\times13)}^{*}\end{bmatrix}=\frac{1}{h_{13,13}}\cdot\mathbf{hp}^{(13)*}, \qquad (3)$$

где $\widehat{\mathbf{k}}_{\Sigma}^{*}=\left[k_{j}^{(\Sigma)*}\right]_{j=1}^{M_{comp}=12}$ – $M_{comp}=12-$мерный весовой вектор компенсационных каналов; $h_{13,13}$ – последний элемент вектора $\mathbf{hp}^{(13)*}=\mathbf{e}_{13}^{*}\cdot\mathbf{H}_{(13\times13)}$ треугольной матрицы $\mathbf{H}_{(13\times13)}=\left(h_{i,j}\right)_{i,j=1}^{13}$ (см. [2], п. 4); $\mathbf{e}_{13}^{*}=[0\ 0\ldots0\ 1]$ – последняя строка единичной $\mathbf{I}_{(13\times13)}$ матрицы; $\mathbf{0}_{13}^{*}=[0\ 0\ldots0\ 0]$ – $13-$мерный вектор-строка из нулевых элементов.

Матрица $\begin{bmatrix}\mathbf{H}_{(13\times13)}\\ \mathbf{N}_{(13\times13)}^{*}\end{bmatrix}$ получена пропусканием единичной матрицы $\mathbf{I}_{(13\times13)}$ через настроенный **АРФ**, параметры которого оценены по обучающей выборке $\begin{bmatrix}\mathbf{Y}_{(12\times60)}\\ \mathbf{y}^{(60)*}\end{bmatrix}$, состоящей из отсчетов сигналов 12 вспомогательных и одного основного (суммарного, первого или второго разностного) канала. При использовании регуляризованого алгоритма оценивания весового вектора с регуляризатором $\beta_{o}^{-1}\cdot\mathbf{I}_{(13\times13)}$ (см. [2], п. 3) такое пропускание единичной матрицы уже не нужно.

Таким образом, для формирования трех весовых векторов для суммарного и двух разностных каналов необходимо три $13-$канальных **АРФ**. Схема формирования весового вектора для суммарного канала показана на рис. 3.

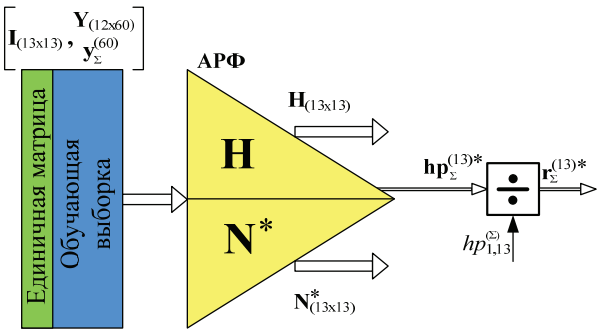


Рис. 3. Схема алгоритма (2) формирования весового вектора для суммарного канала на основе **АРФ**

Однако реализация трех $13-$канальных АРФ есть неоправданно сложной. Поэтому разработана адаптивная система одновременной помехозащиты 3-х информационных каналов на основе одного параллельного **АРФ** [6] для технической реализации в опытном образце. На рис. 4 показана структура такого $15-$канального $13-$ступенчатого **АРФ** с 12-ю общими вспомогательными каналами и тремя информационными (суммарным и двумя разностными). Его основой является элементарный решетчатый фильтр (**ЭРФ**) – двухвходовой сумматор с перекрестными связями.

Соответствующий алгоритм формирования на его основе необходимых весовых векторов

$$\mathbf{R}=\left[\mathbf{E}_{(3\times15)}^{*},\ \mathbf{0}_{(3\times15)}^{*}\right]\cdot\begin{bmatrix}\mathbf{H}_{(15\times13)}\\ \mathbf{N}_{(15\times13)}^{*}\end{bmatrix}\cdot\mathbf{C},$$

$$\mathbf{C}=\begin{bmatrix}1/hp_{1,13}^{(\Sigma)} & 0 & 0\\ 0 & 1/hp_{1,13}^{(\Delta1)} & 0\\ 0 & 0 & 1/hp_{1,13}^{(\Delta2)}\end{bmatrix} \qquad (4)$$

описан ниже.

В (4) $\mathbf{E}_{(3\times15)}^{*}$ – матрица, которая состоит из последних трех строк единичной матрицы $\mathbf{I}_{(15\times15)}$; матрица $\begin{bmatrix}\mathbf{H}_{(15\times13)}\\ \mathbf{N}_{(15\times13)}^{*}\end{bmatrix}$ получена на выходе **АРФ** в результате его настройки (оценки параметров) по обучающей выборке

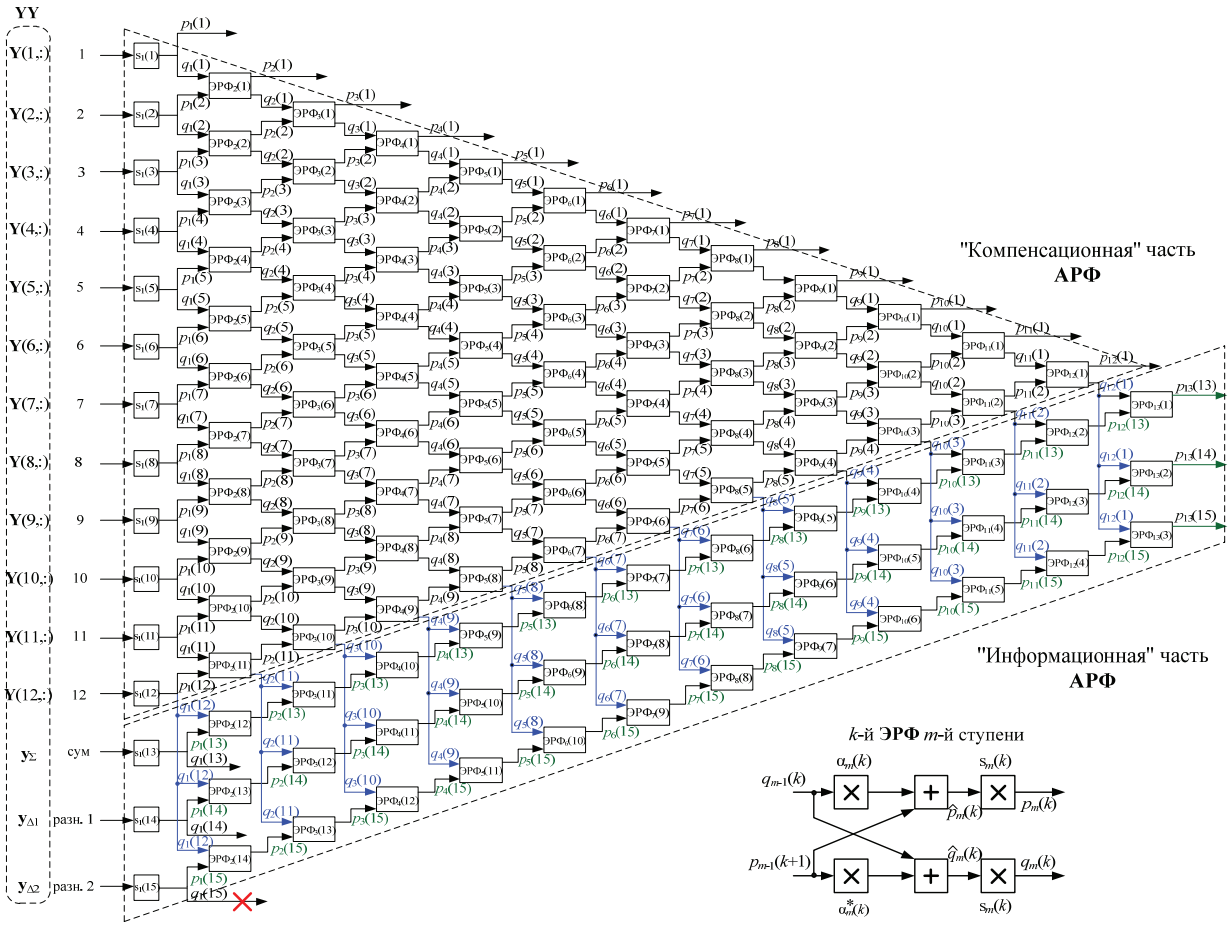


Рис. 4. Схема 15 – канального 13 – ступенчатого АРФ

$$\mathbf{YY}_{(15\times 60)} = \begin{bmatrix} \mathbf{Y}_{(12\times 60)} \\ \mathbf{y}_{\Sigma}^{(60)*} \\ \mathbf{y}_{\Delta 1}^{(60)*} \\ \mathbf{y}_{\Delta 2}^{(60)*} \end{bmatrix} \tag{5}$$

и "прогона» через него "специфической" единичной матрицы

$$\mathbf{II}_{(15\times 13)} = \begin{bmatrix} \mathbf{I}_{(13\times 13)} \\ \mathbf{e}_{13}^{*} \\ \mathbf{e}_{13}^{*} \end{bmatrix}. \tag{6}$$

Элементами диагональной матрицы $\mathbf{C}$ (4) выступают множители, нормирующие последний элемент весовых векторов

$$\begin{aligned} \mathbf{r}_{\Sigma}^{(13)*} &= \mathbf{hp}_{\Sigma}^{*} / hp_{1,13}^{(\Sigma)} = \left[\mathbf{k}_{\Sigma}^{*}, 1 \right], \\ \mathbf{r}_{\Delta 1}^{(13)*} &= \mathbf{hp}_{\Delta 1}^{*} / hp_{1,13}^{(\Delta 1)} = \left[\mathbf{k}_{\Delta 1}^{*}, 1 \right], \\ \mathbf{r}_{\Delta 2}^{(13)*} &= \mathbf{hp}_{\Delta 2}^{*} / hp_{1,13}^{(\Delta 2)} = \left[\mathbf{k}_{\Delta 2}^{*}, 1 \right]. \end{aligned} \tag{7}$$

Перейдем к описанию алгоритма адаптивной цифровой системы пространственной обработки сигналов на фоне маскирующих шумовых помех, который реализуется в два этапа – основном (на «рабочем ходе») и подготовительном (на этапе вычисления весовых векторов после набора обучающей выборки).

На рис. 5 приведена схема алгоритма одновременного формирования матрицы $\mathbf{R}_{(3\times 13)}$ (2) весовых векторов на основе одного **АРФ**, показанного на рис. 4.

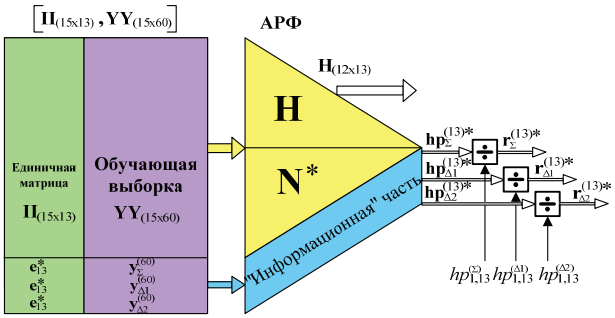


Рис. 5. Схема алгоритма (3) формирования матрицы весовых векторов $\mathbf{R}_{(3\times 13)}$ (2) на основе **АРФ**

Матрица весовых векторов $\mathbf{R}_{(3\times 13)}$ (2) формируется по следующей процедуре.

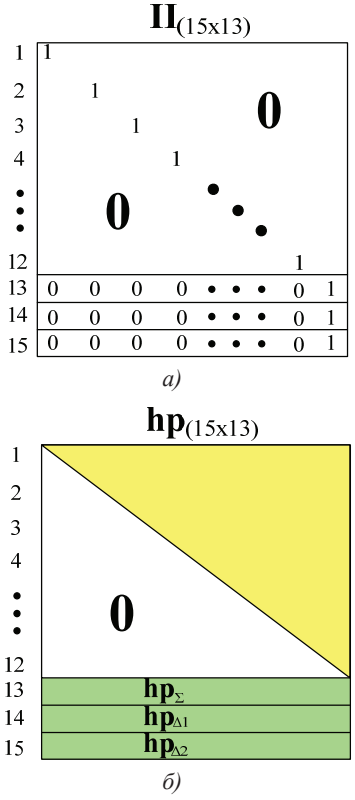
Обучающая 15×60 выборка $\mathbf{YY}_{(15\times 60)}$ (5) используется для оценки параметров (настройки) **АРФ**.

Одновременно с обучающей выборкой через оцененные параметры **АРФ** "прогоняется" матрица $\mathbf{II}_{(15\times13)}$ (6), которая в оценке параметров **АРФ** не участвует. После первой ступени матрица $\mathbf{II}_{(15\times13)}$ преобразуется в две подматрицы $\mathbf{hp}_{(15\times13)}$ и $\mathbf{hq}_{(15\times13)}$.

После "прогона" матрицы $\mathbf{II}_{(15\times13)}$ весовые векторы $\mathbf{R}_{(3\times13)}$ получаются в последних трех строках матрицы $\mathbf{hp}_{(15\times13)}$ после нормировки каждого из них на его последний (13- й) элемент.

1. По обучающей выборке $\mathbf{YY}_{(15\times60)}$ (5), строки которой поступают на соответствующие входы **АРФ** (рис. 4), определяются множители $s_1(\ell)$ $(\ell\in1,15)$ первой степени $(m=1)$ и параметры $\alpha_m(\ell)$, $\beta_m(\ell)=\alpha_m^*(\ell)$, $s_m(\ell)=c_m(\ell)$ всех **ЭРФ** (рис. 4) его следующих ступеней $(m\in2,\ 13;\ \ell\in1,\ 15-m+1)$. Процесс вычисления этих параметров называется настройкой **АРФ** [7].

2. Через настроенный **АРФ** с параметрами $\alpha_m(\ell)$ и $s_m(\ell)$, полученными по обучающей выборке в предыдущем пункте, "прогоняется" единичная матрица $\mathbf{II}_{(15\times13)}$ (рис. 6).



а)

б)

Рис. 6. Структура матриц $\mathbf{II}_{(15\times13)}$ (*а*) на входе и $\mathbf{hp}_{(15\times13)}$ (*б*) на выходе **АРФ**

На выходе **АРФ** формируется матрица $\mathbf{hp}_{(15\times13)}$, каждая из последних трех строк которой нормируется на "свой" последний (13-й) элемент $hp_{1,13}$. Полученные после нормировки последние строки соответствуют весовым векторам для суммарного $\mathbf{r}_{\Sigma}^{(13)*}$, первого $\mathbf{r}_{\Delta1}^{(13)*}$ и второго $\mathbf{r}_{\Delta2}^{(13)*}$ разностных каналов. Эти весовые векторы используются в весовых сумматорах (рис. 1, 2).

3. Общая схема настройки **АРФ** по обучающей выборке $\mathbf{YY}_{(15\times60)}$ (5).

Настройка должна определить

– 15 нормирующих множителей $s_1(\ell)$ $(\ell\in1,15)$, первой $(m=1)$ ступени **АРФ** (рис. 4) – по выборке $\mathbf{YY}_{(15\times60)}$.

– параметры $\alpha_m(\ell)$ и $\beta_m(\ell)=\alpha_m^*(\ell)$ ℓ-го $(\ell\in1,15-m+1)$ **ЭРФ** m-й $(m\in2,13)$ ступени **АРФ** (рис. 4) – по выходным сигналам предыдущей ступени.

– нормирующие множители $s_m(\ell)=c_m(\ell)$ $(m\in2,13;\ \ell\in1,15-m+1)$ – по выходным сигналам соответствующего "ненормированного" **ЭРФ**.

2. ОПИСАНИЕ ОПЫТНОГО ОБРАЗЦА АДАПТИВНОЙ СИСТЕМЫ ЗАЩИТЫ РЛС ОТ ШУМОВЫХ ПОМЕХ

Опытный образец (рис. 7) цифровой системы адаптивной защиты радиолокаторов от маскирующих шумовых помех выполнен на основе 15-входового 13-ступенчатого параллельного адаптивного решетчатого фильтра (рис. 4) на базе программируемой логической интегральной схемы (**ПЛИС**).

Рис. 7. Опытный образец

Требуемые в задачах обработки сигналов на фоне помех функции матриц, обратных корреляционным, в **АРФ** формируются без явного вычисления этих матриц, что обеспечивает важные практические преимущества по сравнению с традиционными методами. Например, **АРФ** сохраняет устойчивость в условиях ограниченной разрядной сетки [2].

Опытный образец обеспечивает одновременную защиту трех основных (информационных) каналов (суммарного и двух разностных) от 1–12 источников **ШП** 12 - ю компенсационными каналами.

Для этого **АРФ** формирует набор из трех весовых векторов пространственной (межканальной) обработки $\mathbf{r}_{\Sigma}^{(13)*}$, $\mathbf{r}_{\Delta 1}^{(13)*}$, $\mathbf{r}_{\Delta 2}^{(13)*}$, как функции матриц, обратных корреляционным матрицам помехи, заданных в факторизованной форме.

Микросхема **ПЛИС** позволяет создавать системы на кристалле (SistemOnChip) для решения многочисленных классов задач, в частности, для реализации алгоритмов обработки сигналов с распараллеливанием процессов. В опытном образце на параллельных процессах реализована полная ступень **АРФ**, весовые сумматоры (скалярные переножители) и пр.

Для решения такого класса задач **ПЛИС** содержит следующие архитектурные блоки:

- сигнальные процессоры (до 2800 DSP процессоров на кристалле, реально задействовано в образце – 2080 DSP процессоров),
- блочная память суммарной емкости до 37 Мбайт – для хранения промежуточных данных в процессе обработки сигналов;
- 485 тысяч логических элементов – для построения схем межблочного обмена;
- развитую систему интерфейсов, включая современные последовательные гигабитные интерфейсы, в частности PCIexpress 8 lane;
- развитую структуру скоростной синхронизации блоков с малым перекосом фаз;
- блоки ввода/вывода с поддержкой многочисленных современных сигнальных стандартов.

Все параллельные структуры DSP обработки имеют тактовую частоту 200 МГц, что позволило обеспечить время пространственной фильтрации (скалярного произведения векторов) в одном элементе дальности, равное 5 нс.

Кроме памяти, встроенной в микросхему, плата опытного образца имеет высокоскоростное оперативное запоминающее устройство типа DDR3 (емкостью 1 ГБ), память начальных настроек EEPROM (1КБ).

Для программирования и отладки программного обеспечения используется последовательный интерфейс JTAG.

Обмен данными осуществляется через встроенный в микросхему процессора интерфейс PCI Express 8-lane.

Модификация (перепрограммирование) **ПЛИС** возможна из дополнительного накопителя флэш-памяти FLASH (128 МБ).

Через разъемные соединения FMC возможно подключение дополнительных мезонинных модулей стандарта FMC.

3. РЕЗУЛЬТАТЫ ИСПЫТАНИЙ ОПЫТНОГО ОБРАЗЦА

Иллюстрируются видом экрана ИКО РЛС 10-см диапазона до (*а*) и после (*б*) компенсации шумовых помех от $n = 5$ (рис. 8) и $n = 10$ (рис. 9) точечных внешних источников. Видно, что при выключенной системе защиты (*а*) шумовые помехи маскируют полезные сигналы и отметки воздушных целей обнаружить практически невозможно, тогда как после ее включения они уверенно обнаруживаются.

Результаты предварительных испытаний опытного образца на основе **АРФ** по смоделированным шумовым помехам и цифровым записям реальных шумовых помех показали существенный выигрыш в эффективности помехозащиты по сравнению со штатными системами существующих РЛС, в частности, цифровым автокомпенсатором (**ЦАК**) с корреляционными обратными связями и градиентным алгоритмом настройки весовых коэффициентов [1, 8].

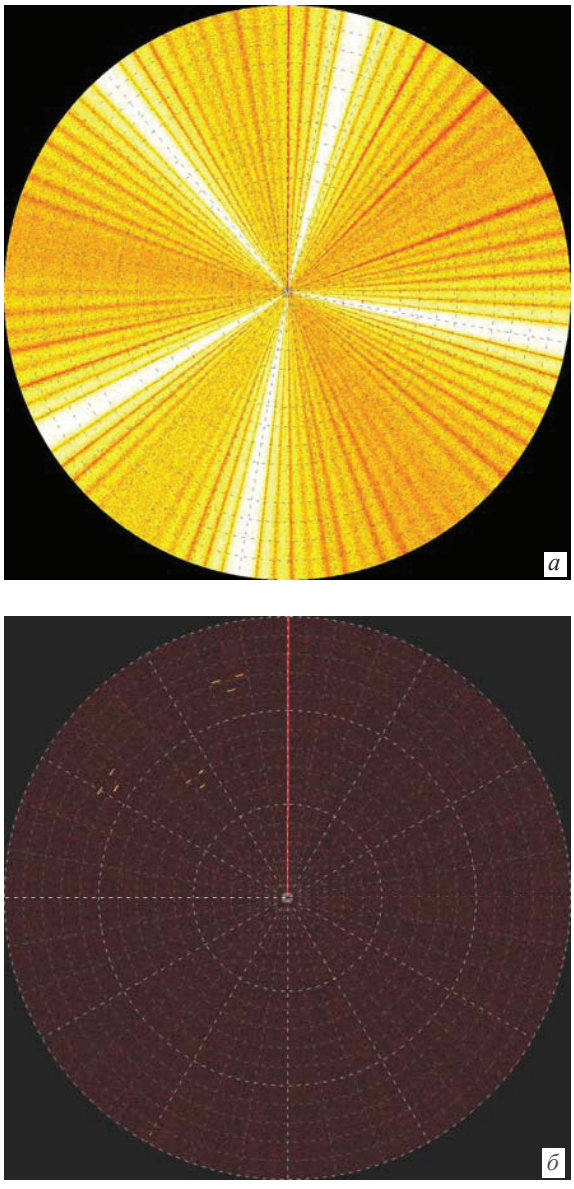


Рис. 8. Экран ИКО до (*а*) и после компенсации (*б*)

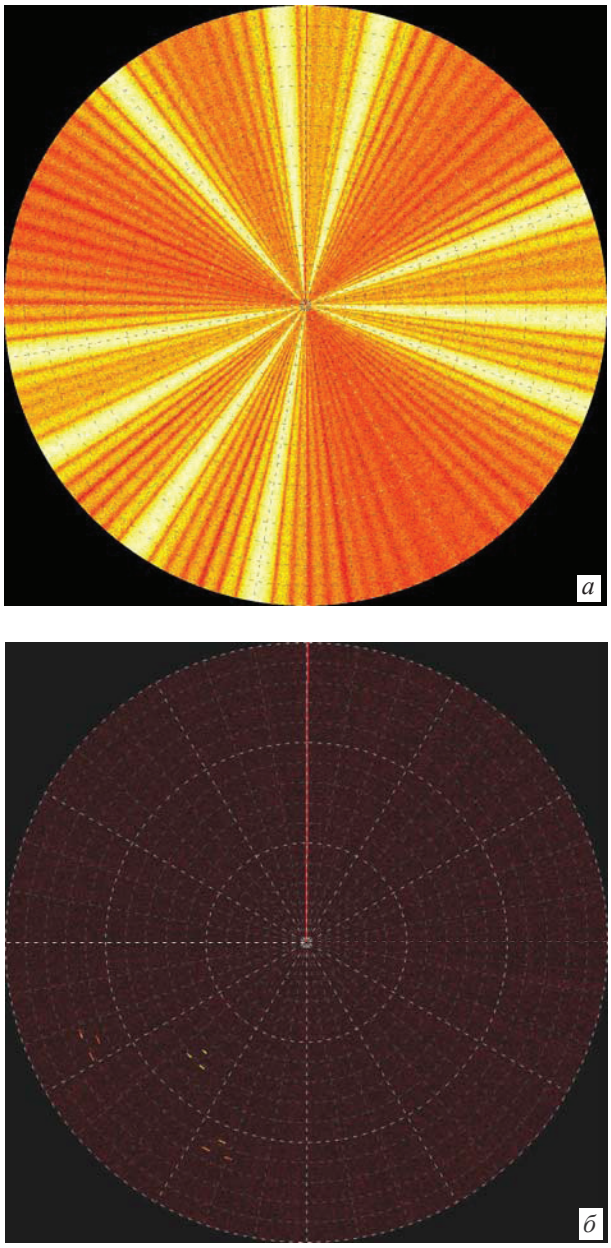


Рис. 9. Экран ИКО до (*а*) и после компенсации (*б*)

Так, на рис. 10 показаны зависимости средних потерь

$$\bar{\hat{\chi}} = \frac{\bar{\hat{\mu}}}{\mu} \le 1,$$

$$\hat{\mu} = \left| \mathbf{x}^* \cdot \hat{\mathbf{r}} \right|^2 \Big/ \hat{\mathbf{r}}^* \cdot \mathbf{\Phi} \cdot \hat{\mathbf{r}}, \quad \mu = \mathbf{x}^* \cdot \mathbf{\Psi} \cdot \mathbf{x}, \qquad (7)$$

$$\hat{\mathbf{r}} = \hat{\mathbf{\Psi}} \cdot \mathbf{x}, \quad \hat{\mathbf{\Psi}} = \hat{\mathbf{\Phi}}^{-1},$$

выходного отношения сигнал/(помеха + шум) (**ОСПШ**) $\hat{\mu}$ адаптивного фильтра с импульсной характеристикой (**ИХ**) $\hat{\mathbf{r}} = \hat{\mathbf{\Psi}} \cdot \mathbf{x}$ по сравнению с максимальным **ОСПШ** $\mu = \mathbf{x}^* \cdot \mathbf{\Psi} \cdot \mathbf{x}$ оптимального фильтра с **ИХ** (весовым вектором) $\mathbf{r} = \mathbf{\Psi} \cdot \mathbf{x}$ в гипотетических условиях полной априорной определенности от объема обучающей выборки K смоделированных шумовых помех, создаваемых $n = 4$ источниками, действующими в области боковых лепестков ДН ФАР, при отношении помеха/шум в основном (суммарном) канале $h_0 = 30$ дБ. Здесь $\mathbf{\Psi} = \mathbf{\Phi}^{-1}$ – матрица, обратная корреляционной матрице помехи (**КМ**) $\mathbf{\Phi}$, $\mathbf{x}$ – вектор пространственного сигнала (фазового распределения на апертуре).

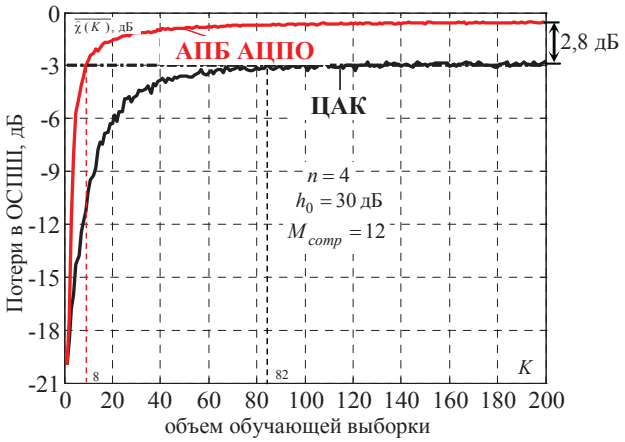


Рис. 10. Зависимость потерь в **ОСПШ** от объема обучающей выборки

Анализ рис. 10 показывает, что опытный образец на основе **АРФ** в переходном режиме обеспечивает быстродействие адаптации $(K = 8)$, определяемое объемом выборки K, при котором потери **ОСПШ** $\bar{\hat{\chi}}(K)$ не превышают 3 дБ, на порядок выше, чем ЦАК $(K = 82)$.

Это обусловлено тем, что скорость сходимости градиентных алгоритмов (**ЦАК**), в отличие от квазиньютоновских алгоритмов, определяется спектром (совокупностью собственных значений) **КМ** помех его вспомогательных каналов. Эта **КМ** и, следовательно, ее спектр зависят от числа, интенсивности и взаимного расположения источников помех.

Кроме того, в установившемся режиме обеспечивается также выигрыш в **ОСПШ**, равный 2,8 дБ.

Рис. 11 иллюстрирует существенный выигрыш $\Delta = k_{p\text{ОпОбр}} - k_{p\text{ЦАК}}$ (в дБ) в коэффициенте подавления k_p опытного образца по сравнению с ЦАК в испытаниях по **ШП**, создаваемых тремя постановщиками для метровой РЛС. При этом опытный образец

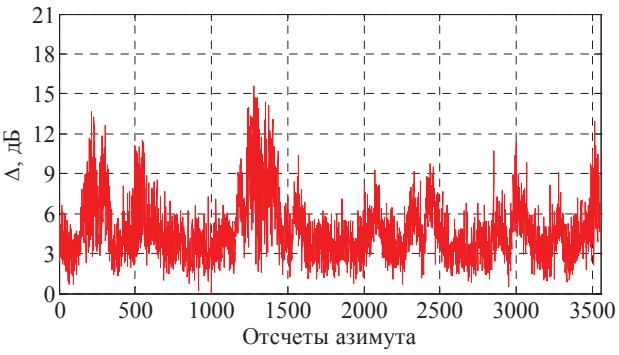


Рис. 11. Выигрыши в коэффициенте подавления

настраивался по обучающей выборке объемом $K = 16$, а **ЦАК** – по $K = 55$, количественно компенсационных каналов – $M_{comp} = 3$. Видно, что в зависимости от азимута направления визирования он составляет от 3 до 15 дБ.

Таким образом, внедрение созданного опытного образца адаптивной цифровой пространственной обработки сигналов на фоне маскирующих шумовых помех в существующие и новые РЛС позволит обеспечить рекордные на сегодняшний день показатели эффективности адаптации.

Литература

[1] *Рябуха В.П.* Адаптивные системы защиты РЛС от шумовых помех. 1. Корреляционные автокомпенсаторы на основе стохастических градиентных алгоритмов адаптации – Х.: Прикладная радиоэлектроника. – 2016. – Т. 15, № 1 – С. 11–25.

[2] *Рябуха В.П.* Адаптивные системы защиты РЛС от шумовых помех. 2. Квазиньютоновские корреляционные автокомпенсаторы. Адаптивные решетчатые фильтры. – Х.: Прикладная радиоэлектроника. – 2016. – Т. 15, № 2. – С. 88–99.

[3] *Рябуха В.П.* Адаптивные системы защиты РЛС от шумовых помех. 3. Математическая модель системы пространственной обработки сигналов в РЛС с двумерной плоской ФАР – Х.: Прикладная радиоэлектроника. – 2016. – т. 15, № 4. – С. 301–315.

[4] *Рябуха В.П.* Адаптивные системы защиты РЛС от шумовых помех. 4. Выбор количества, структуры и месторасположения компенсационных модулей в РЛС с плоской ФАР – Х.: Прикладная радиоэлектроника. – 2017. — Т. 16, № 1. — С. 11–25.

[5] *Леховицкий Д.И.* Адаптивные решетчатые фильтры. Часть I. Теория решетчатых структур II. / *Д.И. Леховицкий, Д.С. Рачков, А.В. Семеняка, В.П. Рябуха, Д.В. Атаманский* // Прикладная радиоэлектроника. – 2011. – Т. 10, № 4. – С. 381–404.

[6] Патент на корисну модель №112834 «Система захисту основних (інформаційних) каналів від шумових завад» від 26.12.2016, власник – Харківський національний університет радіоелектроніки, винахідники: Д.І. Леховицький, В.П. Рябуха, А.В. Семеняка, Є.А. Катюшин.

[7] *Леховицкий Д.И.* Адаптивные решетчатые фильтры. Част. II. Алгоритмы настройки АРФ / *Д.И. Леховицкий, Д.С. Рачков, А.В. Семеняка, В.П. Рябуха, Д.В. Атаманский* // Прикладная радиоэлектроника. – 2011. – Т. 10, № 4. – С. 405–418.

[8] Радиоэлектронные системы. Основы построения и теория: Справочник/ *Я.Д. Ширман, С.Т. Багдасарян, А.С. Маляренко, Д.И. Леховицкий, С.П. Лещенко, Ю.И Лосев, А.И. Николаев, С.А Горшков, С.В. Москвитин, В.М. Орленко* / Под ред. *Я.Д. Ширмана*. – М.: Радиотехника. – 2007. – 512 с.

Поступила в редколлегию 20.12.2017

Леховицкий Давид Исаакович, докт. техн. наук, профессор, начальник отделения Государственного предприятия «Научно-исследовательский институт радиолокационных систем «Квант-Радиолокация». Область научных интересов – адаптивная пространственно-временная обработка сигналов на фоне помех в информационных системах различного назначения.

Рябуха Вячеслав Петрович, канд. техн. наук, доцент, заместитель начальника отделения Государственного предприятия «Научно-исследовательский институт радиолокационных систем «Квант-Радиолокация». Область научных интересов – радиолокационные системы, обнаружение и измерение параметров сигналов на фоне помех.

Семеняка Андрей Викторович, канд. техн. наук, ведущий научный сотрудник Государственного предприятия «Научно-исследовательский институт радиолокационных систем «Квант-Радиолокация». Область научных интересов – унифицированные процессоры и системы адаптивной обработки сигналов на фоне помех.

Катюшин Евгений Анатольевич, научный сотрудник Государственного предприятия «Научно-исследовательский институт радиолокационных систем «Квант-Радиолокация». Область научных интересов – моделирование адаптивных систем пространственно-временной обработки сигналов на фоне помех.

Гриценко Виктор Николаевич, главный специалист научно-технического центра Казенного предприятия "Научно-производственный комплекс "Искра". Область научных интересов – программирование цифровых сигнальных процессоров и программируемых логических интегральных схем.

УДК 621.396.965:621.391.26

Адаптивні системи захисту РЛС від шумових завад. 5. Дослідний зразок системи завадозахисту / Д.І. Леховицький, В.П. Рябуха, А.В. Семеняка, Є.А. Катюшин, В.М. Гриценко // Прикладна радіоелектроніка: наук.-техн. журнал. – 2017. – Том 16, №3, 4. – С. 97–105.

П'ята стаття циклу статей по адаптивних системах захисту РЛС від маскувальних шумових завад. Описується дослідний зразок системи адаптивної цифрової просторової обробки сигналів на тлі маскувальних шумових завад на основі адаптивного решітчастого фільтра, виконаний на базі

логічної інтегральної схеми, що програмується, наводяться результати попередніх випробувань.

Ключові слова: дослідний зразок, шумові завади, логічна інтегральна схема, що програмується, випробування.

Іл.: 11 Бібліогр.: 08 найм.

UDC 621.396.965:621.391.26

Adaptive radar noise jamming protection systems. 5. Exploratory model of a jamming protection system. / D.I. Lekhovitskiy, V.P. Riabukha, A.V. Semenyaka, E.A. Katyushin, V.M. Grytsenko // Applied Radio Electronics: Sci. Journ. – 2017. – Vol. 16, № 3, 4. – P. 97–105.

This article is the fifth one of a series of articles devoted to adaptive radar masking noise jamming protection systems. An exploratory model of the system, is described that is based on an adaptive lattice filter made on the base of a programmable logic integral circuit, for adaptive digital space processing of signals embedded in masking noise jamming. Results of pre-testing are given.

Keywords: exploratory model, noise jamming, programmable integral circuit, testing

Fig.: 11. Ref.: 08 items.

УДК 621.396.96

РАЗВИТИЕ МЕТОДА ДЕКОМПОЗИЦИИ ПРИ ФОРМИРОВАНИИ РАДИОМЕТРИЧЕСКИХ ИЗОБРАЖЕНИЙ НАЗЕМНЫХ ОБЪЕКТОВ СЛОЖНОЙ ФОРМЫ В БЛИЖНЕЙ И ПРОМЕЖУТОЧНОЙ ЗОНАХ АНТЕННЫ

В. Н. БЫКОВ, С. Н. БЫКОВ, С. А. ВИННИЧЕНКО, А. М. ГРИЧАНЮК, Н. Н. КОЛЧИГИН, Г. Г. ОСИНОВЫЙ

Предложено применение известного метода декомпозиции, используемого для измерения эффективной поверхности рассеяния объектов сложной формы в ближней и промежуточной зонах антенны радиолокатора, для оценки с помощью радиометрического измерительного комплекса миллиметрового диапазона (ММД) интегральной радиояркостной температуры наземного объекта сложной формы и формирования его двухмерного радиометрического изображения. Представлены характеристики и методика измерений радиояркостной температуры объектов изучаемой сцены с помощью радиометрического измерительного комплекса 8 мм диапазона в ближней и промежуточной зонах антенны. Произведена оценка снижения радиояркостного контраста «объект – фон» за счет применения радиопоглощающего материала.

Ключевые слова: наземный объект сложной формы, радиометрический измерительный комплекс, миллиметровый диапазон, радиопоглощающий материал.

ВВЕДЕНИЕ

Известно применение метода декомпозиции для экспериментально-расчетного определения радиолокационной характеристики – эффективной поверхности рассеяния (ЭПР) наземного объекта [1]. Применение радиолокационных станций для определения ЭПР объектов в дальней зоне антенны часто трудно реализуемо технически. Это вызвано необходимостью устранения мешающих переизлучений от соседствующих с объектом естественных ландшафтов (деревьев, кустов) и искусственных сооружений техногенного характера. Применение для этих целей безэховых камер ограничивает размеры исследуемых объектов.

В работе [2] приведена методика измерения характеристик радиолокационного отражения объектов декомпозиционным методом в ближней и промежуточной зонах антенны. В основу методики положен тот факт, что поле, отраженное от объекта сложной формы, имеет локальный характер. Таким образом, полное поле от объекта представляет сумму полей от локальных разрешаемых участков (без учета взаимодействия). Коэффициент отражения K_i каждого из локальных участков можно измерить с помощью малогабаритного измерителя коэффициента отражения в ближней и промежуточной зонах антенны.

Поверхность объекта сложной формы делится на разрешаемые участки, со сторонами каждого участка больше длины волны $d > \lambda$. Размеры участков разрешения выбираются равными размеру облучаемого «пятна» диаграммы направленности антенны (ДНА) по уровню половинной мощности, для заданного расстояния R. Измеритель коэффициента отражения при измерении амплитуды отраженного сигнала от составных частей объекта располагается на расстоянии R от центров разрешаемых участков таким образом, чтобы его оптическая ось проходила через центры участков. При каждом последующем измерении измеритель коэффициента отражения перемещается (параллельно оси R) на величину d.

Так как поле, отраженное от объекта сложной формы, представляет собой сумму полей от отдельных участков разрешения, то средняя ЭПР всего объекта $\bar{\sigma}_{об}$ приближенно равна сумме средних ЭПР локальных участков $(\bar{\sigma}_i)$, при этом считается, что фазы отраженных полей взаимно независимы и случайны:

$$\bar{\sigma}_{об} = \frac{1}{N}\sum_{i=1}^{N}\bar{\sigma}_i , \qquad (1)$$

где N – количество участков разбиения объекта.

ЭПР локальных участков объекта определяется с помощью эталона и рассчитывается по формуле:

$$\bar{\sigma}_i = \frac{P_{об}}{P_{эт}}\bar{\sigma}_{эт} = K_{i\ об}\bar{\sigma}_{эт}, \qquad (2)$$

где $P_{об}$ и $P_{эт}$ – мощности отраженных сигналов от участка объекта и эталона, соответственно, $K_{i\,об} = \frac{P_{об}}{P_{эт}}$ – значения коэффициента отражения от участка объекта по мощности. В качестве эталона рассматривается плоский металлический экран с коэффициентом отражения $K_{эт} = 1$, геометрические размеры которого равны: $a = 2Rtg\,\theta^0_{0,5}/2$, $b = 2Rtg\,\varphi^0_{0,5}/2$, $\theta^0_{0,5}, \varphi^0_{0,5}$ – значения ширины диаграммы направленности передающей, в данном случае рупорной, антенны по половинной мощности в двух плоскостях.

Указанный метод декомпозиции может быть применим для оценки интегральной радиояркостной температуры объекта, радиояркостного контраста «объект–фон», формирования радиометрических (РМ) изображений объектов по результатам экспериментальных измерений, полученных при помощи РМ датчиков миллиметрового диапазона (ММД) волн. РМ датчик ММД представляет собой апертурную (зеркальную параболическую или линзовую) антенну и радиометрический приемник миллиметрового диапазона.

В работе [3] приведены РМ изображения, полученные с помощью радиометрического измерительного комплекса ММД в дальней зоне антенны (рис.1, рис.2). В приведенной работе формирование РМ изображений осуществляется путем пространственного объединения радиояркостных температур разрешаемых элементов объекта, т. е. также имеет место реализация метода декомпозиции.

Рис.1. Фото и РМ изображение объекта в дальней зоне

Рис.2. Внешний вид РМ измерительного комплекса ММД

Отличие метода [3] от метода, приведенного в работах [1,2], состоит в том, что визирование объекта осуществляется из одной точки посредством углового перемещения диаграммы направленности антенны (ДНА) радиометрического измерительного комплекса в горизонтальной и вертикальной плоскостях, а не за счет параллельного переноса антенны. При этом, как показали результаты формирования изображений малоразмерного наземного объекта на дальности порядка 20 м (рис.1), геометрические искажения изображений практически не наблюдаются.

В связи с тем, что формирование изображений в дальней зоне антенны не всегда представляется возможным, а безэховая камера, как дорогостоящее сооружение, может отсутствовать, представляется целесообразным рассмотреть возможность применения метода декомпозиции для оценки радиояркостных температур и радиояркостного контраста отдельных разрешаемых элементов объекта в ближней и промежуточной зонах антенны.

Целью данной статьи является развитие метода декомпозиции при формировании радиометрических изображений объектов в ближней и промежуточной зонах антенны.

1. ХАРАКТЕРИСТИКИ РАДИОМЕТРИЧЕСКОГО ИЗМЕРИТЕЛЬНОГО КОМПЛЕКСА

Подробное описание радиометрического измерительного комплекса (РМИК) ММД (рис.2), функциональная схема которого показана на рис.3, приведено в работах [3, 4]. Технические характеристики РМ датчика ММД приведены в таблице 1.

Рис.3. Схема РМИК ММД

Таблица 1

Характеристики РМ датчика ММД

Длина волны	8,6 мм
Фокусирующая система – двухзеркальная антенна Кассегрена, диаметр	340 мм
Линейное разрешение на дальности: 25 м 10 м	 750 мм 300 мм
Тип РМ приемника	модуляционный, прямого усиления
Диапазон измеряемых температур	0 … 500 К
Флуктуационная чувствительность	0,077 К/с
Постоянная времени измерений	1 с, 0,1 с, 0,01 с
Погрешность измерения радиояркостной температуры	0,85 К
Вид выходной шкалы	линейная
Поляризация излучения	линейная, вертикальная (горизонтальная)

Опорно-поворотное устройство (ОПУ), на котором размещены антенна и высокочастотная часть радиометра, позволяет осуществлять обзор пространства в широком диапазоне углов: до $\pm 90°$ от направления на объект (по азимуту) и $\pm 60°$ от горизонта (по углу места).

Аналого-цифровой преобразователь (АЦП) обеспечивает оцифровку выходного сигнала РМ приемника в ПЭВМ, путем преобразования медленно меняющегося напряжения с аналогового выхода РМ в цифровую последовательность.

АЦП является многоканальным и допускает проведение одновременных измерений и обработки сигналов 8 каналов (датчиков). Количество уровней дискретизации входного сигнала в каждом из каналов 4096 (12 разрядов двоичного кода).

Блок управления и синхронизации задает режим работы ОПУ и обеспечивает синхронность работы поворотного устройства, АЦП и ПЭВМ в процессе получения РМ изображений.

Результаты съемки записываются на жесткий диск ПЭВМ в виде:

- текстового файла, содержащего таблицу значений (отсчетов) аналого-цифрового преобразователя;
- графического файла формата BMP;
- информационного текстового файла, описывающего условия проведения эксперимента.

Для снижения шумов АЦП применяется фильтрация результатов радиометрической съемки. При заданном размере окна фильтра вычисляется среднее значение (усреднение) или находится медианное значение (медианная фильтрация). Результат медианной фильтрации, с шириной сглаживающего окна 5, представлен в виде графика на рис.4, где кривая 1 – данные без обработки, кривая 2 – результат медианной фильтрации.

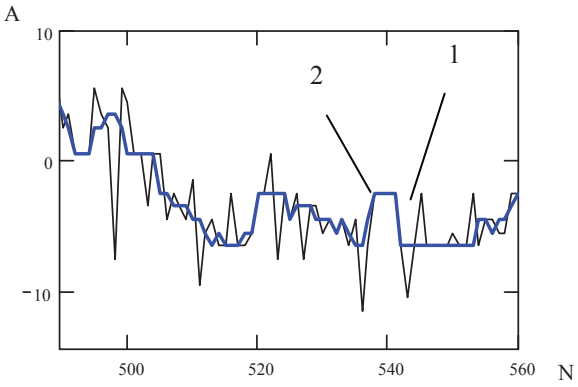


Рис.4. Результат медианной фильтрации шумов АЦП и радиометра

2. МЕТОДИКА ПРОВЕДЕНИЯ ИЗМЕРЕНИЙ

Методика проведения измерений поясняется на примере измерения коэффициента излучения радиопоглощающего материала (РПМ), предназначенного для маскировки объектов из металла в ММД.

Основным режимом формирования РМ изображений в ММД является режим автоматического управления положением опорно-поворотного устройства. В этом режиме осуществляется построчное сканирование луча ДНА радиометра в заданном секторе телесного угла с последующим формированием растровых полутоновых, либо цветных изображений на экране дисплея ПЭВМ. При этом сигнал с выхода аналогового канала радиометра поступает на АЦП управляющей ЭВМ, а получаемые данные регистрируются в памяти ПЭВМ в виде относительных двоичных отсчетов (уровней сигнала) для каждой точки изображения.

Предусмотрен также режим ручного управления положением поворотного устройства. В этом случае наведение и позиционирование луча ДНА радиометра на требуемый участок объекта осуществляет оператор путем нажатия клавиш на блоке управления и контроля процесса наведения посредством оптического визира.

Последовательность проведения измерений:

1. Установка динамического диапазона радиометра в пределах от температуры неба в зените до температуры имитатора абсолютно черного тела (АЧТ).
2. Установка антенны в первоначальное положение, например, под углом $\theta=35^0$ от надира.
3. Радиальное размещение в зоне обзора антенны плоского открытого металлического листа, металлического листа под РПМ, и имитатора АЧТ (см. рис. 5).
4. Проведение измерений в соответствии с нижеследующим алгоритмом.

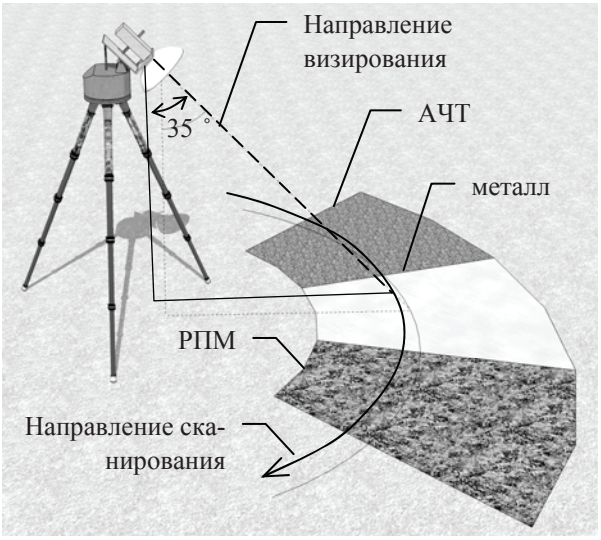


Рис. 5. Схема расположения тестовых образцов поверхностей в зоне сканирования антенны РМИК

Алгоритм измерения излучательной способности:

1. Сканирование исследуемых поверхностей с записью результатов измерения в память ПЭВМ.
2. Обработка результатов измерения на ПЭВМ:

а) разделение цифрового массива отсчетов АЦП на три части, соответствующие металлу, металлу под РПМ и имитатору АЧТ;

б) вычисление средних значений отсчетов АЦП для всех исследуемых материалов (см. рис.6);

в) вычисление коэффициента излучения РПМ.

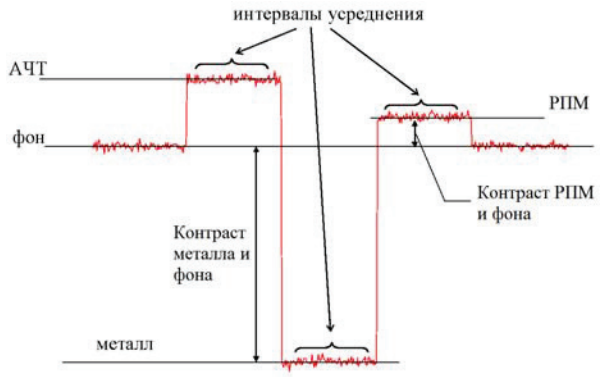


Рис. 6. Результаты оценки средних значений радиояркости и контрастов подстилающих поверхностей

Методика расчета коэффициента излучения РПМ. Методика расчета коэффициента излучения РПМ заключается в следующем:

1. Принятые допущения:

- ввиду малых расстояний от антенны до подстилающей поверхности (ближняя либо промежуточная зона антенны) затуханием в атмосфере пренебрегаем;
- полагаем, что металлический лист является зеркально отражающей поверхностью, а имитатор АЧТ и РПМ – диффузно рассеивают электромагнитные волны;
- радиояркостная температура неба, отраженная от диффузно рассеивающей поверхности, равна температуре неба при угле наблюдения $90° - \theta = 55°$.

2. Исходные данные для расчета:

T_H – радиояркостная температура неба при угле наблюдения 55° [5] $(T_H \approx 50\,K)$;

T_0 – температура подстилающей поверхности (измеряется термометром);

k_M – коэффициент излучения окрашенного металла $(k_M = 0{,}01)$;

$k_{АЧТ}$ – коэффициент излучения имитатора АЧТ $(k_{АЧТ} = 0{,}98)$;

A_M – среднее арифметическое отсчетов АЦП, соответствующих радиояркости металла (рассчитывается по результатам измерений);

$A_{АЧТ}$ – среднее арифметическое отсчетов АЦП, соответствующих радиояркости АЧТ (рассчитывается по результатам измерений);

$A_{РПМ}$ – среднее арифметическое отсчетов АЦП, соответствующих радиояркости РПМ (рассчитывается по результатам измерений).

3. Расчет радиояркостной температуры АЧТ и металла:

$$T_{АЧТ} = T_0 \cdot k_{АЧТ} + T_H (1 - k_{АЧТ}),$$
$$T_M = T_0 \cdot k_M + T_H (1 - k_M).$$

4. Расчет радиояркостной температуры РПМ:

$$T_{РПМ} = \frac{(A_{РПМ} - A_M) \cdot (T_{АЧТ} - T_M)}{A_{АЧТ} - A_M} + T_M .$$

5. Расчет коэффициента излучения РПМ:

$$k_{РПМ} = \frac{T_H - T_{РПМ}}{T_H - T_0}.$$

3. ОЦЕНКА СНИЖЕНИЯ РАДИОЯРКОСТНОГО КОНТРАСТА «ОБЪЕКТ – ФОН»

Известно, что излучательная способность фона (грунт, сухая трава) лежит в пределах $k_Ф = 0{,}85 - 0{,}95$.

Значение радиояркостной температуры фона находится по формуле:

$$T_Ф = T_0 \cdot k_Ф + T_H (1 - k_Ф).$$

Оценка снижения контраста «металл под РПМ – фон земной поверхности» производится по формуле:

$$R = \frac{|T_Ф - T_M|}{|T_Ф - T_{РПМ}|},$$

где R – коэффициент снижения радиояркостного контраста замаскированного объекта.

Оценка погрешности измерений. Относительная погрешность измерения контраста зависит от относительной погрешности измерения радиояркостных температур объекта и фона.

Оценим максимальную относительную погрешность измерения радиояркостной температуры.

Максимальные относительные погрешности измерения физических величин, по которым оценивается радиояркостная температура, таковы:

$$^{TM}T_0 = \frac{1}{600} = 0{,}167\%;$$

$$^{TM}k = \frac{1}{100} = 1\%;$$

$$^{TM}T_H = \frac{5}{280} = 1{,}79\%.$$

Полагая, что погрешности данных величин распределены по нормальному закону (максимальная погрешность в 2,7 раза больше среднеквадратической погрешности) и статистически независимы, получаем, что дисперсия оценки радиояркостной температуры в соответствии с разработанной методикой составит величину:

$$\sigma^2_{T_M} = \left(\frac{dT}{dk}\right)^2 \cdot \sigma^2_k + \left(\frac{dT}{dT_0}\right)^2 \cdot \sigma^2_{T_0} + \left(\frac{dT}{dT_H}\right)^2 \cdot \sigma^2_{T_H} =$$

$$= (T_0 - T_H)^2 \cdot \sigma^2_k + k \cdot \sigma^2_{T_0} + \sigma^2_{T_H}.$$

Подставляя в данное соотношение соответствующие значения погрешностей, получаем:

$$\sigma^2_{T_M} = (300-20)^2 \cdot 0{,}0037^2 + 0{,}98 \cdot 0{,}185^2 +$$

$$+1{,}85 = 2{,}957\,K\,.$$

Инструментальная погрешность радиометра известна: $\sigma^2_{T_{PM}} = 0{,}85\,K$.

Таким образом, среднеквадратическая погрешность измерения радиояркостной температуры составляет:

$$\sigma^2_T = \sqrt{\sigma^2_{T_M} + \sigma^2_{T_{PM}}} = \sqrt{2{,}957^2 + 0{,}85^2} = 3{,}077\,K\,.$$

Погрешность измерения радиояркостного контраста составляет: $\sigma^2_{\Delta T} = \sqrt{3{,}077^2 + 3{,}077^2} = 4{,}352\,K$.

При максимальном динамическом диапазоне принимаемого сигнала 280 K относительная среднеквадратическая погрешность измерения радиояркостного контраста составляет 1,554 %.

ВЫВОДЫ

На основе проведенного анализа известного метода декомпозиции, используемого для оценки радиолокационных характеристик объектов в ближней и промежуточной зонах антенны измерителя, предложено использование метода декомпозиции для оценки радиояркостных характеристик объектов сложной формы пассивными радиометрическими системами ММД. Показано, что метод декомпозиции и приведенная в работе методика измерения радиояркостной температуры материалов при помощи радиометрического измерительного комплекса ММД позволяют производить оценку снижения радиояркостного контраста объекта сложной формы на однородном фоне, за счет применения радиопоглощающего материала (покрытия).

Литература

[1] Патент на корисну модель № 115935. Переносний пристрій для вимірювання коефіцієнта відбиття. Колчигін М.М., Биков С.М., Биков В.М., Хардіков В.В., Демченко О.А., Іванченко Д.Д., Половніков Г.Г., Калугін Б.А. Зареєстровано в Державному реєстрі патентів України на корисні моделі 25.04.2017, Бюл. № 8. (19) UA (11) 115935 (51) МПК G01R 27/06(2006.01). Заявка U 2016 13621 від 30.12.2016. Рішення про видачу Патенту України від 25.04.2017 р. – 4 с.

[2] Патент на корисну модель № 119169. Спосіб вимірювання ефективної площі розсіяння великогабаритних об'єктів в ближній зоні. Колчигін М.М., Легенький М.М., Масловський О.А., Биков В.М., Субач Н.Є., Васильченко І.І., Биков С.М., Осіновий Г.Г., Бутрим О.Ю. Зареєстровано в Державному реєстрі патентів України на корисні моделі 11.09.2017, Бюл. № 17. (19) UA (11) 119169 (13)U МПК G01S 13\00. Заявка u 2017 03910 від 20.04.2017. Рішення про видачу патенту України від 11.09.2017 р. – 6 с.

[3] Матричные радиометрические корреляционно-экстремальные системы навигации летательных аппаратов: Монография [Текст] / В.И. Антюфеев, В.Н. Быков, А.М. Гричанюк, Д.Д. Иванченко, Н.Н. Колчигин, В.А. Краюшкин, А.М. Сотников. – Х.: Изд-во ООО «Щедрая усадьба плюс», 2014. – 372 с.

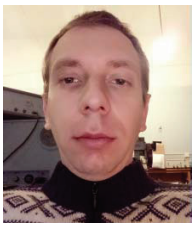
[4] A scanning measuring radiometry complex with computer control / V. Antyufeev, V. Bykov, A. Grichaniuk, D. Ivanchenko, V. Krayushkin / 2007 6th International Conference on Antenna Theory and Techniques, **IEEE Explore,** p. 486-488, **ISBN:** 978-1-4244-1584-7.

[5] Справочник по радиолокации. Под ред. М. Сколника, Нью-Йорк, 1970. Пер. с англ. (в 4-х томах). Том 4. Радиолокационные станции и системы. – М.: «Сов. радио», 1978. – 376 с.

Поступила в редколлегию 18.12.2017

Быков Виктор Николаевич, докт. техн. наук, с.н.с., ведущий научный сотрудник, профессор кафедры теоретической радиофизики, Харьковский национальный университет имени В.Н. Каразина, Харьков. Научные интересы: радиотеплолокация, системы навигации летательных аппаратов, дистанционное зондирование Земли, цифровая обработка изображений.

Быков Сергей Николаевич, научный сотрудник кафедры теоретической радиофизики, Харьковский национальный университет имени В.Н. Каразина. Научные интересы: системы навигации летательных аппаратов, дистанционное зондирование Земли.



Винниченко Сегрей Александрович, научный сотрудник кафедры теоретической радиофизики, Харьковский национальный университет имени В.Н. Каразина. Научные интересы: метрология, СВЧ измерения, радиотеплолокация.

Гричанюк Александр Михайлович, канд. техн. наук, научный сотрудник, Харьковский национальный университет Воздушных Сил имени Ивана Кожедуба. Научные интересы: радиотеплолокация, системы навигации летательных аппаратов, дистанционное зондирование Земли, цифровая обработка изображений.

Колчигин Николай Николаевич, докт. физ.-мат. наук, проф., заведующий кафедрой теоретической радиофизики, Харьковский национальный университет имени В.Н. Каразина. Научные интересы: исследование характеристик рассеяния электромагнитных волн на объектах сложной формы, взаимодействие сверхкоротких импульсов со сложными объектами, разработка и моделирование антенн для импульсных и широкополосных сигналов.

Осиновый Геннадий Геннадиевич, начальник проектного отдела, Государ-ственное предприятие «КБ «Южное», Днепропетровск. Научные интересы: исследование характеристик рассеяния электромагнитных волн на объектах сложной формы.

УДК 621.396.96

Розвиток методу декомпозиції при формуванні радіометричних зображень наземних об'єктів складної форми у ближній та проміжній зонах антени / В.М. Биков, С.М. Биков, С.О. Вінніченко, О.М. Грічанюк, М.М. Колчигін, Г.Г. Осіновий // Прикладна радіоелектроніка: наук.-техн. журнал. – 2017. – Том 16, № 3, 4. – С.106–111.

Запропоновано застосування відомого методу декомпозиції, який застосовується для вимірювання ефективної поверхні розсіяння об'єктів складної форми у ближній та проміжній зонах антени радіолокатора, для оцінки за допомогою радіометричного вимірювального комплексу міліметрового діапазону (ММД) інтегральної температури радіояскравості наземного об'єкта складної форми і формування його двовимірного радіометричного зображення. Наведено характеристики і методика вимірювання температури радіояскравості об'єктів сцени, що вивчається, за допомогою радіометричного вимірювального комплексу 8 мм діапазону у ближній та проміжній зонах антени. Наведено оцінку зниження контрасту радіояскравості «об'єкт–фон» за рахунок застосування радіопоглинаючого матеріалу.

Ключові слова: наземний об'єкт складної форми, радіометричний вимірювальний комплекс, міліметровий діапазон, радіопоглинаючий матеріал.

Табл.:01, Іл.:06, 05 найм.

UDC 621.396.96

Development of the decomposition method in the formation of radiometric images of terrestrial objects of irregular shape in the near and intermediate zones of an antenna / V.N. Bykov, S.N. Bykov, S.A. Vinnichenko, A.M. Grichaniuk, N.N. Kolchigin, G.G. Osinovy // Applied Radio Electronics: Sci. Journ. – 2017. – Vol. 16, № 3, 4. – P.106–111.

The application of the well-known decomposition method used to measure the effective surface of scattering of objects of irregular shape in the near and intermediate zones of a radar antenna is proposed for estimating the integral radar-brightness temperature of a terrestrial irregular shape object and formation of its 2-D radiometric image with the help of a radiometric measuring complex of the millimeter range (MMD). The characteristics and methods for measuring the radio brightness temperature of the objects of the studied scene are described using a radiometric measuring complex of 8 mm range in the near and intermediate zones of the antenna. An estimation of the reduction of the radio-contrast counterpoint "object-background" is made by using a radio absorbing material.

Keywords: terrestrial irregular shape object, radiometric measuring complex, millimeter range, radio absorbing material.

Tab.: 01, Fig.: 06, Ref.: 05 items.

УДК 621.391.629.7

РАЗРАБОТКА ВЫСОКОТОЧНОЙ СИСТЕМЫ ОПРЕДЕЛЕНИЯ ТРАЕКТОРИЙ КОСМИЧЕСКИХ АППАРАТОВ И ДРУГИХ ВЫСОКОДИНАМИЧНЫХ ОБЪЕКТОВ

А. А. ЖАЛИЛО, А. И. ДОХОВ, Е. В. КАТЮШИНА, Е. М. ВАСИЛЬЕВА, А. И. ЯКОВЧЕНКО, О. А. ЛУКЬЯНОВА

В статье представлены промежуточные итоги выполненных исследований и разработки высокоточной многопозиционной фазовой системы траекторных измерений (МФСТИ). В ходе работ выполнено обоснование реализуемости системы и проведена оценка достижимой точности определения траекторий космических аппаратов (КА) и приземных высокодинамичных летательных аппаратов. Представлено краткое описание построения и основных сегментов МФСТИ. Показано, что предложенный способ реализации системы позволяет достичь более высокой точности траекторных определений по сравнению с аналогами при минимальной стоимости разработки системы, её реализации и эксплуатации.

Ключевые слова: глобальная навигационная спутниковая система (ГНСС), ГНСС-технологии, космический аппарат (КА), летательный аппарат (ЛА), космический обьект (КО), многопозиционная фазовая система траекторных измерений (МФСТИ), высокодинамичные обьекты.

ВВЕДЕНИЕ

Анализ многочисленных открытых источников информации свидетельствует о том, что за рубежом проводились и проводятся активные работы по поиску новых технологий, способов и средств точного позиционирования, определения параметров движения высокодинамичных объектов, включая средства выведения и навигации/управления космических аппаратов (КА) на заданных околоземных орбитах. В частности, существует и особая сфера – сфера траекторных измерений для проведения летных испытаний и отработки автономных (инерциальных и др.) систем управления высокодинамичных летательных аппаратов (ЛА) специального назначения. История создания и развития высокоточных радиотехнических систем траекторных измерений восходит от систем MISTRAM, AZUSA (США), ВЕГА (СССР) [1, 2]. В США с конца 1970-х годов на смену указанным весьма дорогим и сложным системам разрабатываются более дешевые и мобильные траекторные системы, использующие технологии глобальных навигационных спутниковых систем (ГНСС). Так, для целей отработки систем управления межконтинентальных баллистических ракет морского базирования вводится в действие однопунктная корабельная система SATRACK, использующая ретранслированные с борта объекта одно- и двухчастотные сигналы GPS [3]. Непосредственное использование ГНСС-технологий и размещение соответствующих средств (полноценных спутниковых навигационных приемников) на борту контролируемых объектов (вместо ретрансляции спутниковых сигналов на пункт приема) также принципиально возможно и есть множество указаний на использовании ГНСС-приемников на борту высокодинамичных объектов в составе систем управления полётом, интегрированных со средствами инерциальной навигации, корреляционно-экстремальной навигации или астронавигации. Следует упомянуть и относительно новое развивающееся на Западе направление в технологиях точного позиционирования высокодинамичных объектов. Речь идет о многопозиционной наземной системе LOCATA (Австралия, США) [4], которая не использует сигналы ГНСС, но по принципу построения и функционирования соответствует выражению «GPS наоборот».

В Украине же в силу ряда объективных причин технологии в области траекторных измерений практически не развивались, хотя для космических приложений были осуществлены несколько проектов для низкоорбитальных КА. В настоящее же время возрастает актуальность и потребность создания эффективных высокоточных средств траекторных измерений для перспективных специализированных КА Украины [5] при их выведении и для навигации практически на всех околоземных орбитах с высотами до 36 тыс. км, включая области разрывного навигационного ГНСС.

Поэтому задача создания и исследования отечественной системы и технологий точных определений параметров движения КА и других высокодинамичных объектов, средств их независимого траекторного контроля в ходе летных испытаний является актуальной. Выполняемая в настоящее время в ХНУРЭ разработка высокоточной многопозиционной фазовой системы траекторных измерений (МФСТИ) отвечает этому направлению.

1. ПРИНЦИПЫ ПОСТРОЕНИЯ И ФУНКЦИОНИРОВАНИЯ МФСТИ

Для решения задачи создания МФСТИ с максимально возможными точностными характеристиками авторы предложили новую концепцию построения и функционирования системы, основанную на измерении необходимой совокупности параметров с помощью распределенного в пространстве радиотехнического комплекса, состоящего из подвижного бортового сегмента контролируемых объектов (КО) и наземного сегмента, которые образуют единую систему. Под-

вижной бортовой сегмент КО – бортовой приёмопередатчик/ретранслятор решает задачу приема широкополосных ГНСС-подобных трёхчастотных радиосигналов, передаваемых наземным передатчиком, их преобразования и излучения (с известным смещением частот для исключения интерференции) в дециметровом диапазоне волн в направлении сети наземных универсальных модифицированных приемников сигналов ЛА и сигналов ГНСС, образующие многопозиционный интерферометр. Одна из важнейших особенностей подхода к созданию МФСТИ заключается в достижении надежного разрешения фазовой неоднозначности разностей фазовых наблюдений наземных приемников сигналов высокодинамичных КО и одновременно сигналов ГНСС с сантиметровой точностью. В таком случае погрешности оценивания направляющих косинусов КО (аналогов измерений углов – азимута и угла места) будут соответствовать заданным характеристикам на максимальных отдалениях КО от измерительных пунктов системы. Такая задача является новой, а подход к ее решению базируется на использовании разработанных авторами проекта новых методов и идей, которые прошли апробацию в ходе предыдущих исследований.

Концепция построения МФСТИ заключается в совместном использовании: 1) принципов построения и функционирования полигонных многопозиционных фазометрических систем типа MISTRAM, AZUSA (США), ВЕГА (СССР), 2) сигналов и технологий (модифицированных аппаратных и программно-математических решений) глобальных навигационных спутниковых систем (ГНСС), 3) сигналов и технологий SBAS (системы типа EGNOS (ЕС), WAAS (США)) – региональных широкозонных функциональных космических и наземных дополнений ГНСС. Концепцию построения и функционирования МФСТИ определения параметров движения и навигации КА отражает рис. 1.

Разрабатываемая система включает наземный сегмент и бортовой приёмопередатчик/ретранслятор ГНСС-подобных сложных фазоманипулированных сигналов на трех разнесенных на ~350–400 МГц несущих частотах в дециметровом диапазоне волн (~1,7-2,1 ГГц). Наземный сегмент включает:

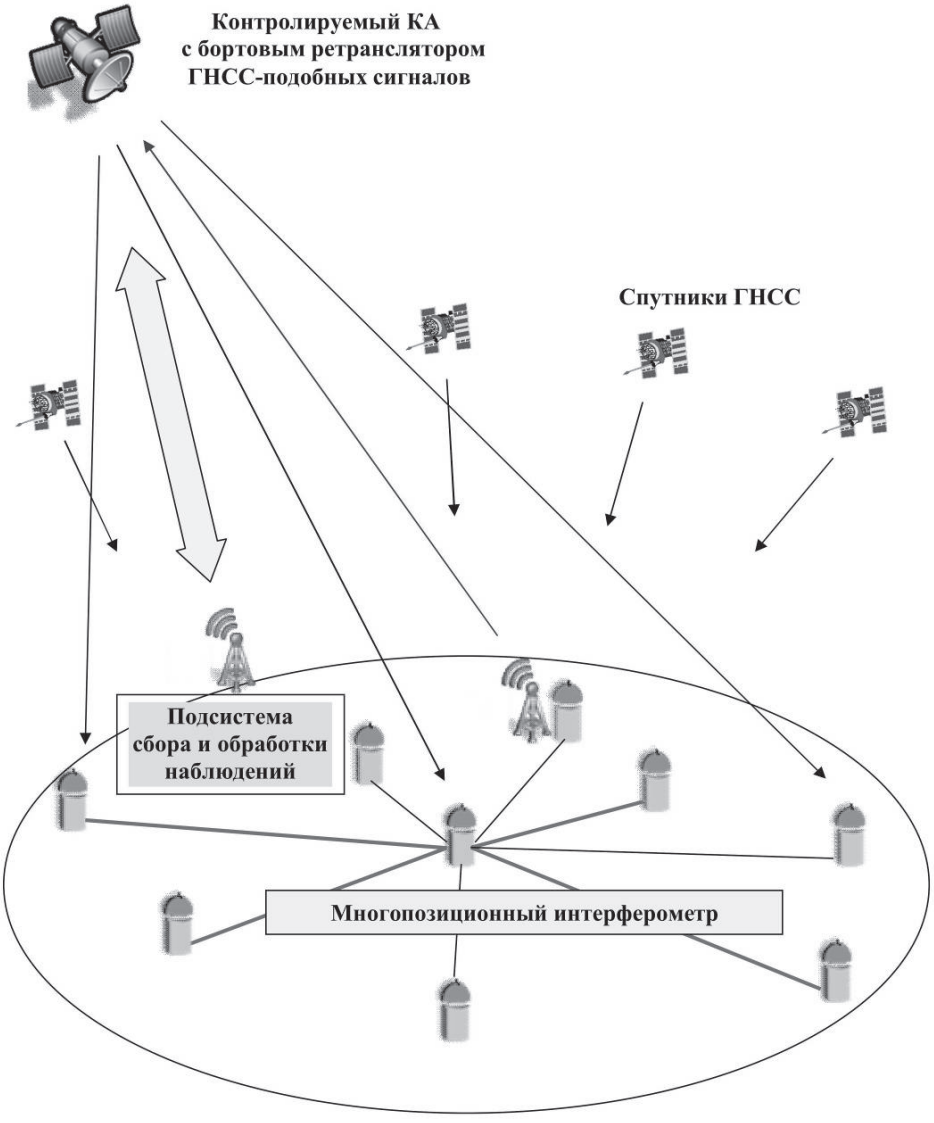


Рис. 1. Построение МФСТИ

а) передатчик измерительных/навигационных ГНСС/GPS-подобных сигналов (по типу SBAS) – дальномерный тракт;

б) многопозиционный фазовый интерферометр – разнесенные однотипные многоканальные специализированные приемники, принимающие и обрабатывающие сигналы ГНСС (для высокоточной координатной привязки фазовых центров приемных антенн и прецизионной синхронизации шкал времени приемников), и одновременно принимающие и обрабатывающие сигналы от наблюдаемых КО (L и S диапазонов), ретранслированных бортовыми приемопередатчиками КО;

в) центр сбора и обработки наблюдений МФСТИ.

В случае проведения измерений параметров движения КА, при необходимости, МФСТИ может быть на информационном уровне объеденена с телеметрической станцией для передачи на борт КА сигналов управления движением, формируемых на основе результатов траекторных/навигационных определений.

Измеряемыми параметрами являются кодовые и фазовые наблюдения петлевой дальности на трассах «наземный передатчик – КО – приемники» и фазовые наблюдения разностей псевдодальностей на трассах «КО – разнесенные в пространстве приемники». Приемники сигналов ГНСС и контролируемых объектов должны образовывать интерферометр (с примерно перпендикулярными базами) и дополнительные, меньшие по величине измерительные базы для целей более надежного разрешения фазовой неоднозначности. Максимальные базы интерферометра между разнесенными приемниками МФСТИ могут составлять от ~100 км до ~1200 км (для территории Украины) при определении параметров траекторий КА в ближнем и дальнем космосе.

Рассматриваемая универсальная система предполагает модульный принцип построения с возможностью оптимальной реконфигурации системы под конкретные задачи для определения параметров движения конкретных КА/ЛА с возможностью быстрого развертывания и ввода в эксплуатацию в заданном районе. Обмен измерительной информацией между элементами системы и центром сбора и обработки для целей прецизионной координатной привязки и синхронизации разнесенных приемных модулей осуществляется с использованием Интернет либо иных средств. Следует также отметить необходимость калибровки инструментальных задержек в измерительных трактах аппаратуры МФСТИ и смещений фазовых центров антенн, т. к. в фазометрической системе учёт систематических погрешностей измерений является принципиально важным.

Предложенный принцип построения системы позволяет достичь наибольшей точности определения параметров траектории объекта, даже если расстояния до него существенно превышают размеры измерительных базисов, при условии, что измерения дальности осуществляются с метровым уровнем точности, а измерения направляющих косинусов – с уровнем точности $\sim 10^{-6} \div 10^{-8}$. В этом случае погрешности определения текущих координат КА будут лежать в пределах ~0,1 м – 1,0 м при определении параметров движения на удалениях от ~200 км до ~40 тыс. км. В случаях, когда размеры измерительных базисов МФСТИ будут соизмеримы с расстояниями до КО, без значимой потери точности могут использоваться только высокоточные интерферометрические измерения разностей расстояний (без использования кодовых измерений петлевых дальностей). В этом случае бортовая аппаратура КО может работать в режиме «свистка» без запроса от наземного передатчика, что будет соответствовать схеме «GPS наоборот».

Отличительная особенность построения и функционирования разрабатываемой бортовой аппаратуры (БА) состоят в том, что она должна принимать один запросный сигнал от одного наземного передатчика, а излучать в направлении приемных пунктов три когерентных между собой ГНСС-подобных сигнала (должна соблюдаться и кодово-фазовая когерентность) на разнесенных частотах с одной и той же модулирующей псевдослучайной последовательностью (ПСП) – одним и тем же кодом, как в глобальной навигационной спутниковой системе ГЛОНАСС. Такая схема построения БА позволяет выполнять траекторные определения параметров движения нескольких объектов одновременно. БА каждого из контролируемых объектов должна излучать «ответы» (три указанных выше сигнала) на одних и тех же частотах для экономии частотного ресурса. БА каждого из одновременно контролируемых объектов должна осуществлять кодирование трех ответных фазоманипулированных ГНСС-подобных сигналов псевдослучайными ортогональными последовательностями (ПСП, кодами), уникальными для БА каждого из контролируемых объектов. Кодовое разделение сигналов дает возможность в наземных приемниках осуществить различение (идентификацию) и раздельную оценку параметров принимаемых сигналов в блоках цифровой обработки, сэкономить частотные ресурсы и применить при разработке приемников хорошо отработанные технологии приема и обработки ГНСС-сигналов. Для случая космических приложений на КА допустимо предположение о возможности установки двух антенн – принимающей запросный сигнал и передающей ответные сигналы.

Наземные приемники должны разрабатываться с учетом одного и того же принципа/технологии одновременного приема и обработки как сигналов ГНСС, так и сигналов от контролируемых объектов. Использование при создании МФСТИ уже наработанных и апробированных ГНСС-технологий как в аппаратной части, так и в части программно-математического обеспечения – это одно из ключевых преимуществ предложенного принципа построения МФСТИ в це-

лом, приводящее к весьма значительному удешевлению и сокращению сроков разработки системы.

2. РЕЗУЛЬТАТЫ АПРИОРНОЙ ОЦЕНКИ ТОЧНОСТИ ОПРЕДЕЛЕНИЯ ПАРАМЕТРОВ ДВИЖЕНИЯ КА И ДРУГИХ ВЫСОКОДИНАМИЧНЫХ ОБЪЕКТОВ

С использованием разработанных модели погрешностей наблюдений и алгоритмов априорной оценки точности (АОТ) МФСТИ получены оценки ожидаемой точности КА и других высокодинамичных объектов для различных вариантов построения и функционирования системы. Априорная оценка точности определения параметров движения КА проведена для низких, средних и высоких орбит. При этом использовались различные конфигурации МФСТИ с максимальными базовыми расстояниями от ~700 км до ~1100 км. Ниже представлены итоговые обобщенные результаты АОТ траекторных определений КА и приземных высокодинамичных ЛА.

Оценочные значения среднеквадратических погрешностей определения параметров движения КА находятся в пределах:

– от несколько сантиметров до ~20÷30 сантиметров по координатам и от нескольких миллиметров в секунду до ~2÷3 сантиметров в секунду – для низкоорбитальных КА на высотах до ~1000 км);

– от ~0,25÷0,6 м (в плане) до ~0,4÷1,2 м (по высоте) по координатам и от ~2÷4 см/с (в плане) до 3,6÷18 см/с (по высоте) по составляющим вектора скорости – для среднеорбитальных и геостационарных/геосинхронных КА (на высотах ~19÷36 тыс. км).

Оценочные значения среднеквадратических погрешностей определения параметров движения приземных (до высот ~150÷200 км) высокодинамичных ЛА находятся в пределах ~0,05÷0,40 м по координатам и ~0,5÷1,6 см/с по составляющим вектора скорости.

Предложенная концепция МФСТИ и рассмотренные пути реализации системы, как показали исследования, позволит достичь более высокой по сравнению с аналогами точности определений параметров траекторий летательных и космических аппаратов на любых высотах в диапазоне до 36 тыс. км при минимальной стоимости разработки системы, её реализации и эксплуатации.

3. ОСНОВНЫЕ РЕЗУЛЬТАТЫ ОЦЕНКИ ВОЗМОЖНОСТИ РЕАЛИЗАЦИИ МФСТИ

1. Проведенные расчеты показали, что при принятых исходных данных требуемые энергетические соотношения радиолиний МФСТИ полностью удовлетворяются и обеспечивают работоспособность системы.

2. Предложенная универсальная структурная схема бортовой аппаратуры подтвердила возможность её технической реализации, необходимой для выполнения задач МФСТИ. Предлагаемая аппаратура позволяет обеспечить необходимый уровень выходной мощности передатчика, заданную чувствительность приемного устройства, необходимую полосу слежения с учетом доплеровского сдвига частоты принимаемого сигнала.

Показана возможность технической реализации разрабатываемой наземной аппаратуры, необходимой для выполнения задач МФСТИ. Представлены основные принципы построения и функционирования разрабатываемой наземной аппаратуры МФСТИ.

3. Представлены результаты предварительной проработки структуры программно-математического обеспечения МФСТИ для совместной обработки наблюдений параметров сигналов от контролируемых объектов и сигналов ГНСС и определения параметров движения (координат и составляющих вектора скорости) контролируемых объектов в условиях высокой динамики изменения параметров принимаемых сигналов.

4. Определены этапы разработки МФСТИ, произведена оценка ориентировочной стоимости ОКР (~2,2 млн. у.е.), сроков её выполнения (~2,5 года) и стоимости изготовления комплекта образца системы при мелкосерийном производстве. Оценочная стоимость одного комплекта серийного образца МФСТИ составляет ~140,0÷160,0 тыс. у.е. в зависимости от предназначения и исполнения системы. Предложен состав кооперации организаций Украины для выполнения ОКР.

ВЫВОДЫ

1. Предложена новая концепция построения траекторной измерительной системы (МФСТИ) на основе сочетания принципов построения многопозиционных фазометрических систем и современных ГНСС-технологий точного позиционирования.

2. Определены архитектура и принципы функционирования сегментов МФСТИ, которая предполагает модульный принцип построения с возможностью оптимальной реконфигурации под конкретные задачи с возможностью быстрого развертывания и ввода в эксплуатацию в заданном районе.

3. МФСТИ является альтернативой всем рассмотренным аналогам траекторных измерительных систем (бортовые навигационные приемники GPS (ГНСС), система SATRACK, система LOCATA), обладает высокой точностью, соответствует современным передовым зарубежным технологическим решениям или даже превосходит их. Для КА, движущихся на средних и высоких орбитах, когда определение параметров движения по сигналам ГНСС затруднено или невозможно из-за разрывности навигационного поля, МФСТИ может стать единственной системой, обеспечивающей определение параметров движения КА с заданной точностью.

4. Определены этапы разработки МФСТИ, произведена оценка ориентировочной стоимости ОКР, сроков её выполнения и стоимости изготовления комплекта образца системы.

Литература

[1] Range Instrumentation, Ernest H. Ehling, Published by Prentice-Hall, Englewood Cliffs, N.J., 1967, 634 pp.

[2] *Литус Ю.П., Малафеев Е.Е., Михайлов Ю.В.* Высокоточная многопараметрическая система внешнетраекторных измерений параметров движения летательных аппаратов «ВЕГА» // Прикладная радиоэлектроника. – 2006. – Том 5, № 4.– С. 448–453.

[3] *Thompson T., Levy L.J., Westerfield E.E.* The SATRACK System: Development and Applications // Johns Hopkins APL TECHNICAL DIGEST, Volume 19, Number 4 (1998), pp.436-447.

[4] Craig Desiree L. LOCATA Corporation. USAF's New Reference System. Truth on the Range // Inside GNSS, № 3, May/June 2012, pp. 37-48.

[5] *Зайцева А.Ю., Маслей В.Н., Галабурда Д.А., Белоусов К.Г., Москалев С.И., Зайцев С.С., Шовкопляс Ю.А.* Электрореактивный буксир для межорбитальной транспортировки космических аппаратов // Космічна наука і технологія. 2015. – Т. 21, № 5.– С. 24–27.

Поступила в редколлегию 8.12.2017

Жалило Алексей Александрович, кандидат технических наук, ведущий научный сотрудник НИЦ ИИРЭСТ, ХНУРЭ. Область научных интересов: высокоточное позиционирование и навигация по сигналам ГНСС.

Дохов Александр Иванович, кандидат технических наук, профессор, заместитель проректора по научной работе ХНУРЭ. Область научных интересов: радиолокация, спутниковая навигация

Катюшина Елена Владимировна, старший научный сотрудник НИЦ ИИРЭСТ, ХНУРЭ. Область научных интересов: навигация с использованием сигналов ГНСС.

Васильева Елена Михайловна, кандидат технических наук, директор Центра электромагнитных измерений, Национальный научный центр «Институт метрологии». Область научных интересов: радиотехника, приборы и устройства СВЧ-диапазона, радиолокация.

Яковченко Александр Иванович, старший научный сотрудник НИЦ ИИРЭСТ, ХНУРЭ. Область научных интересов: высокоточное позиционирование и навигация по сигналам ГНСС.

Лукьянова Ольга Алексеевна, научный сотрудник НИЦ ИИРЭСТ, ХНУРЭ. Область научных интересов: навигация с использованием сигналов ГНСС.

УДК 621.391.629.7

Розробка високоточної системи визначення траєкторій космічних апаратів та інших високодинамічних об'єктів / О.А. Жаліло, О.І. Дохов, О.В. Катюшина, О.М. Васильєва, О.І. Яковченко, О.О. Лук'янова // Прикладна радіоелектроніка: наук.-техн. журнал. – 2017. – Том 16, № 3, 4. – С. 112–116.

В статті наведено проміжні підсумки виконаних досліджень і розробки високоточної багатопозиційної фазової системи траєкторних вимірювань (БФСТВ). В ході робіт виконано обґрунтування можливості реалізації системи та проведено оцінку досяжної точності визначення траєкторій космічних апаратів (КА) і приземних високодинамічних літальних апаратів. Подано стислий опис побудови і основних сегментів БФСТВ. Показано, що запропонований спосіб реалізації системи дозволяє досягти більш високі точності траєкторних визначень порівняно з аналогами при мінімальній вартості розробки системи, її реалізації і експлуатації.

Ключові слова: глобальна навігаційна супутникова система (ГНСС), ГНСС-технології, космічний апарат (КА), літальний апарат (ЛА), космічний об'єкт (КО), багатопозиційна фазова система траєкторних вимірювань (БФСТВ), високодинамічні об'єкти.

Іл. 1. Бібліограф.: 05 найм.

UDC 621.391.629.7

Development of a high-precision system for determining trajectories of spacecraft and other high-dynamic objects / *Zhalilo A.A., Dokhov A.I., Katiushina E.V., Vasileva E.M., Yakovchenko A.I., Lukyanova O.A.* // Applied Radio Electronics: Sci. Journ. – 2017. – Vol. 16, № 3, 4. – P. 112–116.

The paper contains preliminary results of the performed studies and the development of a high-precision multi-position phase system of trajectory measurements (MPSTM). In the course of the work the feasibility of the system was justified and an assessment of the achievable accuracy of determining the trajectories of space vehicles and near ground high-dynamic flying vehicles was made. A brief description of construction and main segments of the MPSTM is presented. The proposed method of the system realization allows achieving a higher accuracy of trajectory determinations in comparison with the analogues at a minimum cost of the system development, its implementation and operation.

Keywords: Global Navigation Satellite System (GNSS), GNSS-technologies, spacecraft, aircraft, space object, multi-position phase system of trajectory measurements (MPSTM), high-dynamic objects.

Fig. 1. Ref.: 05 items.

ФОРМИРОВАНИЕ И ОБРАБОТКА СИГНАЛОВ

UDK 519.6

ON THE ISSUE OF SOLVING THE PROBLEM OF ELECTROMAGNETIC COMPATIBILITY OF THE WIRELESS TELECOMMUNICATION SYSTEMS

O. A. SERKOV, G. I. CHURYUMOV

The main condition for ensuring electromagnetic compatibility in mobile communication systems is an increase in the signal-to-noise ratio. To implement this, methods are used that combine the dynamic change in transmitter power, the organization of multiple access and the dynamic allocation of communication channels. It is shown that the most effective and promising direction for solving this problem is the use of noise-like signals.

Keywords: telecommunications, electromagnetic compatibility, noise-like signal, wireless communication, mobile device.

INTRODUCTION

The main purpose of wireless telecommunication systems (WTS) is the quality of service (QoS) of a large number of consumers. Trends in the development of the WTS demonstrate both the continuous growth of mobile traffic and the information capacity of the entire system as a whole. Ensuring high-quality joint operation of such a great number of devices is a difficult task. At the same time, an increase in the number of connected mobile devices entails an increase in the requirements for the medium of information transfer.

It is well known that the quality of services provided to the consumer is determined by the requirements of electromagnetic compatibility (EMC) of the WTS, in particular, by the signal-to-noise ratio (S/N) P_s / P_n. In a case when the bandwidth ΔF is given, a value of this ratio contributes to the quality of the services provided to the consumer and determines the throughput of the communication channel, irrespective of the way the information is transmitted, i.e.

$$C = \Delta F \cdot \log_2\left(1 + \frac{P_s}{P_n}\right), \qquad (1)$$

where P_s is the power of the useful signal and P_n is the noise power. The value of C is customarily measured in bit per second.

The purpose of this paper is a determination of the conditions for ensuring EMC requirements in the WTS.

I. DESCRIPTION OF THE WAYS FOR INCREASING QOS

One of the ways to improve the criterion of the QoS is known to increase the power of the emitted signal while reducing the level of a noise (interference) and increasing the ratio S/N. However, as the power of the radiated signal increases in one of communication channels, the level of the noise in adjacent channels increases and, as a consequence, the ratio S/N decreases. On the other hand, as the signal power decreases, the information capacity of the WTS decreases and the number of consumers decreases. Moreover, to ensure high quality of the signal, it is necessary that the power of the received signal significantly exceeded background noise.

1. One of way to solve this problem is ***the method of dynamic change in transmitter power*** in the communication channel, depending on its state. Dynamic power control depends on the mobile device, and without considering the response of the base station, it continuously transmits the unmodulated pilot signal. This signal allows the mobile device to synchronize with the forward channel from the base station to the mobile device, which gives the reference phase for demodulation. It should also be used to monitor power. The mobile device monitors the power level of the received pilot signal and sets the transmitted power in the reverse channel from the mobile device to the base station, inversely proportional to the signal power. With this approach, the intensities of the signals in the forward and reverse communication channels are to be highly correlated. The circuit allows you to respond to fast signal intensity fluctuations. Such a fast response is required in the reverse link, where, with a random increase in the intensity of the received signal, all other signals can be suppressed at the base station. When controlling closed loop power, the signal strength in the reverse channel from the mobile device to the base station is equalized. This takes into account the characteristics of this reverse channel, such as the power level of the received signal, the signal-to-noise ratio or the frequency of the occurrence of erroneous bits in the received signal. The base station makes a power control decision and transmits the power control commands to the control channel of the mobile device. Closed-loop control is also used to equalize the power in the forward channel. In this case, the mobile device provides the base station with information about the quality of the received signal, and then the base station adjusts the transmitted power. In addition, the effects of reflection, diffraction and scattering can cause a rapid change in the levels of received

power, even at short distances. Due to different paths of propagation of radio waves (multipath propagation), interference of signals occurs, which creates a complex electromagnetic situation at the receiving site. The digital encoded signal comes in the form of several copies shifted in time. However, if the difference in the shift is greater than the duration of one pulse, the receiver is synchronized with the most powerful component of the received signal, while the rest are discarded. This ensures the resistance to multipath signal propagation.

2. An increase in the ratio S/N in the WTS is also possible due to the formation of the corresponding directivity diagrams of antenna systems [2]. Such an implementation is achieved by using ***the multiple access method***. For this, a request is made for the organization of a temporary communication channel. In this case, a circular pattern (CP) of the antenna system is used. Then the coordinates of the mobile device are determined. With the help of a digital antenna array (DAA), during a communication session, a highly directional CP is formed at the request source, increasing the ratio S/N by several orders of a magnitude. The conducted simulation showed the possibility of organizing with the help of the DAAs up to 8 simultaneously operating independent communication channels [3].

Fig. 1 shows the results of modelling the 12-element antenna array. At the same time, the coordinates of the interference sources are determined and they form CP with the minimum antenna directivity factor, making the ratio S/N in the given direction minimal.

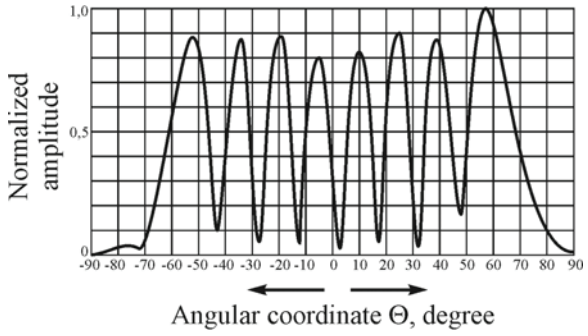


Fig. 1. Results of modelling

3. The air interface DECT (Digital European Cordless Telecommunications) is summoned to ensure the electromagnetic compatibility of equipment from different manufacturers. The base stations and subscriber terminals constantly scan all 120 available communication channels, while measuring the signal power in each of them. When establishing a new connection, the mobile device selects the channel with the lowest interference value. Thus, ***the method of dynamic channel allocation*** allows you to avoid frequency planning. Dynamic switching between channels is also possible during a communication session, since the mobile device continues to constantly analyze the level of noise (interference) in the available communication channels even when establishing a connection. Moreover, switching is possible both to another channel of the same base station and to another base station. An essential fact to ensure the requirements of EMC for the WTS is the low power of the emitted signal – from 10 to 250 mW. This allows you to locate the base stations in close proximity to one another, which allows you to achieve a record density of simultaneous connections (up to 10,000 Erl./km^2) with the most efficient use of the radio spectrum (500 Erl./MHz/km^2).

The physical limitations of the frequency resource and the need to improve the performance of communication channels in the transmission of information forces one to use complex signals that significantly improve the quality of information. Due to the fact that information is an ordered set of fixed symbols of an arbitrary nature, the theory of information should be considered as the mathematical basis of the theory of communication [3]. It is designed to address the challenges of improving the performance of communication systems. These are tasks of formalizing the description of information sources, their optimal coding, and also determining the maximum permissible bandwidth (1) of communication channels [4]. At the same time, information theory is designed to optimize communication systems as a whole by solving multicriterion problems taking into account mathematical models of various elements. Thus, it is possible to obtain high information transmission rates by creating superdense communication channels using signal-code structures for the transmission of information. They provide a data transfer rate close to the capacity of the communication channel (1).

4. One such practical solution is the use of ***noise-like (ultrawideband) signals***. These are signals in which the width of the spectrum is commensurable with the central frequency [5]. In this case, as it is shown in [6], the information is encoded by means of time-position-pulse modulation. The displacement of the pulse relative to its nominal position in the forward sequence sets "0", and backward "1". Moreover, the magnitude of the displacement should not exceed a quarter of the pulse duration. So, for example, in a sequence of pulses of 0.5 ns the duration with a pulse interval of 100 ns, the pulse that arrived 100 ps before is zero, and the one that arrives 100 ps later is a unit. One information bit is encoded by a sequence of many pulses, for example, 200 pulses per bit. As the encoding pulse, a Gaussian monocycle is used, which is described by the first derivative of the Gaussian distribution function

$$A(t) = A_0\sqrt{2e}\,\frac{t}{\Delta t}e^{-(t/\Delta t)^2}, \qquad (2)$$

where Δt is the pulse duration and A_0 is the amplitude of the pulse. The general view of the Gauss monocycle is shown in Fig. 2.

The shape of the power spectrum of such a pulse is described by the relation

$$S(\omega) = A_0\sqrt{2\pi e}\cdot\omega\cdot\Delta t^2\cdot t\cdot e^{-\left(\frac{\omega^2\cdot\Delta t^2}{2}\right)^2}, \qquad (3)$$

where ΔF is the width of the power spectrum of the pulse (Fig. 3). In this case, the base of the ultrashort pulse is $B = \Delta t \Delta F \approx 1$. So, for example, when using pulses of duration Δt from 2.0 ns to 0.1 ns, the bandwidth of the power spectrum is, respectively, from 500 MHz to 10 GHz, and the signal spectrum will occupy the frequency band from 0 to $\Delta F \approx 1/\Delta t$.

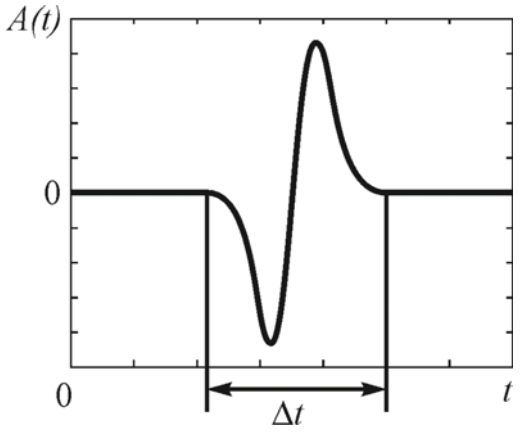


Fig. 2. Gauss monocycle shape

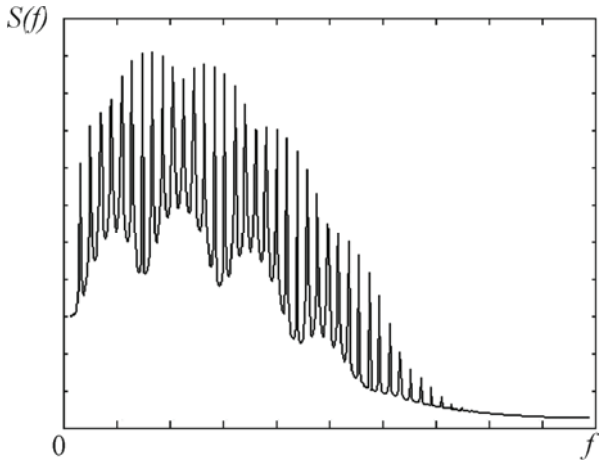


Fig. 3. Spectrum of the Gauss monocycle

To encode an information symbol, it is not single ultrashort pulse that is used, but their sequence. When using a sequence of ultrashort pulses, the signal base increases in proportion to their number. However, a regular sequence of such pulses does not carry any information. Its spectrum has a pronounced comb nature. Thus, such a signal can interfere with other radio engineering systems. To eliminate interference and organize independent channels in one frequency band, the position of each pulse is shifted by the time proportional to the current value of some pseudo-random sequence. In this case, the shift time is one or two orders of magnitude higher than the time shifting. As a result, the signal spectrum is substantially smoothed out, becomes noise-like and no longer interferes with other devices operating in the same band. Using a system of orthogonal codes to control the time delays of pulses, there are up to a thousand voice independent communication channels per base station created in one band without the use of special algorithms for digital signal processing [7]. Using orthogonal pseudorandom sequences-special codes for identifying connections form separate communication channels protected from interference are formed. Due to the fact that all channels are located in a singlewide frequency range, the signal becomes noise-like. To isolate from the general cacophony of radio signals, the part that is intended for the given receiver, it is necessary to assign a separate numerical code for each user. All other signals will be perceived as noise. Thus, in a single frequency band, several transceivers that do not interfere with each other can operate. Due to the broadband signal, its power is reduced with a very long base, below the white noise level. Logical channels are formed by spreading the signal spectrum with Walsh sequences. Each of these sequences is one of the rows of the Hadamard matrix. Their main property is that all rows of the matrix and their inversion are mutually orthogonal [7, 8]. For example, the Hadamard matrix of the second order has the form

$$A_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},$$

but of the fourth order

$$A_4 = \begin{bmatrix} A_2 & A_2 \\ A_2 & -A_2 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}.$$

For example, to extend the information flow, we use a 64-bit Walsh sequence. As a result, each information bit of the source stream corresponds to 128 output sequence chips. The gain in relation to s/i for the extended and original signal is 10 log 128 = 21 dB. Taking into account that the s/i ratio of 3 dB is acceptable at the receiver input, the transmission of information signals can be carried out at a signal level 18 dB below the level of interference disturbance.

Being synchronized with the transmitter and knowing the pseudo-random channel sequence, the correlator determines the deviation of the received pulses, forming at the output +1, if the signal, for example, came to 100 ps before the end of the interpulse interval, and -1 if it came to 100 ps is later and 0 otherwise. These values are accumulated in the integrator. As a result, narrowband interference from a transmitter with a continuous carrier or a signal from another impulse transmitter can prevent the reception of individual pulses, but not an information bit as a whole. The accumulated value of the correlator from random interference is 0. This allows you to avoid the interference of the signal that occurs when building communication within the premises and the conditions of complex terrain. The reflected signal enters the correlator with a delay and is perceived as a random interference, without affecting the direct signal in any way. Moreover, due to the broadband signal, its attenuation in various

media is rather small. Short pulses easily pass through various obstacles, since signal suppression does not occur throughout the entire range.

To evaluate noise immunity, the notion of increased processing should be used. In spread spectrum systems, processing gain is defined as the ratio of the channel bandwidth to the bandwidth of the information signal. Thus, for systems of spreading the spectrum by the method of direct sequence with a channel width of 5 MHz and an information signal of 10 kHz, the gain is 27 dB. For the same signal transmitted by a 2 GHz bandwidth, the gain is 53 dB. Thus, because of the high effective amplification of signals in noise-like systems, they can operate with a very low average transmitter power (50 mcW – 2 mW). Therefore, they do not interfere with existing radio systems, working with them in the same frequency range.

One of the most important elements for implementing noise-like technologies are powerful pulse keys. They must have commutation fronts with a duration of about 10-100 ps with a megahertz repetition rate and very high stability. In this case, the commutated voltage is measured in hundreds and thousands of volts. To implement the method, it is required to create generators capable of generating ultrashort pulses of nano- and picosecond duration and a repetition rate of up to tens of megahertz. Moreover, the temporal position of these pulses should be determined with an accuracy of at least 10 ps.

II. ANALYSIS

The analysis shows that at low power noise-like systems are able to transmit data inside buildings and objects with complex architectures. A characteristic feature inherent in communication systems based on ultra wideband (UWB) signals is the high electromagnetic compatibility of existing communication systems. Small signal levels, use of coding and noise-like structure of UWB systems practically do not interfere with other devices, which allows in most cases to work on a license-free basis. Expansion of the communication channel band and transition to channels with an ultra-wide band allows practically unlimited increase in the number of communication channels. While signals between subscribers, their frequencies and types of modulation being distributed beforehand, communication is realized between subscribers without mutual listening and mutual interference. At the same time, multi-channel but time-separated communication does not require an increase in transmitter power, while simultaneous transmission of different information to several subscribers requires an increase in this power or a reduction in the information transfer rate. Another advantage of this system in comparison with conventional narrow-band systems is their weak sensitivity to the distortions in conditions of multipath propagation of radio waves. For transmission in UWB systems, very short pulses are used, so there are no intersymbol distortions, since the energy of the received pulse practically always has time to completely die out before the next copy arrives. The most important criterion, characterizing the efficiency of wireless communication systems, is the high potential specific density of data transmission. It is defined as the value of the achievable total data transfer rate per square meter of the work area and has the dimension "bit/s/m^2", and according to the results obtained, the UWB systems have the highest value of this indicator today – about 1 Mbit/s/m^2.

III. CONCLUSIONS

Thus, the main way to ensure the requirements of electromagnetic compatibility in mobile communication systems is to increase the ratio S/N. The implementation of this direction is carried out through the use of methods of dynamic change in transmitter power, organization of multiple access and dynamic distribution of communication channels. However, the most effective and promising direction is the use of noise-like signals.

References

[1] *Knyazev A.D.* Elementy teorii i practiki obespecheniya electromagnitnoi sovmestimosti radioelektronnykh sredstv. –M.% Radio i svyaz', 1984. – 336 p.

[2] The Models and Methods of Assigning an Anchor in Unattended Telecommunication Systems on the Basis of the Form of Parallel Information Flows/ Nikitin S.O. // Dis. On the course. Candidate of science. Kharkiv. 2016.

[3] *Shannon K.* Works on Information Theory and Cybernetics.-M .: IL. – 1963. – 830 p.

[4] Development of Approaches to Creating the Theory of the Value of Information / Serkov AA, Logvinenko NF. // Bulletin of NTU "KhPI". Themes. Vyp .: Informatics and Modelling. - Kharkov: NTU "KhPI". – 2009.

[5] *Varganov ME, Zinoviev Yu.S., Astanin L.Yu. and others.* Radiocative Characteristics of Aircraft. M .: Radio and Communication, 1985.

[6] Ultra-wideband Communication. Second Birth? / Shakhnovich I.V. // Electronics: Science, Technology, Business No. 4. - 2001, pp. 8 – 15.

[7] Transmission of Information by Orthogonal Functions / Henning F. Harmuth / Springer-Verlag, Berlin Heidelberg New York 1970.

[8] *Vishnevsky VI, Lyakhov AI, Portnoy SL, Shakhnovich I.V.* Broadband Wireless Data Transmission Networks. M.: Technosphere, 2006. – 288p.

Manuscript received December, 18, 2017

Gennadiy I. Churyumov was born in the former U.S.S.R., in 1952. In 1974 and 1981, he received the Dipl.-Ing. degree in electronic engineering, the Ph.D. degree from Kharkiv Institute of Radio Electronics, Kharkiv, Ukraine, respectively, as well as the Doctor of Sc. degree from Institute of Radio Physics and Electronics of the National Academy of Sciences of Ukraine, in 1997. In 2002, he became a professor of Kharkiv National University of Radio Electronics, where he is now head of the Microwave & Optoelectronics Lab. He is a senior member of the IEEE and a member of the European Microwave Association. His general research interests

have been in the fields of the computer modeling of electromagnetic problems and nonlinear phenomena, microwave theory and technique and practical aspects of electromagnetic energy application.

Oleksandr A. Serkov is a Doctor of Science and Professor of the National Technical University “Kharkiv Polytechnic Institute”. Besides he is a Head of the Information Systems Department of the National Technical University "Kharkiv Polytechnic Institute", Honored Inventor of Ukraine. Scientific interests: durability and survivability of info communication systems in conditions of the action of powerful electromagnetic radiations; general theory and practice of ensuring the requirements of electromagnetic compatibility.

УДК 519.6

К вопросу решения проблемы электромагнитной совместимости беспроводных телекоммуникационных систем / А.А. Серков, Г.И. Чурюмов // Прикладная радиоэлектроника: науч. – техн. журнал. – 2017. – Том 16, № 3, 4. – С. 117 – 121.

Основным путем обеспечения требований электромагнитной совместимости в системах мобильной связи является повышение соотношения сигнал / шум. Реализация этого направления осуществляется за счет использования методов динамического изменения мощности передатчиков, организации множественного доступа и динамического распределения каналов связи. Показано, что наиболее эффективным и перспективным направлением является использование шумоподобных сигналов.

Ключевые слова: телекоммуникации, электромагнитная совместимость, шумоподобный сигнал, беспроводная связь, мобильное устройство.

Рис.: 3. Библиогр.: 8 назв.

УДК 519.6

До питання вирішення проблеми електромагнітної сумісності бездротових телекомунікаційних систем / О.А. Сєрков, Г.І. Чурюмов // Прикладна радіоелектроніка: наук. – техн. журнал. – 2017. – Том 16, № 3, 4. – С. 117 – 121.

Основним шляхом забезпечення вимог електромагнітної сумісності в системах мобільного зв'язку є підвищення співвідношення сигнал / шум. Реалізація цього напрямку здійснюється за рахунок використання методів динамічної зміни потужності передавачів, організації множинного доступу і динамічного розподілу каналів зв'язку. Показано, що найбільш ефективним і перспективним напрямком є використання шумоподібних сигналів.

Ключові слова: телекомунікації, електромагнітна сумісність, шумоподібний сигнал, бездротовий зв'язок, мобільний пристрій.

Іл.: 3. Бібліогр.: 8 найм.

ЭЛЕКТРОННАЯ ТЕХНИКА И ПРИБОРЫ

УДК 621.382.2.029.64

СЦЕНАРИЙ ПЕРЕХОДА К ХАОСУ ЧЕРЕЗ ПЕРЕМЕЖАЕМОСТЬ В ЛАВИННО-ГЕНЕРАТОРНЫХ ДИОДАХ МИКРОВОЛНОВОГО ДИАПАЗОНА

К. А. ЛУКИН, П. П. МАКСИМОВ

Впервые исследован сценарий перехода к хаосу через перемежаемость в лавинно-генераторном диоде (ЛГД) микроволнового диапазона. Основным управляющим параметром сценария является напряжение обратного смещения. Показано, что с увеличением напряжения в колебаниях уменьшаются участки с регулярными периодами и одновременно увеличиваются участки с нерегулярными периодами. Установлено, что максимальная ширина спектральных полос ЛГД может достигать 34 ГГц, а мощность автоколебаний – десятки ватт. Исследована устойчивость временных реализаций двух дискретизированных отсчетов лавинного тока с близкими начальными условиями на участках фазовых траекторий с регулярными и нерегулярными колебаниями.

Ключевые слова: лавинно-генераторные диоды, сценарий перехода к хаосу через перемежаемость, странный хаотический аттрактор.

ВВЕДЕНИЕ

Разработка диодных генераторов широкополосных и сверхширокополосных хаотических сигналов на основе методов хаотизации колебаний в полупроводниковых системах микроволнового диапазона является актуальной задачей современной электроники миллиметрового диапазона. Такие сигналы используются в современной шумовой радиолокации [1–4], а также в качестве носителей информации в системах скрытной связи [5,6]. Как известно, в этой области наиболее перспективным является лавинопролетный диод (ЛПД) [7,8], динамический хаос в которых изучался в работах [9,10]. Одним из важных этапов исследования диодных приборов генерирующих хаотических сигналов является изучение различных сценариев перехода к хаосу в динамических системах [11]. Например в [9,12] экспериментально получены хаотические колебания в генераторе на лавинно-пролетном диоде (ГЛПД) 8 мм диапазона длин волн и изучен переход к хаосу. Основным управляющим параметром в ГЛПД является ток через диод, который однозначно определяется напряжением обратного смещения на резком *p*–*n*-переходе [7,9]. Согласно [9] переход к хаосу в ГЛПД происходит следующим образом: по мере увеличения тока сначала начинает нарастать мощность колебаний, а затем в процесс включаются новые резонансы колебательной системы ГЛПД. При этом и паузы между возбуждаемыми цугами колебаний уменьшаются и практически исчезают. Спектр колебаний усложняется и становится непрерывным.

В работе [12] обнаружена хаотическая нестабильность токов в обратносмещенных *p*–*n*-структурах, а в [13,14] впервые представлена диффузионно-дрейфовая модель (ДДМ) лавинно-генераторных диодов (ЛГД) на основе обратносмещенных резких *p*–*n*-переходов. Установлено, что автоколебания в ЛГД определяются тремя основными параметрами: концентрацией акцепторов в *p*-области, концентрацией доноров в *n*-области и напряжением обратного смещения на *p*–*n*-переходе [13,14]. Временные и спектральные характеристики автоколебаний определяются только параметрами ЛГД – для генерации автоколебаний не требуется колебательный контур.

В работе авторов [15] исследованы режимы работы ЛГД с внешним сигналом и определены начальные условия, при которых диод работает в режиме генерации хаотических колебаний. Следуя результатам этой работы, исследуем сценарий перехода к хаосу через перемежаемость в ЛГД с внешним сигналом.

В настоящей работе выполнено численное моделирование различных режимов автоколебаний в ЛГД на основе обратносмещенных резких кремниевых *p*–*n*-переходов [13-15] при воздействии внешнего СВЧ сигнала с целью исследования сценария перехода к хаосу через перемежаемость регулярных и хаотических колебаний при изменении напряжения обратного смещения U/U_{av}.

1. ПОСТАНОВКА ЗАДАЧИ

На рис. 1 приведена одномерная модель обратносмещенного резкого *p*–*n*-перехода. За начало координат принята точка $x_2 = 0$ – граница раздела *p*- и *n*-областей. Координаты x_1 и x_3 – границы легирования акцепторной и донорной примесями соответственно. Координаты w_p и w_n – границы обедненных *p*- и *n*-областей *p*–*n*-перехода, J_{in} – входной сигнал. Исследуется Si ЛГД с однородным легированием *p*- и *n*-областей с плотностью акцепторной N_a и донорной N_d примесей, соответственно. В *p*–*n*-переходе статическая часть напряженности электрического поля E (без

учета влияния заряда подвижных носителей) изменяется по линейному закону, достигая максимального значения в точке x_2.

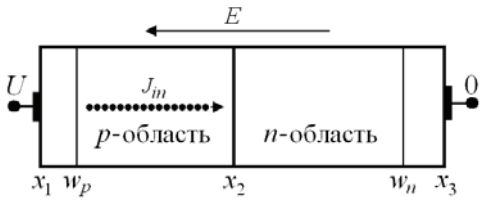


Рис. 1. Одномерная модель *p–n*-перехода с резкой границей раздела *p– и n*-областей
E – напряженность электрического поля,
U – напряжение обратного смещения

Математическая модель ЛГД базируется на системе дифференциальных уравнений в частных производных ДДМ полупроводниковых структур, содержащих резкие *p–n*-переходы [10]. Для численного интегрирования дифференциальные уравнения преобразовывались в систему конечно-разностных уравнений. Погрешность аппроксимации дифференциальных операторов разностными не превышает $O(\tau + h)$, где τ – шаг временной сетки и h – шаг пространственной сетки, удовлетворяющие условию устойчивости Куранта $\tau \le h / v$ (v – скорость носителей заряда).

Алгоритм решения конечно-разностных уравнений ДДМ [18-19] основан на модифицированном методе встречных прогонок [19], в котором введены и используются граничные условия для всех искомых величин на границе резкого *p–n*-перехода: $x_2 = 0$. В результате введения таких граничных условий степень легирования и другие параметры *p*- и *n*-областей полагаются однородными, и интегрирование может выполняться с постоянным шагом, что существенно улучшает эффективность метода. В результате решения уравнений этой модели получаем пространственно-временную реализацию $x_{n,m}$, состоящую из N последовательных временных и M пространственных отсчетов: $x(n\tau, mh)$, где $n = 0,\ldots, N\text{-}1$, $m = 0, \ldots M\text{-}1$. Общее число пространственно-временных отсчетов определяется произведением $N{\cdot}M$. Для удобства дальнейшего рассмотрения введена частота дискретизации $f_s = 1/\tau$. Шаг дискретизации на оси Фурье частот определяется длительностью полученной временной реализации и для быстрого преобразования Фурье (БПФ) будет определяться следующим образом: $df = 1/(\tau N) = f_S / N$.

Достоверность результатов основана на применении устойчивого алгоритма решения конечно-разностных уравнений ДДМ ЛГД и подтверждена согласованностью результатов тестовых задач с известными результатами [7].

В данной работе рассмотрены различные режимы генерации ЛГД при воздействии на него **внешнего** сигнала с безразмерной амплитудой A_{st} и частотой f и следующих значениях основных параметров: $\tau_{эф}$ = = 2,5мс, $N_a = 10^{17}$ см$^{-3}$, $N_d = 5{,}3\cdot10^{16}$ см$^{-3}$, $A_{st} = 0{,}05$ и f = = 0,6 ГГц, где $\tau_{эф}$ – время жизни неосновных носителей, N_a – концентрация акцепторов, N_d – концентрация доноров, U/U_{av} – безразмерное напряжение обратного смещения, U_{av} – статическое напряжение ударной ионизации.

2. ВОЛЬТАМПЕРНАЯ ХАРАКТЕРИСТИКА

Принцип действия ЛГД основан на обнаруженной ранее авторами [12–14] токовой неустойчивости в обратно-смещенном несимметричном *p–n*-переходе с ударной ионизацией. При этом вольтамперная характеристика (ВАХ) обладает участком с отрицательной дифференциальной проводимостью, если корректно учитывается влияние эффекта компенсации заряда примесных атомов зарядом подвижных носителей на напряженность электрического поля, и следовательно, коэффициент ударной ионизации [12–15].

На рис. 2 приведена типичная ВАХ в *n*-области обратносмещенного резкого Si *p–n*-перехода, заимствованная из работы [14]. На ВАХ условно можно выделить четыре характерных участка, два из которых существенно влияют на характеристики ЛГД. На нелинейном участке (*c–d*) заряд подвижных носителей сравним по величине с зарядом примесных атомов. Это приводит к уменьшению электрического поля вследствие нейтрализации заряда примесных атомов зарядом подвижных носителей, поэтому рост лавинного тока существенно замедляется. На участке (*d–e*) имеет место токовая неустойчивость, и зависимость протекающего тока от приложенного напряжения становится нестационарной, при этом на рис.2 условно показаны две ветви нестационарной плотности тока: ветвь (*d–e'*) показывает максимальныее, а (*d–e''*) – минимальные значения амплитуды плотности тока. На этом участке и наблюдается отрицательная дифференциальная проводимость *p–n*-перехода, которая обуславливает генерацию автоколебаний [12,14]. Из рис. 2 видно, что амплитуда автоколебаний увеличивается с повышением напряжения обратного смещения на диоде и при $U/U_{av} > 1{,}51$ наблюдается эффект гашения ударной ионизации, при котором объемный заряд подвижных носителей полностью нейтрализует объемный заряд примесных атомов. Эффект гашения может быть использован для генерации импульсных сигналов.

Следовательно, резкий Si *p–n*-переход в зависимости от напряжения обратного смещения может работать как в режиме усиления входного сигнала на устойчивом участке, так и в режиме генерации автоколебаний на участке с токовой неустойчивостью. В *p*-области *p–n*-перехода имеет место аналогичная ВАХ. В частности, наличие двух ВАХ в ЛГД обуславливает синхронную генерацию двух колебаний с разными частотами в *p*- и *n*-областях *p–n*-перехода, соответственно [16].

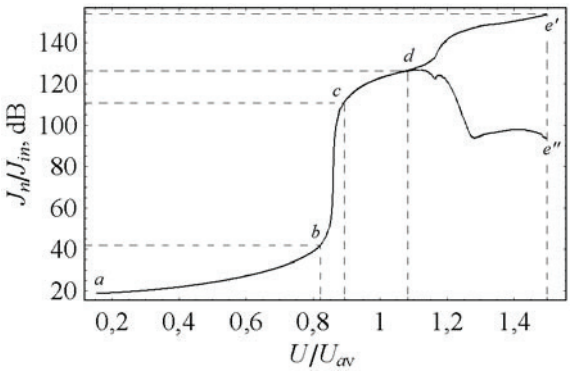


Рис. 2. Типичная вольтамперная характеристика ЛГД на основе обратносмещенного резкого Si *p–n*-перехода

3. ГЕНЕРАЦИЯ ХАОТИЧЕСКИХ КОЛЕБАНИЙ В ЛГД ПРИ РАЗЛИЧНЫХ НАПРЯЖЕНИЯХ СМЕЩЕНИЯ

В этом разделе приведены результаты численного интегрирования системы уравнений ДДМ ЛГД [17,18] при внешнем воздействии для различных значениий напряжения смещения, а также обнаружен и описан переход к генерации хаотических колебаний в неавтономном ГЛД через перемежаемость с ростом напряжения смещения. Рассчитанные зависимости мощности генерируемых колебаний и их спектральные характеристики представлены на рис.3–7.

На рис. 3, а приведена временная зависимость мощности $P(t)$ вынужденных колебаний в ЛГД под воздействием внешнего СВЧ сигнала с частотой $f = 0,6 ГГц$ (период колебаний $T = 1,667 нс$) при напряжении, превышающем напряжение лавинного пробоя в 1,1 раза ($\boldsymbol{U/U_{av}}$ **= 1,1)**. Видно, что в ЛГД устанавливаются периодические колебания с частотой близкой к частоте внешнего сигнала 0,64 ГГц и вариациями мгновенной мощности $P(t)$ в пределах 10 – 70 Вт. Регулярность этих колебаний обусловлена тем, что при данном напряжении обратного смещения компенсация заряда примесных атомов зарядом подвижных носителей недостаточна для появления токовой неустойчивости [12, 13] и, следовательно, для реализации автоколебательного режима. В отсутствие автоколебаний, изменение напряженности электрического поля во времени определяется только частотой внешнего сигнала. На рис. 3,б приведен Фурье-спектр $P(f)$ мощности генерируемых колебаний, который состоит только из спектральной линии входного сигнала на частоте 0,64 ГГц.

На рис. 4, а колебания мгновенной мощности $P(t)$ на временном отрезке (0…0,2) нс имеют короткий одиночный всплеск, обусловленный влиянием заряда подвижных носителей на напряженность электрического поля. Установившиеся колебания являются периодическими с периодом $T = 1,82$ нс ($f = 0,55 ГГц$), а максимальная мощность колебаний превышает 115 Вт.

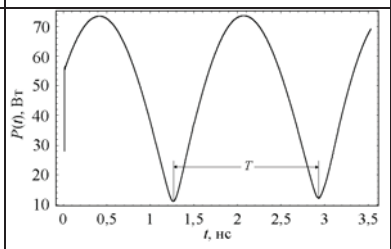
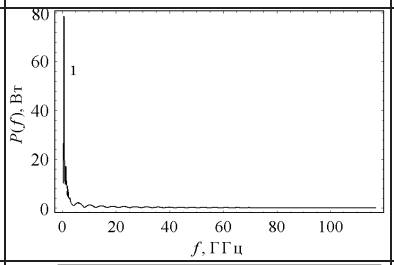
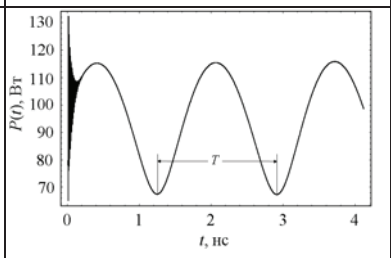
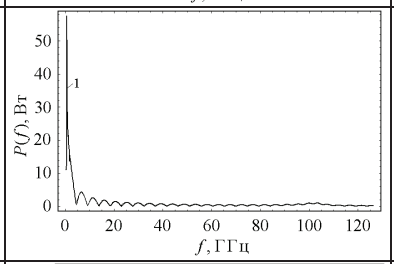
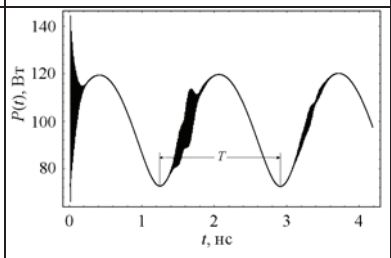
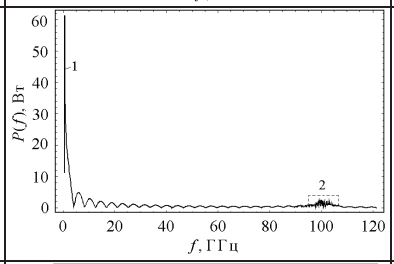
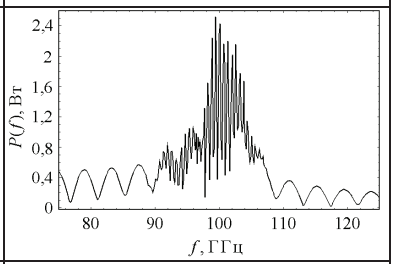
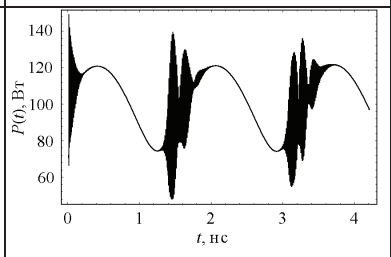
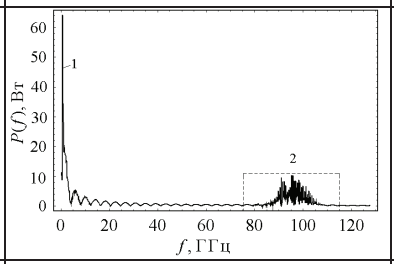
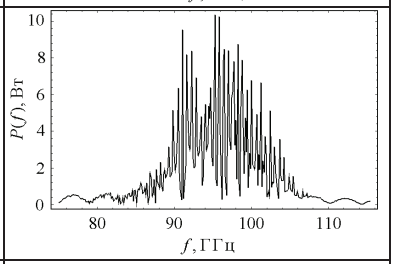
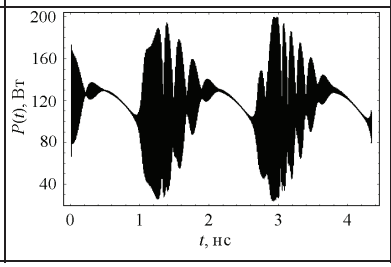
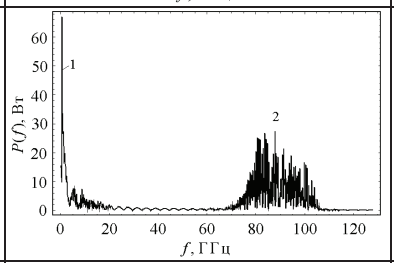
На рис. 4, б приведен Фурье-спектр $P(f)$ мощности колебаний, рассчитанный с временным шагом $\tau =$ = 51,5 фс. Спектр состоит из спектральной линии входного сигнала на частоте 0,55 *ГГц*, со спектральной плотностью мощности $P(f) =$ 58 *Вт/Гц*. Кроме того, на частотах 100 и 104 *ГГц* наблюдается незначительное увеличение амплитуды спектральных линий, появление которых связано с возбуждением автоколебаний электронной и дырочной компонент выходной $P(t)$ ЛГД благодаря токовой неустойчивости [12 – 14].

На рис. 5, а приведена временная зависимость мгновенной мощности $P(t)$ ЛГД. Внешний сигнал ЛГД имеет период колебаний 1,66 нс (f = 0,60 *ГГц*), максимальная амплитуда $P(t)$ достигает 120 Вт.

Видно, что увеличение напряжения обратного смещения приводит к появлению нерегулярных фрагментов на части периода регулярных колебаний выходной мощности $P(t)$, а именно на переднем фронте второго и третьего периодов. Эти нерегулярные фрагменты вызваны проявлением взимодействия сигнала внешнего воздействия с сигналами автоколебаний электронной и дырочной компонент тока ЛГД, которая увеличивается с ростом напряжения обратного смещения на *p–n*-переходе.

На рис. 5, б приведен Фурье-спектр выходной мощности ЛГД, $P(f)$, который состоит из спектральной линии 1 входного сигнала на частоте 0,68 ГГц и значением спектральной плотности мощности 61,4 Вт/Гц, а также непрерывного спектра в высокочастотной области, 2, автоколебаний ЛГД с основными частотами 99,43 и 100,12 ГГц и полосой частот ΔF порядка 6 ГГц (рис. 5, в).

На рис. 6, а представлена временная реализация мгновенной мощности $P(t)$ ЛГД при воздействии внешнего сигнала с частотой *0.602 ГГц* (период колебаний 1,66 *нс*). Видно, что $P(t)$ имеет периодические и непериодические участки, мощность которых усиливается с ростом напряжения обратного смещения. Размеры участков регулярных колебаний уменьшаются, а нерегулярных – увеличиваются. Такое изменение формы колебаний обусловлено увеличением связи между внешним сигналом и электронной и дырочной компонентами токов в *p–n*-переходе. На рис. 6, б приведен Фурье-спектр зависимости выходной мощности $P(f)$, который как и ранее состоит из отдельной спектральной линии, 1, на частоте близкой к частоте внешнего сигнала (0,68 ГГц), и сплошной полосы частот, 2, автоколебаний ЛГД с шириной порядка 19 ГГц (рис. 6,в). Из рис.7 видно, что увеличение напряжения обратного смещения до значения (U/U_{av} = = 1,7) приводит к усилению наблюдаемого эффекта стохастизации колебаний в рассматриваемом диоде: спектральная пдотность мощности и интегральная мощность увеличиваются, а ширина спетра мощности хаотических колебаний расширяется до 36 ГГц.

Нормированное напряжение обратного смещения	Временная реализация мощности $P(t)$ генерируемых колебаний. **а)**	Полный Фурье-спектр мощности $P(f)$ генерируемых колебаний. **б)**	Хаотическая часть Фурье-спектра мощности $P(f)$ генерируемых колебаний (2) **в)**
Рис. 3 U/U_{av} = 1,1			
Рис. 4 U/U_{av} = 1,54			
Рис. 5 U/U_{av}= 1,585			
Рис. 6 U/U_{av} = 1,6			
Рис. 7 U/U_{av} = 1,7			

4. ХАРАКТЕРИСТИКИ ЛГД ПРИ МАКСИМАЛЬНОМ НАПРЯЖЕНИИ ОБРАТНОГО СМЕЩЕНИЯ

При $U/U_{av} > 1{,}885$ в ЛГД происходит гашение ударной ионизации. На рис. 8 – 9 представлены временные и спектральные характеристики ЛГД в этом режиме. На рис. 8, а приведены колебания электронной $J_n(t)$ и дырочной $J_p(t)$ (*пунктирные линии*) компонент плотности полного тока $J(t)$ ЛГД. (Средний период автоколебаний $J(t)$ равен 8 пс.), а рис. 8, б – полный лавинный ток, полученный в результате суммирования электронной и дырочной компонент $J(t) = J_p(t) + J_n(t)$. Максимальная амплитуда колебаний получена при суммировании компонент $J_p(t)$ и $J_n(t)$ в фазе и достигает 58 кА/см^2, минимальная амплитуда колебаний – в противофазе и превышает 8 кА/см^2. Видно, что колебания лавинного тока $J(t)$ имеют нерегулярный характер, что может наблюдаться в режиме динамического хаоса в ЛГД.

Для подтверждения этого предположения был построен фазовый портрет изучаемой динамической системы для следующих интегральных переменных $U(t) = -\int_{w_p}^{w_n} E(x,t)dx$ – падение напряжения и $J(t) = \frac{1}{w}\int_0^w J(x,t)dx$ – плотностью лавинного тока –

усредненные по координате. На рис. 8, в приведен аттрактор установившихся колебаний в фазовой плоскости ЛГД. Направление движения фазовой точки показано стрелками. Видно, что амплитуда напряжения $U(t)$ изменяется в диапазоне 8…56 В, а дока $J(t)$ – в диапазоне 8…58 кА/см^2. Точками 2 и 3 отмечены участки аттрактора, в которых изменяется характер динамических процессов.

В окрестности точки 2 падение напряжения $U(t)$ максимально, скорость носителей заряда достаточна для ударной ионизации атомов, поэтому при движении изображающей точки на участке (2–3) наблюдаются генерации электронно-дырочных пар. В результате синхронно уменьшается падение напряжения $U(t)$ и увеличивается плотность лавинного тока $J(t)$.

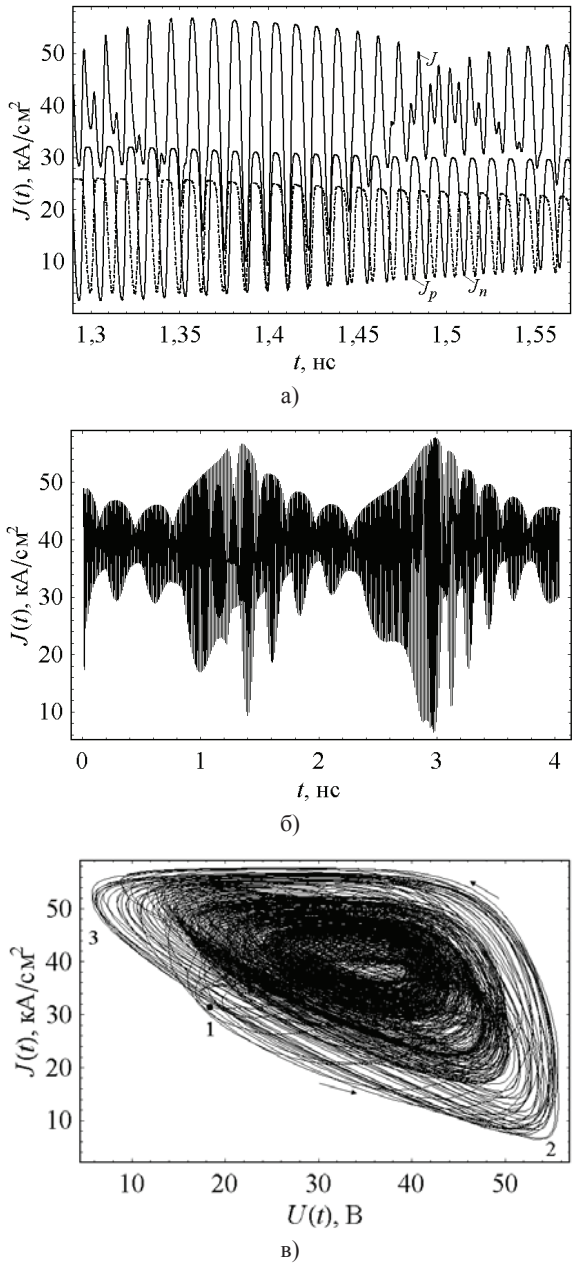


Рис. 8. Временная реализация полного лавинного тока $J(t)$ (а) и его компонент $J_p(t)$ и $J_n(t)$ (б) и странный хаотический аттрактор сверхширокополосного ЛГД (в)

В окрестности точки 3 падение напряжения $U(t)$ минимально, скорость носителей заряда недостаточна для ударной ионизации атомов, поэтому при движении изображающей точки на участке (3–2) синхронно наблюдается увеличение напряжения $U(t)$ и уменьшение плотности лавинного тока $J(t)$ вследствие ухода подвижных носителей на контакты p–n-перехода. Следовательно, при движении изображающей точки на участке (3–2) синхронно восстанавливаются исходные значения падения напряжения $U(t)$ и плотности лавинного тока $J(t)$.

Как известно странный хаотический аттрактор характеризуется неустойчивостью принадлежащих ему фазовых траекторий. Изучение устойчивости фазовых траекторий в рассматриваемой системе было выполнено с помощью метода возвратов Пуанкаре. Согласно этому методу возврат траектории в окрестность произвольно выбранной трансверсальной плоскости сечения Пуанкаре на ней называют возвратом Пуанкаре [11]. Для периодических колебаний траектория изображающей точки будет замкнутой и возвраты Пуанкаре будут повторяться, со сколь угодно высокой точностью. В то же время, для нерегулярных колебаний число различающихся возвратов увеличивается, и интервал времени между двумя последовательными возвратами Пуанкаре оказывается каждый раз другим, так что можно ввести статистическое распределение времен возврата. Такая статистика возвратов Пуанкаре характерна для динамического хаоса фазовых траекторий динамической системы [11].

На рис. 9, а показана временная реализация мгновенной мощности $P(t)$ ЛГД. Средний период колебаний $P(t)$ определяется периодом внешнего сигнала и равен 1,7 нс. Предельная величина напряжения обратного смещения приводит к росту амплитуды нерегулярных колебаний до 280 Вт. Такое изменение амплитуды мгновенной мощности обусловлено увеличением лавинного тока и напряжения обратного смещения. Это приводит к повышению компенсации заряда примесных атомов зарядом подвижных носителей. В результате напряженность электрического поля снижается, а связь между внешним сигналом, электронной и дырочной компонентами выходной мощности $P(t)$ повышается.

На рис. 9, б приведен Фурье-спектр выходной мощности ЛГД, который состоит из спектральной линии 1 внешнего сигнала с частотой 0,6 ГГц и хаотической составляющей колебаний со спектральной плотностью мощности 69,6 Вт/Гц и шириной спектра частот $\Delta F > 30$ ГГц .

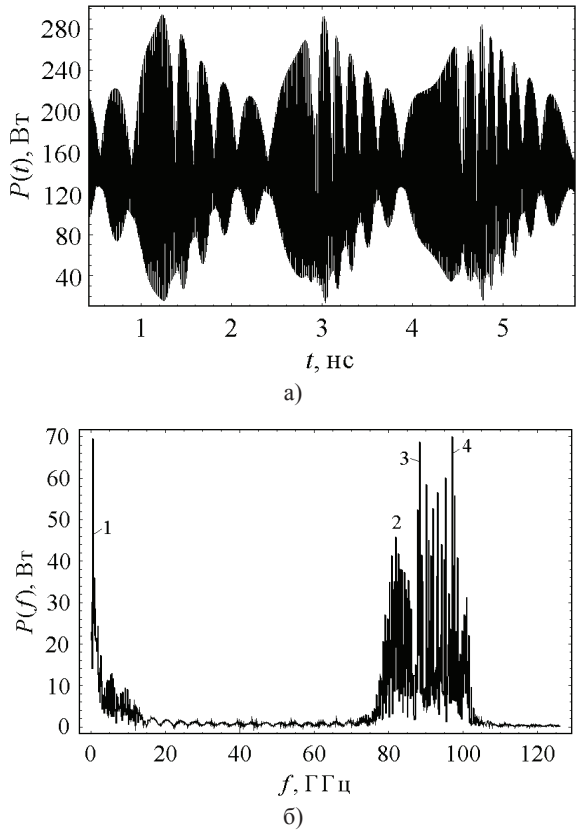


Рис. 9. Временная реализация выходной мощности $P(t)$ при напряжении U/U_{av} = 1,885 (а) и Фурье-спектр выходной мощности ЛГД (б)

ВЫВОДЫ

Исследован сценарий перехода к хаосу через перемежаемость регулярных и нерегулярных колебаний в ЛГД с внешним воздействием на всем участке ВАХ с токовой неустойчивостью (U/U_{av} = 1,585 – 1,885 В, $N_a = 10^{17}$ см$^{-3}$, $N_d = 5{,}3\cdot10^{16}$ см$^{-3}$). Показано, что в ЛГД при увеличении напряжения обратного смещения имеет место сценарий перехода к хаосу через перемежаемость регулярных и нерегулярных колебаний. Переход к хаосу происходит следующим образом. По мере увеличения напряжения обратного смещения $U/U_{av} \geq$ 1,585 начинает нарастать амплитуда спектральных линий, увеличивается ширина спектральных полос и число дополнительных частот. При напряжении обратного смещения свыше $U/U_{av} >$ 1,645 ширина спектральных полос и число частот практически не изменяются, а мощность спектральных линий продолжает увеличиваться до тех пор, пока напряжение обратного смещения не достигнет напряжения $U/U_{av} >$ 1,885. Форма колебаний усложняется, фазовые траектории становятся неустойчивыми, и такое состояние ЛГД характеризуется странным аттрактором в фазовом пространстве его интегральных переменных.

Литература

[1] *Lukin K. Noise Radar Technology* / Telecommunications and Radio Engineering, 2001. – V. 55, # 12. – pp. 8–16.

[2] *Лукин К. А.* Шумовая радиолокация милиметрового диапазона / К. А. Лукин // – Харьков: Ин-т радиофизики и электрон. НАН Украины. – 2008. – 13, спец. вып. С. 344–358.

[3] *Lukin K.A.* 'The principles of noise radar technology'. Proc. NRTW-2002, Yalta, Crimea, Ukraine, 18–20 September 2002, pp. 13–22

[4] *Lukin K.A.* 'Noise radar technology: the principles and short overview', Appl. Radio Electron., 2005, 4, (1), pp. 4–13.

[5] *Дмитриев А. С.* Динамический хаос: новые носители информации для систем связи / А. С. Дмитриев, А. И. Панас. – М.: Физматлит, 2002. – 252 с.

[6] *Залогин Н. Н.* Широкополосные хаотические сигналы в радиотехнических и информационных системах / Н. Н. Залогин, В. В. Кислов. – М.: Радиотехника, 2006. – 208 с.

[7] *Тагер А. С.* Лавинно-пролетные диоды и их применение в технике СВЧ / А. С. Тагер, В. М. Вальд-Перлов.– М.: Сов. радио, 1968. – 480 с

[8] *Касаткин Л. В.* Полупроводниковые устройства диапазона миллиметровых волн / Л. В. Касаткин, В. Е. Чайка – Севастополь: Вебер, 2006. – 319 с.

[9] *Мясин Е. А.* Генерация хаотических колебаний в автогенераторе на лавинно-пролетном диоде / Е. А. Мясин // Письма в ЖТФ. 2012. – 38. Вып. 2. – С. 87–94.

[10] *Мясин Е. А.* Хаотическая и регулярная динамика автономных автоколебательных систем, содержащих *p–n*-переход / *Мясин Е. А.*, В. Я. Кислов // Радиотехника и электроника. 1997. – № 12. – С. 1487–1492.

[11] *Кузнецов С. П.* Динамический хаос / С. П. Кузнецов. – Изд-во Физматлит. 2001. – 296 с.

[12] *Lukin K.A., Cerdeira H.A., and Colavita A.A.* Chaotic instability of currents in a reverse biased multilayered structure / Appl. Phys. Lett. – 1997. – vol. 71, No. 17. – pp. 2484–2486.

[13] *Lukin K. A.* Self-oscillations in reverse biased *p–n*-junction with current injection / K. A. Lukin, H. A. Cerdeira, and P. P. Maksymov // Appl. Phys. Lett. – 2003. – vol. 83, No. 20. – pp. 4643-4645.

[14] *Lukin K. A.* Internal Amplification of Current Pulses inside a Reverse Biased *pn–i–pn*-structure / K. A. Lukin, H. A. Cerdeira, A. A. Colavita, P. P. Maksymov // International Journal of Modeling and Simulation – 2003. – 23, No. 2. – P. 77–84.

[15] *Лукин К. А.* Вольтамперная характеристика и наведенный ток во внешней цепи лавинно-генераторных диодов на основе резких обратносмещенных *p–n*-переходов / К А. Лукин, П. П. Максимов // Радиофизика и электроника. – 2015. – 6(20), № 4. – С. 45–53.

[16] *Лукин К. А.* Синхронная генерация двух колебаний микроволнового и терацерцевого диапазонов в лавинно-генераторных диодах с внешним сигналом / К. А. Лукин, П. П. Максимов // Радиофизика и электроника. – 2016. – 7(21), № 2. – С. 66–73.

[17] *Максимов П. П.* Режимы работы лавинно-генераторных диодов микроволнового диапазона / П. П. Максимов // Радиофизика и электрон. – 2016. – 7(21), № 1. – С. 55–60.

[18] *Максимов П. П.* Алгоритм решения уравнений диффузионно-дрейфовой модели полупроводниковых структур с лавинными *p–n*-переходами / П. П. Максимов // Радиофизика и электроника. – Харьков: Ин-т радиофизики и электрон. НАН Украины. – 2008. – 13, № 3. – С. 523–528.

[19] *Лукин К. А.* Модифицированный метод встречных прогонок / К. А. Лукин, П. П. Максимов // Радиофизика и электроника. – Харьков: Ин-т радиофизики и электрон. НАН Украины. – 1999. – 4, № 1. – С. 83–86.

Поступила в редколлегию 15.11.2017

Лукин Константин Александрович, доктор физико-математических наук, профессор, заведующий отделом нелинейной динамики электронных систем Института радиофизики и электроники им. А. Я. Усикова НАН Украины. IEEE Fellow, Руководитель исследовательской группы "Шумовая радарная технология" научно-технологической организации НАТО. Научные интересы: токовые неустойчивости в *p–n*-переходах, динамический хаос в электронных и радиофизических системах, генерация и обработка случайных сигналов, шумовая радиолокация, спектральная интерферометрия, радарная томография, наземные шумовые РСА для дистанционного зондирования.

Максимов Павел Павлович, канд. физ.-мат. наук, старший научный сотрудник отдела нелинейной динамики электронных систем Института радиофизики и электроники им. А. Я. Усикова НАН Украины. Научные интересы: численные методы решения дифференциальных уравнений в частных производных, нелинейная динамика токов в полупроводниковых приборах на основе обратно смещенных электроннодырочных переходов, численное исследование вольтамперной характеристики (ВАХ) резких *p-n*-переходов с постоянным напряжением обратного смещения и определение параметров, исследование автоколебательных режимов в лавинно-генераторных диодах – перспективных полупроводниковых источников электромагнитных колебаний микроволнового и терагерцевого диапазонов.

УДК 621.382.2.029.64

Сценарій переходу до хаосу через переміжність у лавинно-генераторних діодах мікрохвильового діапазону / К. О. Лукін, П. П. Максимов // Прикладна радіоелектроніка: наук.-техн. журнал. – 2017. – Том 16, № 3, 4. – С. 122 – 128.

Вперше досліджено сценарій переходу до хаосу через переміжність в лавинно-генераторному діоді мікрохвильового діапазону. Основним параметром, що управляє сценарієм, є напруга зворотного зсуву. Показано, що зі збільшенням напруги в коливаннях зменшуються ділянки з регулярними періодами і одночасно збільшуються ділянки з нерегулярними періодами. Встановлено, що максимальна ширина спектральних смуг може досягати 34 ГГц, а потужність автоколивань – десятки ват. Досліджено стійкість тимчасових реалізацій двох дискретизованих відліків лавинного струму з близькими початковими умовами на ділянках фазових траєкторій з регулярними і нерегулярними коливаннями.

Ключові слова: лавинно-генераторні діоди, сценарій переходу до хаосу через переміжність в ЛГД, дивний атрактор.

Іл.: 9. Бібліогр.: 19 найм.

UDC 621.382.2.029.64

Scenario of transition to chaos through intermittency in avalanche generator diodes of microwave range / K. A. Lukin, P. P. Maksymov // Applied Radio Electronics: Sci. Journ. – 2017. – Vol. 16, № 3, 4. – P. 122 – 128.

The scenario of transition to chaos through intermittency in an avalanche-generating diode (AGD) in the microwave range has been investigated for the first time. The main control script parameter is the reverse bias voltage. It is shown that with increasing voltage fluctuations portions with regular periods are reduced and at the same time areas with irregular periods increase. It was found that the maximum width of the spectral AGD bands can reach 34 GHz, and the power of self-oscillations can run into tens of watts. The stability of temporal realizations of two sampled avalanche current samples with close initial conditions on the sections of phase trajectories with regular and irregular oscillations is investigated.

Keywords: avalanche-generating diodes, scenario of transition to chaos through intermittency, strange chaotic attractor.

Fig.: 9. Ref.: 19 items.

УДК 615.471.03

К ВОПРОСУ ОБ ОПРЕДЕЛЕНИИ ЭФФЕКТИВНОЙ ДОЗЫ ОБЛУЧЕНИЯ ПАЦИЕНТОВ ПРИ ПРОВЕДЕНИИ ОБСЛЕДОВАНИЙ НА ЦИФРОВОМ РЕНТГЕНОВСКОМ МАММОГРАФЕ

А. В. КИПЕНСКИЙ, С. В. ЛИТВИНЕНКО, Е. В. ХОМЕНКО, О. И. РОМАНОВ, О. В. БОНДАРЬ

В статье изложена усовершенствованная методика определения эффективной дозы облучения пациентов при проведении обследований на цифровом рентгеновском маммографе с приемником рентгеновского излучения, который реализован по схеме: рентгено-люминесцентный экран – оптический объектив – ПЗС-матрица. Приведены типовые значения априорной оценки радиационного выхода рентгеновских излучателей, используемые в методике.

Ключевые слова: рентгеновское излучение, маммография, эффективная доза облучения, анодное напряжение, толщина молочной железы.

ВВЕДЕНИЕ

Рак молочной железы (МЖ) в настоящее время занимает первое место среди злокачественных заболеваний женщин стран СНГ. Непальпируемый рак относится к одной из ранних стадий опухолевого процесса, когда клиническое воздействие имеет высокую вероятность позитивного исхода. Выявление непальпируемого рака возможно только с помощью высокочувствительных рентгеновских маммографов, которые представляют собой специализированные системы для получения снимков МЖ [1–3]. Современный маммограф оснащается встраиваемым или съемным приемником рентгеновского излучения. Цифровой приемник рентгеновского излучения может быть построен на основе полноформатной панели приемных элементов, или реализован по схеме: рентгено-люминесцентный экран (РЛЭ) – оптический объектив (ОО) – ПЗС-матрица (матрица на основе приборов с зарядовой связью). По такой схеме, например, построены цифровые приемники рентгеновского излучения маммографов СИМА и МАДИС, которые разработаны и серийно производятся фирмой РАДМИР (г. Харьков) [4, 5].

На рис. 1 представлена обобщенная структурная схема маммографа с цифровым приемником рентгеновского излучения (РИ), построенным по схеме: РЛЭ – ОО – ПЗС-матрица. Из структурной схемы видно, что рентгеновское излучение, пройдя исследуемый объект, преобразуется в световое излучение с помощью РЛЭ, который совмещен с рентгенозащитным стеклом (РЗС). Далее световое излучение РЛЭ фокусируется с помощью объектива на светочувствительную поверхность ПЗС-матрицы.

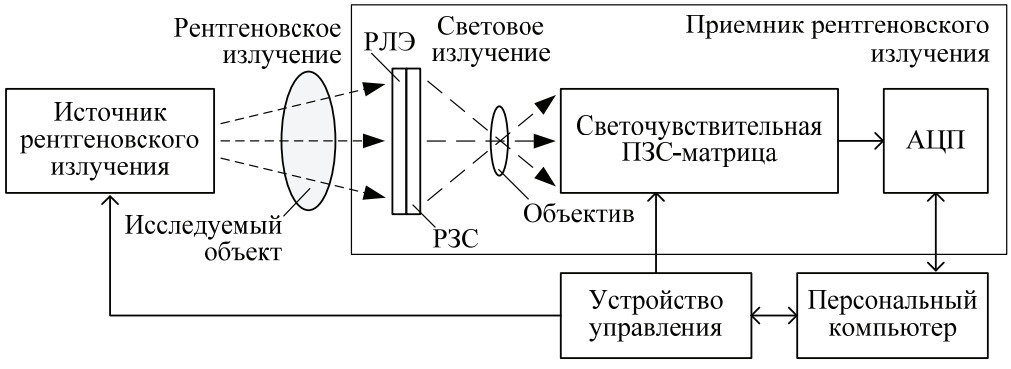


Рис. 1. Структурная схема маммографа с цифровым приемником рентгеновского излучения

Применяемое для просвечивания МЖ рентгеновское излучение, обладает ионизирующим свойством. Ионизирующее воздействие на МЖ может иметь отдаленные последствия в виде канцеро- или соматогенеза в клетках тканей. Поэтому воздействие РИ на биологические объекты необходимо сводить к минимально необходимому. Количественной мерой энергии РИ, поглощенной молочной железой, является эффективная доза, которая зависит не только от интенсивности и спектрального состава воздействующего излучения, но и от параметров самого исследуемого объекта [6].

Отметим, что в состав маммографа не входит встроенный измеритель дозы (или дозиметр с датчиком), т.к. поток рентгеновских квантов от источника РИ настолько ослаблен РЗС, что практически соот-

ветствует естественному фону и не подлежит измерению.

Для медицинских радиологов выпущены различные инструкции и методики по определению эффективной дозы, накопленной в органах и тканях при медицинских обследованиях [7, 8]. Приведенная в [8] методика расчета эффективной дозы относится к маммографам без встроенных измерителей дозы и основана на применении оценки радиационного выхода рентгеновского излучателя, получаемой предварительно при выпуске аппарата из производства, ремонте или регулировке источника РИ по месту эксплуатации маммографа. Под радиационным выходом здесь понимают отношение мощности поглощенной дозы в воздухе, измеренной в точке на оси первичного пучка РИ, отстоящей на расстоянии 1 м от фокуса рентгеновской трубки, к значению анодного тока при заданных значениях анодного напряжения.

Для большинства выпускаемых и эксплуатируемых маммографов расстояние фокус – приемник РИ меньше 1 м (в том числе и для маммографов СИМА и МАДИС) и обычно составляет 60–65 см. Таким образом, при использовании известной методики для измерения радиационного выхода на расстоянии 1 м, необходимо механически отсоединить источник РИ от конструктива маммографа и направить ось первичного пучка в сторону измерителя дозы, расположенного на расстоянии 1 м от источника РИ.

Операции по разборке и съему источника РИ, по измерению радиационного выхода на расстоянии 1 м не являются тривиальными и требуют специальной подготовки технического персонала и организации соответствующего рабочего места, что не всегда выполнимо в условиях лечебно-профилактического учреждения (ЛПУ).

Цель данной работы состоит в разработке методики определения эффективной дозы облучения пациентов при проведении исследований на рентгеновском маммографе без встроенных измерителей дозы и при произвольном расстоянии между фокусным пятном рентгеновской трубки и приемником РИ, которое предусмотрено штатной работой маммографа в соответствии с его функциональным назначением.

1. МЕТОДИКА ОПРЕДЕЛЕНИЯ ДОЗЫ РЕНТГЕНОВСКОГО ОБЛУЧЕНИЯ

Рассмотрим методику определения эффективной дозы, основанную на предварительном измерении радиационного выхода источника РИ маммографа без его демонтажа. На рис. 2 представлен общий вид маммографа СИМА, где показаны рабочий стол пациента, расстояние от фокального пятна рентгеновской трубки до плоскости рабочего стола $L_{\text{ФП}}$ и расстояние от компрессионной пластины до плоскости рабочего стола $L_{\text{КОМ}}$.

Решение задачи определения эффективной дозы рентгеновского облучения пациента при проведении маммографических обследований можно разделить на четыре этапа.

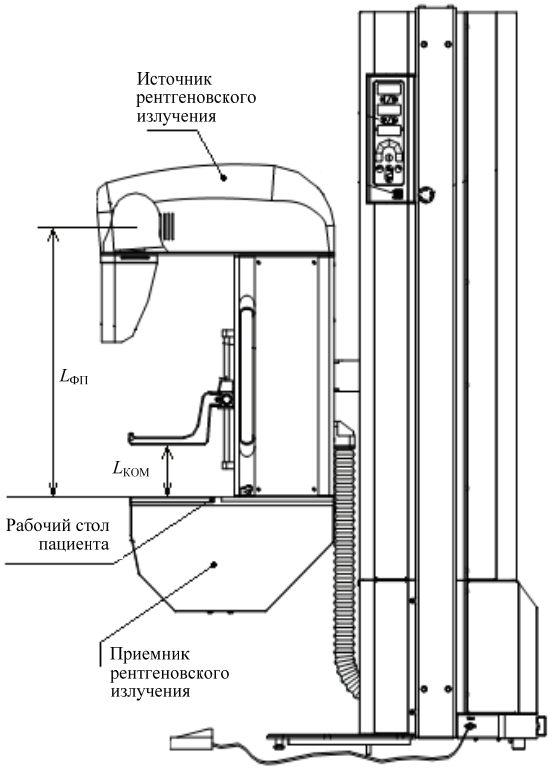


Рис. 2. Общий вид маммографа СИМА

Этап 1. Оценка радиационного выхода рентгеновского излучателя. Измерения радиационного выхода источника РИ выполняются на предприятии-изготовителе при выпуске или после ремонта маммографа, а также они могут быть выполнены при проведении планового технического обслуживания по месту эксплуатации в ЛПУ. Измерения проводят с помощью дозиметра, датчик которого размещают на осевой линии рабочего стола пациента и опускают компрессионную пластину до касания с корпусом датчика.

Измеренные значения дозы на поверхности рабочего стола пациента фиксируют при изменениях анодного напряжения рентгеновской трубки в диапазоне от 22 до 34 кВ (с шагом 1 кВ). Далее, зафиксированные значения дозы, приводят к 1 мА·с по формуле:

$$R_{\text{ПОВ}}(U_{\text{А}}) = \frac{{L_{\text{ФП}}}^2}{(L_{\text{ФП}} - L_{\text{КОМ}})^2} \cdot \frac{D_{\text{ПОВ}}(U_{\text{А}})}{I_{\text{А}} \cdot T_{\text{ЭКС}}}, \qquad (1)$$

где $R_{\text{ПОВ}}(U_{\text{А}})$ – радиационный выход (приведенная к 1 мА·с доза на поверхности рабочего стола или МЖ), мкГр/мА·с; $D_{\text{ПОВ}}(U_{\text{А}})$ – измеренное с помощью дозиметра значение дозы на поверхности рабочего стола пациента при заданном анодном напряжении $U_{\text{А}}$, токе и длительности экспозиции, мкГр; $I_{\text{А}} \cdot T_{\text{ЭКС}}$ – заданное при измерениях произведение ток-время (здесь: ток – сила анодного тока рентгеновской трубки, время – длительность временного интер-

вала экспозиции), мА·с; $L_{КОМ}$ – задаваемое значение толщины МЖ в диапазоне от 0 до 8 см; $L_{ФП}$ – расстояние от фокального пятна рентгеновской трубки до поверхности рабочего стола пациента (приведенные в работе графики и расчеты проводились для $L_{ФП} = 65$ см).

Результаты измерений дозы заносят в рабочую программу маммографа, где по формуле (1) выполняется расчет приведенных значений радиационного выхода.

На рис. 3 в графическом виде приведены зависимости радиационного выхода от анодного напряжения рентгеновской трубки при различных значениях толщины МЖ.

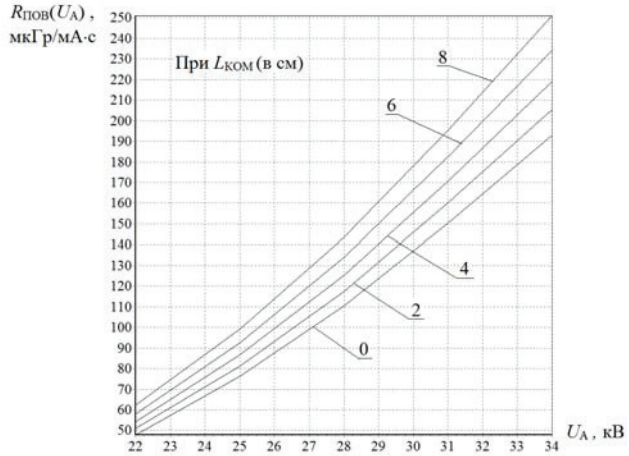


Рис. 3. Зависимости приведенного радиационного выхода источника РИ на поверхности МЖ от анодного напряжения рентгеновской трубки при различных значениях толщины МЖ

В табл. 1 приведены некоторые типовые значения полученных данных для источника РИ, построенного на основе рентгеновской трубки с вращающимся молибденовым анодом.

Таблица 1

Приведенные значения дозы $R_{ПОВ}(U_A)$ на поверхности МЖ (приведенный радиационный выход), мкГр/мА·с

Толщина МЖ $L_{КОМ}$, см	Анодное напряжение U_A, кВ				
	22	25	28	31	34
0	47,8	76,3	110,4	150,3	193,0
2	50,9	81,2	117,5	160,0	205,5
4	54,3	86,6	125,4	170,6	219,2
6	58,1	92,6	134,0	182,4	234,3
8	62,2	99,2	143,6	195,4	251,0

Этап 2. Расчет приведенных средних значений поглощенной дозы. Приведенные средние значения поглощенной дозы рассчитывают для значений напряжения U_A, изменяемого в диапазоне от 22 до 34 кВ и толщины МЖ $L_{ком}$ – в диапазоне от 0 до 8 см по формуле:

$$D_{Ж}(U_A) = K_{Ж}(L_{КОМ}) \cdot R_{ПОВ}(U_A), \qquad (2)$$

где $D_{Ж}(U_A)$ – приведенное среднее значение поглощенной дозы, мкГр/мА·с; $R_{ПОВ}(U_A)$ – значение приведенной к 1 мА·с дозы на поверхности молочной железы, взятое из табл. 1, мкГр/мА·с; $K_{Ж}(L_{КОМ})$ – коэффициент перехода от значений дозы на поверхности МЖ к средней дозе в МЖ (см. [8], табл. 8–1), определенный для комбинации материалов анод трубки/фильтр – молибден/молибден.

Зависимости приведенного среднего значения поглощенной дозы от анодного напряжения рентгеновской трубки при различной толщине МЖ представлены в графическом виде на рис. 4.

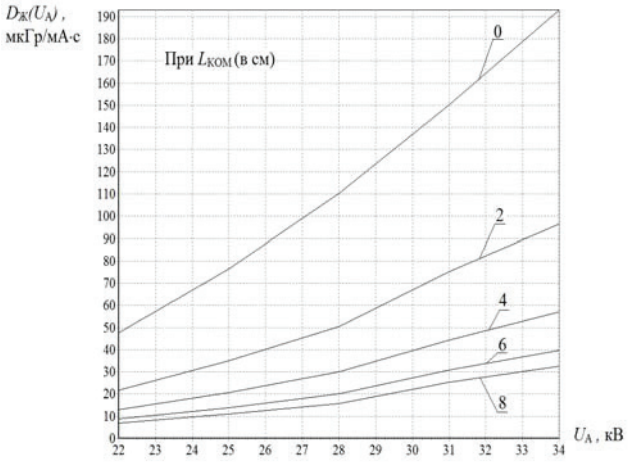


Рис. 4. Зависимости приведенного среднего значения поглощенной дозы от анодного напряжения рентгеновской трубки при различных значениях толщины МЖ

Некоторые типовые результаты вычислений по формуле (2) сведены в табл. 2.

Таблица 2

Приведенные средние значения поглощенной дозы, мкГр/мА·с

Толщина МЖ $L_{ком}$, *см*	$K_{ж}$ *22-29кВ/ 30-35кВ*	Анодное напряжение U_A, *кВ*				
		22	25	28	31	34
0	1/1	47,8	76,3	110,4	150,3	193,0
2	0,43/0,47	21,9	34,9	50,5	75,2	96,6
4	0,24/0,26	13,0	20,7	30,1	44,3	57,0
6	0,15/0,17	8,7	13,8	20,1	31,0	39,8
8	0,11/0,13	6,8	10,9	15,8	25,4	32,6

Этап 3. Расчет приведенных значений эффективной дозы. Приведенные значения эффективной дозы определяют по формуле:

$$E_{ПР}(U_A) = D_{Ж}(U_A) \cdot W_Р \cdot W_Т, \qquad (3)$$

где $E_{ПР}(U_A)$ – приведенное значение эффективной дозы, мкЗв/мА·с; $D_{Ж}(U_A)$ – приведенное среднее значение поглощенной дозы (взятое из табл. 2), мкГр/мА·с; $W_Р = 1$ мкЗв/мкГр – взвешивающий ко-

эффициент (переводит поглощенную дозу в эквивалентную); $W_T = 0{,}05$ – взвешивающий фактор (учитывает вероятность лучевого поражения облучаемого органа).

На рис. 5 в графическом виде представлены зависимости приведенного значения эффективной дозы от анодного напряжения рентгеновской трубки при различной толщине МЖ.

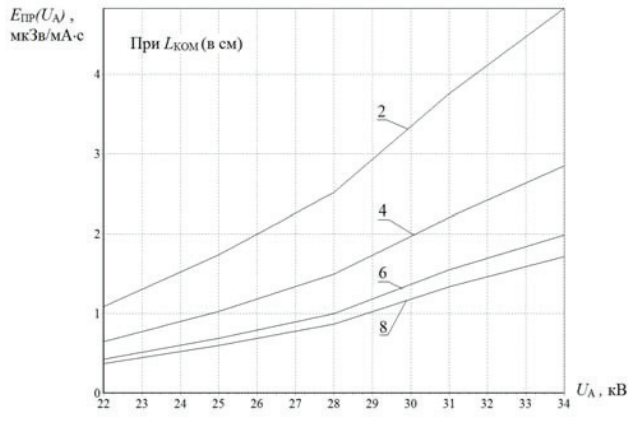


Рис. 5. Зависимости приведенных средних значений эффективной дозы от анодного напряжения рентгеновской трубки при различных значениях толщины МЖ

Отдельные результаты вычислений по формуле (3) представлены в табл. 3.

Таблица 3

Приведенные значения эффективной дозы, мкЗв/мА·с

Толщина МЖ	Анодное напряжение U_A, *кВ*				
$L_{ком}$, см	22	25	28	31	34
$0< L_{ком} \le 2$	1,09	1,74	2,52	3,76	4,83
$2< L_{ком} \le 4$	0,65	1,03	1,50	2,21	2,85
$4< L_{ком} \le 6$	0,43	0,69	1,00	1,55	1,99
$6< L_{ком}$	0,37	0,60	0,87	1,34	1.72

Этап 4. Определение эффективной дозы облучения пациентов. Значение эффективной дозы облучения МЖ в результате выполнения снимка определяют следующим образом. По измеренному значению толщины МЖ $L_{КОМ}$ и заданному значению анодного напряжения рентгеновской трубки U_A в табл. 3 отыскивают приведенное значение эффективной дозы $E_{ПР}$. Далее определяют эффективную дозу облучения пациента после выполнения снимка МЖ по формуле:

$$E = E_{ПР}(U_A) \cdot I_A \cdot T_{ЭКС}, \qquad (4)$$

где E – эффективная доза облучения, мкЗв; $E_{пр}(U_A)$ – приведенное значение эффективной дозы, мкЗв/мА·с; $I_A \cdot T_{ЭКС}$ – величина произведения ток-время (экспозиция), установленная при выполнении снимка, мА·с.

Рассчитанное в ПК значение эффективной дозы выводится на экран монитора, сохраняется в базе данных рабочей программы и распечатывается в заключении врача.

ВЫВОДЫ

Совершенствование методики позволяет определить эффективную дозу облучения пациентов при проведении обследований на рентгеновском маммографе для любого штатного расстояния между фокусным пятном источника РИ и приемником. Расчет эффективной дозы основан на использовании оценки радиационного выхода источника РИ и не требует демонтажа источника РИ или приемника. Такой подход сокращает продолжительность выполнения работ по определению радиационного выхода, снижает требования к организации рабочего места для выполнения работ (что особенно важно для ЛПУ), повышает эксплуатационную пригодность рентгеновского маммографа.

Литература

[1] *Рожкова Н.И., Кочетова Г.П., Мазо М.Л.* Техническое оснащение вакуумной аспирационной биопсии молочной железы под рентгеновским и ультразвуковым контролем // М.: Журнал «Медицинская техника» № 5 (251), 2008. – С.40–43.

[2] *Hashimoto E.* Practical digital mammography / Beverly E. Hashimoto. // Thieme Medical Publishers, Inc., New York, Stuttgart. – 2008. – P. 205

[3] *Солодкий В.А., Ставицкий Р.В.* Методы визуализации и контроля организма и его систем. – М.: «ГАРТ», 2009. – 352 с.

[4] *Хоменко Е.В., Кущ П.И.* Рентгеновский маммографический цифровой комплекс МАДИС для скрининговых и диагностических обследований молочной железы // Научно-практический журнал «Вестник рентгенлаборантов и рентгенологов». Донецк. 2007, № 1 (11). – С. 21–22.

[5] *Литвиненко С.В., Хоменко Е.В.* Рентгеновский маммографический комплекс СИМА – оптимальное средство для скрининг-диагностики // М.: Журнал «Медицинский бизнес» № 9 (233), 2013.

[6] Радіаційна медицина: підручник за редакцією чл.-кор. НАМН України, проф. М.І. Пилипенка. – К.: ВСВ «Медицина», 2013. – 232 с.

[7] Розрахунок та облік індивідуальної ефективної дози опромінення пацієнта від рентгенодіагностичних процедур. Відомча інструкція. МОЗ України. Харківський науково-дослідний інститут медичної радіології. – Харків, 1995 р.

[8] Ионизирующее излучение, радиационная безопасность. Контроль эффективных доз облучения пациентов при проведении медицинских рентгенологических исследований. Методические указания МУ 2.6.1.2944-11. Федеральная служба по надзору в сфере защиты прав потребителей и благополучия человека. – Москва, 2011 г.

Поступила в редколлегию 13.12.2017

Кипенский Андрей Владимирович – доктор технических наук, профессор кафедры промышленной и биомедицинской электроники Национального технического университета «Харьковский политехнический институт», академик Академии наук прикладной радиоэлектроники. Область научных интересов – теория микропроцессорного импульсного управления изделиями медицинской техники различного назначения.

Литвиненко Сергей Викторович – кандидат технических наук, директор фирмы «Радмир». В 1986 г. окончил Харьковский институт радиоэлектроники. Область научных интересов – исследование воздействия ионизирующего излучения на биологические объекты.

Хоменко Евгений Владимирович – кандидат технических наук, старший научный сотрудник, главный конструктор ООО «Элкомед». В 1975 г. окончил Харьковский политехнический институт. Область научных интересов – проблемы электромагнитного воздействия на материалы и радиофизические системы.

Романов Олег Иванович – главный конструктор фирмы «Радмир». В 1975 г. окончил Харьковский институт радиоэлектроники. Область научных интересов – проблемы формирования и обработки рентгеновских изображений.

Бондарь Олег Владимирович – ведущий инженер-программист ООО «Элкомед». В 1990 г. окончил Харьковский авиационный институт. Область научных интересов – проблемы взаимодействия рентгеновского излучения с веществами, обладающими различными фрактальными свойствами, цифровая обработка рентгеновских изображений.

УДК 615.471.03

До питання про визначення ефективної дози опромінення пацієнтів під час проведення обстежень на цифровому рентгенівському маммографі / А.В. Кіпенський, С.В. Литвиненко, Є.В. Хоменко, О.І. Романов, О.В. Бондар // Прикладна радіоелектроніка: наук.-техн. журнал. – 2017. – Том 16, № 3, 4. – С. 129 – 133.

У статті викладено удосконалену методику визначення ефективної дози опромінення пацієнтів під час проведення обстежень на цифровому рентгенівському маммографі з приймачем рентгенівського випромінювання, що реалізований за схемою: рентгено-люмінесцентний екран – оптичний об'єктив – ПЗС-матриця. Наведені типові значення апріорної оцінки радіаційного виходу рентгенівських випромінювачів, що використовувані в методиці.

Ключові слова: рентгенівське випромінювання, маммографія, ефективна доза опромінення, анодна напруга, товщина молочної залози.

Табл.: 3. Іл.: 5. Бібліогр.: 8 найм.

UDC 615.471.03

On the determination of an effective radiation dose of patients when conducting examinations on a digital X-ray mammograph / A.V. Kipenskyi, S.V. Litvinenko, E.V. Homenko, O.I. Romanov, O.V. Bondar // Applied Radio Electronics: Sci. Journ. – 2017. – Vol. 16, № 3, 4. – P. 129 – 133.

The paper presents a developed technique for determining the effective radiation dose of patients when performing examinations on a digital X-ray mammograph with an X-ray receiver constructed according to the X-ray fluorescent screen – optics – CCD-matrix scheme. Typical values of the a priori estimate of the radiative X-ray emitters yield used in the technique are given.

Keywords: X-ray radiation, mammography, effective dose of radiation, anodic voltage, thickness of mammary gland.

Tab.: 3. Fig.: 5. Ref.: 8 items.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

УДК 621.396.96:621.271.029.65

ИСПОЛЬЗОВАНИЕ СМАРТ-ГРИД ТЕХНОЛОГИЙ ДЛЯ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ПРИМЕНЕНИЯ ОБЪЕКТОВ НАЗЕМНОЙ ТЕХНИКИ

В. И. ЛУЦЕНКО, И. В. ЛУЦЕНКО, А. В. СОБОЛЯК

Рассмотрена возможность построения интеллектуальных сетей из отдельных объектов наземной техники и за счет этого повышения эффективности их применения и живучести. Особое значение имеет повышение информативности каналов получения информации о внешней обстановке путем объединения информационных потоков каналов, использующих различные физические поля (акустические, электромагнитные и т.п.). Оценены дальности обнаружения для различных датчиков и результат, получаемый от их комплексирования.

Ключевые слова: смарт-грид технологии, интеллектуальные сети, объекты наземной техники.

ВВЕДЕНИЕ

То, что в настоящее время называется смарт–грид технологиями или технологиями распределенного интеллекта применялись в военном деле с незапамятных времен. Действительно иерархия построения военной структуры предполагает принятие решений каждым звеном в области зоны своей ответственности, обмен принятыми решениями, результатами их выполнения, а также изменениями обстановки в зоне своей ответственности. Иное дело, что каналы передачи информации между отдельными структурными звеньями в течении веков претерпели существенные изменения. Создание в последнее время роботизированных датчиков, передача и отображение информации отдельных звеньев управления на общий пункт, а также отображение в пределах зоны ответственности каждого из звеньев не только информации, полученной от его информационных датчиков, но и интегральной информации от пункта управления, приводит к тому, что военные системы управления становятся в полной мере смарт-грид системами с распределенным интеллектом.

1. ВОЗНИКНОВЕНИЕ ПОНЯТИЯ SMART GRID

Первоначально интеллектуальные сети Smart Grid рассматривались как перспективная концепция будущей энергетики. Однако появившись применительно к умным энергетическим системам этот термин получил более широкое распространение применительно, например, к концепции построения умного дома, интеллектуальных систем водоснабжения [1–3].

С точки зрения Министерства энергетики США, интеллектуальным сетям (Smart Grid) присущи следующие атрибуты [3]: способность к самовосстановлению после сбоев; возможность активного участия в работе сети потребителей; устойчивость сети к физическому и кибернетическому вмешательству злоумышленников; обеспечение требуемого качества передаваемой электроэнергии; обеспечение синхронной работы источников генерации и узлов хранения электроэнергии; появление новых высокотехнологичных продуктов и рынков; повышение эффективности работы энергосистемы в целом.

Smart Grid можно описать следующими аспектами функционирования: гибкость, доступность, надежность, экономичность.

Аналогичные принципы могут использоваться и при построении интеллектуальных распределенных сетей управления объектами военной техники.

По-видимому, впервые принципы смарт-грид технологий были реализованы в универсальном ракетном комплексе «Гранит» с дальней противокорабельной крылатой ракетой П-700 подводно-надводного старта, разработки 70г.г. 20века [4]. Он предназначен для поражения авианосных групп НАТО.

Комплекс обеспечивает залповую стрельбу всем боекомплектом с рациональным пространственным расположением ракет и позволяет действовать против одиночного корабля по принципу «одна ракета-один корабль» или «стаей» против ордера кораблей. В режиме беглого огня одна ракета, выполняющая роль «наводчика», летит по высокой траектории, чтобы максимально увеличить площадь захвата цели, в то же время другие ракеты летят по низкой траектории. В полёте ракеты обмениваются информацией о целях. Если ракета - «наводчик» перехвачена, тогда одна из других ракет автоматически принимает на себя её функции [4].

Ракеты сами распределяют и классифицируют по важности цели, выбирают тактику атаки и план ее проведения. Для исключения ошибки при выборе маневра и поражения заданной цели в бортовую вычислительную машину (БЦВМ) заложены электронные данные по современным классам кораблей. К тому же в БЦВМ есть и тактические сведения, к примеру, о типе ордеров кораблей, что позволяет ракете определить, кто перед ней – конвой, авианесущая или де-

сантная группа, и атаковать главные цели в ее составе.

В БЦВМ заложены данные по противодействию средствам радиоэлектронной борьбы противника, способным постановкой помех уводить ракеты от цели, тактические приемы уклонения от огня средств противовоздушной обороны. После пуска ракеты сами решают, какая из них будет атаковать, какую цель и какие маневры для этого нужно осуществить в соответствии с заложенными в программу поведения математическими алгоритмами. Ракета имеет и средства противодействия атакующим ее противоракетам. Уничтожив главную цель в корабельной группе, оставшиеся ракеты атакуют другие корабли ордера, исключив возможность поражения двумя ракетами одной и той же цели [4].

Эти идеи получили дальнейшее развитие в последующих комплексах ПКР [5] – в крылатых ракетах 3М-55 «Оникс» и созданной на её базе российско-индийской ракете «БраМос». Особенность этих ракет – в системе искусственного интеллекта, сравнимой с человеческим, позволяющей действовать против одиночного корабля по принципу «одна ракета – один корабль» или «стаей» против ордера кораблей.

«Граниты» и «Ониксы» – «стайные» машины [7]. Именно в залпе раскрывается их главное тактическое преимущество: ракеты сами распределят и классифицируют по важности цели, выберут тактику атаки и план ее проведения. Для исключения ошибки при выборе маневра и поражения именно заданной цели в бортовую вычислительную машину ПКР заложены электронные «портреты» всех современных классов кораблей. Это позволяет повысить достоверность определения типа цели, в том числе и при применении методов радиомаскировки и искажения радиоэлектронных сигнатур целей.

И если в системах ПВО и ПРО принципы построения интеллектуальных распределенных сетей используются, то для объектов наземной техники их внедрение является сейчас актуальной задачей.

Первые шаги в этом направлении сделаны при создании российской платформы «Армата» (Т-14) [6].

В отличие от традиционных танков, Т-14 является «сетецентрическим танком», т. е. предназначен не для одиночного боя, а для работы с группой различных боевых машин в одном тактическом звене, выполняя функции разведки, целеуказания и дистанционного управления через единую систему управления тактического звена от концерна «Созвездие» [6]. Это позволяет всем машинам платформы «Армата» получать оперативную обстановку в режиме реального времени и автоматически рассчитывать баллистические данные для систем управления огнём в сценарии поражения целей не одной «Арматой», а сразу всей группой, которая включает в себя, кроме Т-14, ещё несколько тяжёлых БМП Т-15, САУ 2С35 «Коалиция-СВ» и ударный вертолет [6]. В соответствии с теорией сетецентрической войны танк больше не будет «один в поле воин». Современная война ведется не на поле боя, а в информационном пространстве. Для его создания Т-14 будет получать данные от разведчиков и штабов, от других боевых машин, от беспилотных летательных аппаратов и даже прямо с разведывательных спутников [6]. В перспективе подобная система в совокупности с необитаемой башней позволит создать беспилотный танк. Но это будет уже машина пятого поколения.

Приведенные примеры показывают, что при внедрении смарт–грид технологий управления объектами военной техники, которые могут повысить эффективность ее применения, ключевыми вопросами является создание многоканальных датчиков отображения информационных сцен, в том числе и использующих различных физические поля, а также автоматизация процессов обмена информацией между различными участниками сцен и пунктами управления.

2. ДАТЧИКИ И КАНАЛЫ ПОЛУЧЕНИЯ ИНФОРМАЦИИ ОБЪЕКТОВ НАЗЕМНОЙ ТЕХНИКИ ОБ ОКРУЖАЮЩЕЙ ОБСТАНОВКЕ

Датчики, использующие электромагнитные поля. В настоящее время основными каналами получения информации являются визиры оптического и инфракрасного диапазонов волн. Основные технические характеристики используемых на отечественной и зарубежной БТ оптических и ИК датчиков, заимствованные из работы [7] приведены в табл. 1.

Дополнительно для разведки могут использоваться и существующие излучения систем наземного и космического базирования других диапазонов длин волн. Так может использоваться излучение наземных телевизионных центров [8–9].

Таблица 1

Основные характеристики приборов наблюдения и прицеливания БТТ [7]

Оптико-технические характеристики	Прицелы		Приборы наблюдения					
			дневные		ночные			
	ПП-61 АМ	1ПЗ-2	ТПКУ-2Б	ТНПО-115; ТНП-165	ТКН-1С	ТКН-3	ТВНО-2Б	ТВНЕ-4Б
Увеличение, крат. пост./панкрат.	2,6	1,2/3,0	5	-	2,75	3,0/2,2	1,0	1,0
Перископичность, мм	285	285	200	200	200	200	200	200
Дальность действия, м (день/ночь)	2000	2000	3000	смотровые	-/300	4000/400	-/100	-/120

В последнее время интерес проявляется к созданию активно-пассивных систем, использующих для подсветки воздушной обстановки излучение вещательных КВ станций [10–14]. Кроме того для освещения обстановки может использоваться излучение систем, расположенных в космосе: навигационных спутников [15, 16], а также геостационарных телевизионных и вещательных спутников. Кроме того, для задач разведки могут использоваться и акустические поля, например, собственные акустические шумы объектов техники [17–22]. Ниже будут кратко рассмотрены возможности использования каждого из этих дополнительных информационных каналов, а также получаемый от этого эффект.

ЭПР объектов техники в декаметровом и УКВ диапазонах волн. Для расчета дальностей действия активно-пассивных систем, использующих для подсветки сигналы вещательных КВ и УКВ станций, собственные радиостанции объектов наземной бронетехники, сигналы навигационных и геостационарных телевизионных спутников необходимо знание ЭПР обнаруживаемых наземных и воздушных объектов. Используя результаты экспериментальных исследований на моделях [24–25] в работе [14] была предложена методика и рассчитаны ЭПР воздушных объектов. Используя эту методику расчета, аналогичным образом были оценены ЭПР наземных объектов. Обобщающие данные ЭПР приведены в табл. 2.

Таблица 2

Среднее значение ЭПР объектов в резонансной области

Объект	Назначение	Горизонтальная поляризация		Вертикальная поляризация
		ЭПР в резонансной области		
		Корпус, дБ/м^2	Винт, дБ/м^2	Корпус, дБ/м^2
Вертолет	МЦ	27,3	26,3	18,3
	У	28,6	27,4	17,4
	Т	31,5	30,3	21,4
		Корпус, дБ/м^2	Крыло, дБ/м^2	Корпус, дБ/м^2
Самолет	Ш	26,7	25,4	17,2
	Б	35,6	36,6	23,6
	И	30,5	26,7	19,8
	П	37,6	36,9	26,6
	БПЛА	2,5	12,5	-
		Корпус с пушкой, дБ/м^2	Корпус, дБ/м^2	Корпус, дБ/м^2
Танк		25,3	16,0	13,4

В таблице использованы следующие обозначения: У – ударный, Т – транспортный, МЦ – многоцелевой, Ш – штурмовик, И – истребитель, Б – бомбарди-ровщик. П – пассажирский, БПЛА – беспилотный.

Анализ показывает, что в резонансной области рассеяния ЭПР может иметь значительную величину, достигающую сотен, тысяч квадратных метров, для резонансных частот облучающего поля от единиц до десятка мегагерц.

Подсветка с использованием излучений вещательных КВ станций. Особенностью данного вида радиолокации является использование для подсветки обстановки ионосферной волны вещательной КВ станции. Это позволяет осуществлять подсветку обстановки на удалениях в несколько тысяч километров от передающей станции. Мощность принимаемого отраженного целью сигнала P_t определяется соотношением:

$$P_T = \frac{P_{Tr} G_{Tr} G_R F^2(\theta_T) \sigma_T(\theta_{Tr}, \theta_R) \lambda^2}{(4\pi)^3 R_{TrT}^2 R_{TR}^2 {}^2 L_{TrT} L_{TR}}, \qquad (1)$$

где P_{Tr}, P_T – излучаемая и принимаемая отраженная от цели мощности; G_{Tr}, G_R – коэффициенты усиления передающей и приемной антенн; R_{TrT}, R_{TR} – дальности между передатчиком и целью и целью и приемником, $\sigma(\theta_{Tr}, \theta_R)$ – бистатическая ЭПР цели при направлениях на передатчик и приемник θ_{Tr}, θ_R – соответственно; L_{TrT}, L_{TR} – потери при распространении радиоволн от передатчика до цели и от цели до приемника соответственно; λ – рабочая длина волны излучения.

Мощность принимаемого сигнала P_R от передающей станции:

$$P_R = \frac{P_{Tr} G_{Tr} G_R F^2(\theta_{Tr}) \lambda^2}{(4\pi)^2 R_{TrR}^2 L_{TrR}}, \qquad (2)$$

где $F^2(\theta_{Tr})$ – значение диаграммы направленности приемной антенны по мощности в направлении на передатчик - θ_{Tr} .

Отношение мощностей сигналов, принимаемых от цели и от передающей вещательной станции μ_{TR} с учетом того, что расстояние от станции подсветки до цели и приемной системы существенно больше расстояния от цели до приемника $R_{TrT}^2 \approx R_{TrR}^2 >> R_{TR}^2$, а потери при распространении до цели и приемника примерно одинаковы $L_{TrT} \approx L_{TrR}$, причем цель в первом приближении можно полагать изотропно отражающей $\sigma_T(\theta_{Tr}, \theta_R) \approx \sigma_T = const$ и находящейся в пределах прямой видимости приемной системы $L_{TR} \approx 1$, определяется соотношением:

$$\mu_{TR} = \frac{P_T}{P_R} \approx \frac{F^2(\theta_T)}{F^2(\theta_{Tr})} \frac{\sigma_T}{(4\pi)\ R_{TR}^2}. \qquad (3)$$

Анализ соотношения (3) показывает, что для увеличения отношения сигналов от цели к прямому сигналу передатчика станции подсветки, которым и определяется дальность обнаружения, необходимо увеличивать отношение значений диаграммного множителя в направлениях на цель и на станцию подсветки. При этом целесообразно в направлении на цель ориентировать максимум диаграммы направленности, а в направлении на станцию подсветки формировать ноль диаграммы. Глубина сформированного провала в диаграмме направленности будет ограничивать максимальную дальность обнаружения. Помимо формирования нуля диаграммы направленности в направлении на источник подсветки (ГНСС) повышение соотношения сигнал-помеха может быть достигнуто за счет применения узкополосной доплеровской фильтрации. Известно, что спектр обратного рассеяния от воздушных, надводных и наземных объектов достаточно узкополосен даже в СВЧ диапазоне. Ширина спектра линии корпуса не превышает десятка Гц [14,23]. В КВ и УКВ диапазонах волн он еще уже – менее 1 Гц. Примерно такой же порядок величин имеет в этих диапазонах и величина допплеровского смещения частоты (единицы-десятки Гц) [14]. При доплеровской селекции можно выделять спектральную линию рассеянного объектом сигнала на доплеровской частоте. Отношение сигнал-шум μ при этом будет определяться отношением сигнала цели μ_{TR} к сигналу подсветки, а также отношением уровня спектральной линии несущей к спектральной плотности шума в диапазоне доплеровских частот (скоростей), где происходит обнаружение цели μ_{SN}:

$$\mu = \mu_{TR}\mu_{SN}. \qquad (4)$$

Используя соотношение (3), можно записать выражение для оценки дальности обнаружения в бистатических РЛС:

$$R_{TR} = \sqrt{\frac{\mu_{SN}}{\mu} \frac{\sigma_T}{(4\pi)} \frac{F^2(\theta_T)}{F^2(\theta_{Tr})}}. \qquad (5)$$

Для вероятностей правильного обнаружения 0,9, ложной тревоги 10^{-2} (соотношения сигнал-помеха около μ=10 дБ), уровне шума по отношению к несущей μ_{SN}=40...50 дБ при расстройке на доплеровское смещение частоты, ожидаемые дальности обнаружения объектов с различными ЭПР при разной глубине провала диаграммы направленности приемной антенны в направлении на передатчик, полученные с использованием соотношения (5), приведены на рис. 1. На этом же рисунке заштрихованными областями показаны значения ЭПР наземных и воздушных объектов техники взятые из табл. 2. Для получения оценок ЭПР различных типов объектов в декаметровом диапазоне волн использовались результаты, приведенные в работах [14, 23], а также данные модельных экспериментов [24–25].

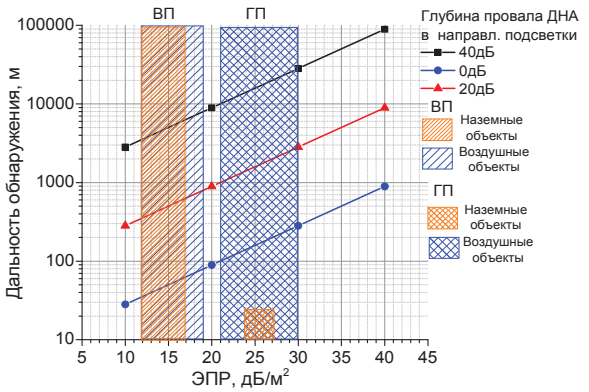


Рис. 1. Дальности обнаружения объектов при использовании подсветки вещательными станциями КВ диапазона

Анализ показывает, что лишь обеспечив достаточно глубокое подавление прямого сигнала подсветки не менее чем на 40дБ можно обеспечить дальности обнаружения в единицы километров для целей с ЭПР более 10м^2. Такие или большие ЭПР в декаметровом диапазоне у объектов как наземной, так и воздушной техники. Несколько больше дальности обнаружения при использовании горизонтальной поляризации излучения и приема, чем вертикальной, что объясняется большими значениями их ЭПР на этой поляризации. Для реализации глубокого подавления прямого сигнала подсветки необходимо либо формирование нуля диаграммы в направлении передатчика, например, интерферометрическим методом с использованием двух антенн, либо применением поляризационных методов подавления прямого сигнала. Однако конкретные технические решения этого вопроса выходят за пределы настоящей работы.

Подсветка обстановки с использованием излучений собственных радиостанций КВ и УКВ диапазонов, установленных на бронетехнике. Помимо внешних источников подсветки объектами наземной техники могут использоваться для этих целей и собственные средства связи в виде КВ и УКВ радиостанций. Для группы объектов бронетехники можно предложить следующий алгоритм использования собственных средств радиосвязи для освещения обстановки. Каждый из объектов группы излучает в течение некоторого времени Δt, определяемого требуемым разрешением по допплеровской частоте Δf монохроматический либо модулированный по амплитуде или частоте сигнал:

$$\Delta t = 1/\Delta f. \qquad (6)$$

Поскольку ширина доплеровской линии отражений от корпуса воздушных объектов менее 1 Гц, то

длительность сигнала подсветки должна составлять несколько секунд, чтобы не происходило ее уширение за счет ограниченного времени облучения. В это время радиостанции остальных объектов работают на прием. Затем подсветку местности осуществляет следующий объект группы, а остальные работают на прием. При работе передатчика радиостанции его приемник ослеплен излучаемым сигналом собственного передатчика. Каждый из объектов может подсвечивать обстановку на своей частоте. При этом частота может использоваться для передачи номера объекта и его координат. При этом получается сочетание режимов уоки – токи с излучением чирп сигнала. Поэтому предложенный нами режим можно назвать: чирп - уоки –токи.

Особенностью данного режима активно-пассивной радиолокации, по сравнению с рассмотренным ранее случаем, является подсветка обстановки поверхностной волной, которая подвержена существенному интерференционному замиранию вследствие влияния поверхности раздела.

Мощность прямого сигнала и сигнала подсветки, переотраженного целью можно определить с учетом соотношений (1, 2):

$$P_R = \frac{P_{Tr} G_{Tr} G_R \lambda^2}{(4\pi)^2 R_R^2} V_R^2, \qquad (7а)$$

$$P_T = \frac{P_{Tr} G_{Tr} G_R \sigma_T(\theta_{Tr},\theta_R) \lambda^2}{(4\pi)^3 R_T^4} V_T^4. \qquad (7б)$$

где $V_R = \frac{h_{Tr} h_R}{\lambda R_R}$, $V_T = \frac{h_{Tr} h_T}{\lambda R_T}$ – множитель ослабления поверхности при дальности связи R_R и дальности радиолокации R_T, а h_{Tr}, h_R, h_T высота антенн передатчика, приемника и цели соответственно, причем $h_{Tr} = h_R$.

Тогда учитывая, что эти мощности должны превышать уровень шумов в μ_T раз при обнаружении цели и μ_R - раз при передаче речевого сигнала:

$$P_R = \mu_T kt \Delta F_R N, \qquad (8а)$$

$$P_T = \mu_R kt \Delta F_T N, \qquad (8б)$$

а также то, что требуемые соотношения сигнал шум в этих случаях примерно одинаковы $\mu_T \approx \mu_R$, используя соотношений (7, 8), можно записать:

$$\frac{\Delta F_T}{\Delta F_R} = \frac{\sigma_T(\theta_{Tr},\theta_R)}{(4\pi) R_T^4 R_R^{-2}} \left(\frac{h_{Tr} h_T}{\lambda R_T}\right)^4 \left(\frac{h_{Tr} h_R}{\lambda R_R}\right)^{-2} =$$

$$= \frac{\sigma_T}{(4\pi)} \frac{R_R^4}{R_T^8} (h_T)^4 (\lambda)^{-2}. \qquad (9)$$

Тогда дальность при таком варианте активно-пассивной радиолокации определиться из соотношения (9):

$$R_T = \left(\frac{\Delta F_T}{\Delta F_R}\right)^{-1/8} \left(R_R^4\right)^{1/2} \left(\frac{\sigma_T}{(4\pi)}\right)^{1/8} (h_T)^{1/2} (\lambda)^{-1/4}. \qquad (10)$$

Результаты оценки дальностей обнаружения от ЭПР цели приведены на рис. 2.

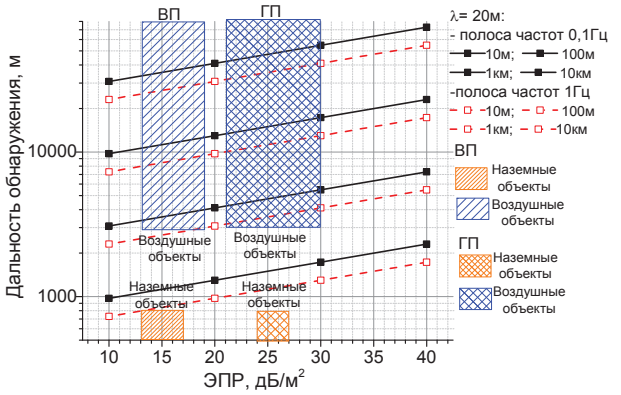


Рис. 2. Дальность обнаружения объектов при подсветке обстановки собственными радиостанциями КВ диапазона

При работе танков в группе идеология использования собственных средств радиосвязи состоит в последовательной подсветке обстановки каждым из танков группы своей радиостанцией, путем излучения в течение некоторого времени монохроматического или модулированного сигнала определенной частоты, которая может быть связана с номером этого объекта в группе, а также его положением в группе. Остальные радиостанции группы работают при этом на прием. Затем подсветку обстановки осуществляет следующая машина, а остальные работают на прием. Частота модуляции может использоваться для оценки разности времен (дальностей) между сигналом, прошедшим от источника подсветки до приемника и суммарной дальности между источником подсветки, целью и приемником.

При оценке дальности действия систем связи и радиолокации (7,10) значения мощности излучения, чувствительности приемника и реализуемые соотношения сигнал / помеха при заданной дальности связи использованы из табл. 3.

Использование для подсветки сигналов ГНСС (ГЛОНАСС, GPS, Galileo, Compass). Для освещения воздушной обстановки могут использоваться излучения глобальных навигационных спутниковых систем (ГНСС), как существующих в настоящее время российской и американской (ГЛОНАСС, GPS), так и появляющихся в будущем европейской и китайской (Galileo, Compass). В настоящем подразделе кратко изложена методика расчета дальности действия, разработанная в работах [15, 16].

Таблица 3

Технические характеристики танковых радиостанций

Радиостанция Р-030У УКВ диапазона		
1.	Диапазон частот	30-110 МГц
2.	Мощность	30 Вт ±5 Вт
3.	Нестабильность частоты	Не более $1\cdot10^{-6}$
4.	Девиация частоты	(5,6±1,2) кГц
5.	Уровень собственных шумов	130 дБ
6.	Чувствительность приемника	0,5 мкВ
7.	Соотношение сигнал/шум	12 дБ
8.	Дальность связи	20-30км
Радиостанция Р-163-50К КВ диапазона		
1.	Диапазон частот	2-30 МГц
2.	Мощность	50 Вт
3.	Нестабильность частоты	$4{,}5\cdot10^{-7}$
4.	Чувствительность приемника	3 мкВ
5.	Соотношение сигнал/шум	12дБ
6.	Дальность связи	50-300км

Для оценки уровня сигнала ГНСС P_{R0} на выходе стандартной антенны приемника потребителя с широкой диаграммой направленности и усилением G_{R0} можно использовать соотношение (2). Уровень сигнала должен составлять не менее P_{R0} [дБ]~ -161 дБ/Вт. Эта величина регламентирована в интерфейсных контрольных документах владельцев навигационных систем ГЛОНАСС и GPS. Это означает, что в месте отражения от объекта сигналы ГНСС на частотах L1 и L2 имеют мощность не менее -161 дБ/Вт на выходе линейно поляризованной антенны с коэффициентом усиления 3 дБ при углах возвышения более 5 градусов. В пересчете на плотность потока мощности это составляет $1{,}38*10^{-14}$ Вт/м^2. Чувствительность по поиску сигнала приемников ГНСС (Sr) на данный момент составляет -175 дБ/Вт при накоплении измерений сигнала на эпохе кода 1 мс и типовым коэффициентом усиления антенны от +5 дБ (в зените) до -2 на углах менее 15 градусов [16]. С использованием соотношения (1) можно записать дальность обнаружения для систем использующих для подсветки обстановки сигналы ГНСС:

$$R_r^2 < 4\cdot10^{-17}\cdot\frac{\sigma}{S_r}\cdot G_r. \qquad (11)$$

Результаты оценок дальности обнаружения [16], с использованием соотношения (11) для чувствительности приемника: S_r=-171 дБ/Вт - накопление измерений на интервале 1 мс, S_r =-181 дБ/Вт на 10 мс, S_r =-= 191 дБ/Вт на 100 мс, S_r =-201 дБ/Вт на 1 с и S_r =-= 211 дБ/Вт на 10 с и использовании ФАР с Δ = 1000 (30 дБ) приведены на рис. 3.

Анализ показывает:

а) использование ГНСС в качестве «подсвета» неприемлемо для локации динамичных объектов с малым ЭПР;

б) начиная с времени накопления более 1с локация возможна для объектов с большим ЭПР.

в) подобный тип подсветки бесперспективен для использования на объектах бронетехники для освещения воздушной и наземной обстановки.

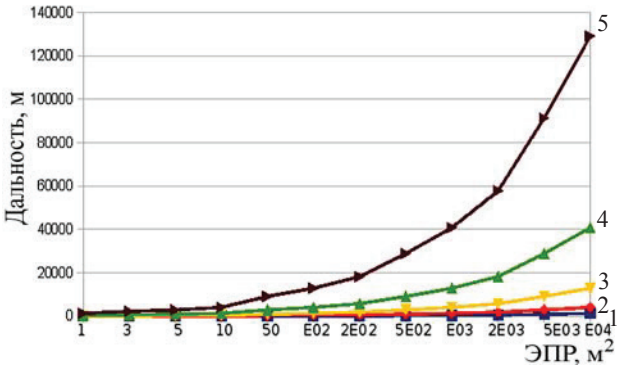


Рис. 3. Дальность радиолокации для различных времен накопления [16]: 1 – время накопления 1 мс; 2 – 10 мс; 3 – 100 мс; 4 – 1 с; 5 – 10 с Усиление приемной антенной решетки 20дБ

Используя приведенные в табл. 2 данные и результаты расчетов на рис. 1, 2, можно оценить дальности обнаружения различных объектов техники при их подсветке как вещательными станциями КВ диапазона, так и собственными радиостанциями, установленными на бронетехнике. Они показаны на рис. 1, 2. заштрихованными областями.

Было показано, что для высотных воздушных объектов дальности обнаружения могут составлять десятки километров. В тоже время наземные и низколетящие объекты могут обнаруживаться лишь на небольших дальностях в единицы километров.

Использование систем акустической разведки для обнаружения наземных и воздушных объектов. Возможность использования собственных акустических шумов объектов для их обнаружения подробно рассмотрена в работах [21, 22] и показано (табл. 4), что использование этого канала позволяет обнаруживать объекты (самолеты, танки, звук выстрела) в отсутствии помех от шума дождя и ветра на удалениях более 8 км. В то же время при дожде и ветре дальность обнаружения существенно снижается и в ряде случаев не превышает 1км.

3. КАНАЛЫ ОБМЕНА ИНФОРМАЦИЕЙ МЕЖДУ УЧАСТНИКАМИ СЦЕН, А ТАКЖЕ РУКОВОДСТВОМ

В настоящее время для обмена информацией между участниками ТЗ БТТ используются радиостанции – коротких волн (КВ) и ультракоротких волн (УКВ). Следующим этапом является автоматизация процесса передачи данных об обстановке между отдельными участниками сцены и командованием, создание автоматизированных систем отображения обстановки с учетом рисков для данного участника сцены.

Таблица 4

Расчетные дальности обнаружения для разных атмосферных условий и типов внешних помех [22]

	Самолет Jet			Вертолет Ми24			Выстрел		
	Влияние атмосферы и поверхности			Влияние атмосферы и поверхности			Влияние атмосферы и поверхности		
	Без помехи	шелест листвы	ветер, дождь	Без помехи	шелест листвы	ветер, дождь	Без помехи	шелест листвы	ветер, дождь
темп.=10, вл.=70%	>8 км	>8 км	1,76 км	>8 км	>8 км	0,9 км	>8 км	>8 км	7,45 км
темп.=20, вл.=70%	>8 км	>8 км	1,7 км	>8 км	>8 км	0,87 км	>8 км	>8 км	6,5 км
темп.=15, вл.=20%	7,3 км	5,7 км	1 км	7,7 км	5,93 км	0,66 км	>8 км	>8 км	3,4 км
	Влияние Атмосферы			Влияние Атмосферы			Влияние Атмосферы		
темп=10, вл=70%	>8 км	>8 км	1,88 км	>8 км	>8 км	0,89 км	>8 км	>8 км	>8 км
темп=20, вл=70%	>8 км	>8 км	1,77 км	>8 км	>8 км	0,86 км	>8 км	>8 км	>8 км
темп=15, вл=20%	>8 км	>8 км	0,95 км	>8 км	>8 км	0,63 км	>8 км	>8 км	8,1 км
	Enginework0800			Enginework2000			T-34		
	Влияние атмосферы и поверхности			Влияние атмосферы и поверхности			Влияние атмосферы и поверхности		
	Без помехи	шелест листвы	ветер, дождь	Без помехи	шелест листвы	ветер, дождь	Без помехи	шелест листвы	ветер, дождь
темп=10, вл=70%	>8 км	7,5 км	<0,5 км	>8 км	7,58 км	<0,5 км	>8 км	7 км	<0,5 км
темп=20, вл=70%	>8 км	6,4 км	<0,5 км	>8 км	=6,5 км	<0,5 км	>8 км	6,1 км	<0,5 км
темп=15, вл=20%	=6,4 км	4,3 км	<0,5 км	=5,9 км	=4 км	<0,5 км	=6,2 км	4 км	<0,5 км
	Влияние атмосферы			Влияние Атмосферы			Влияние Атмосферы		
темп=10, вл=70%	>8 км	>8 км	0,94 км	>8 км	>8 км	0,93 км	>8 км	>8 км	0,88 км
темп=20, вл=70%	>8 км	>8 км	0,91 км	>8 км	>8 км	0,9 км	>8 км	>8 км	0,85 км
темп=15, вл=20%	>8 км	>8 км	0,8 км	>8 км	>8 км	0,75 км	>8 км	>8 км	0,7 км

Для этого также могут использоваться штатные радиостанции, работающие в режиме автоматической передачи телеметрических данных. Кроме того необходимо отображение как задач, выполняемых соседями, так и технической готовности каждого из участников к их выполнению.

Интеграция в единую систему управления (ЕСУ) тактического звена (ТЗ) также резко сокращает проблему «дружественного огня». Точное определение по ЕСУ ТЗ координат собственной техники (используя ГНСС приемники) гарантирует, что танки группы не уничтожат случайно собственных коллег. Информационный обмен между объектами БТТ группы своих координат и разведанных координат противника позволяет повысить эффективность их боевого применения.

Приемники ГНСС позиционирования совместно с автоматизированной системой обмена информацией с командным пунктом и участниками ТЗ позволяет осуществлять обстрел противника по расчетным координатам его нахождения. Каждый участник ТЗ, обнаружив противника после определения его координат относительно собственных (используя лазерный дальномер и угломерные оптические системы), передает их в ЕСУ, которая распределяет по остальным участникам ТЗ, которые могут осуществлять их обстрел по расчетным координатам.

Примером подобного информационного обмена являются современные противокорабельные ракетные комплексы РФ [4, 5].

Очевидно, если противники имеют однотипные информационные системы с одинаковыми техническими возможностями, то у них будут одинаковы и вероятности выживания. Если же у одного из противников технические возможности систем разведки, наведение оружия, управления оружием и самого оружия лучше, то повышается и вероятность его выживания в конфликте. К аналогичному результату приводит и появление дополнительных информационных каналов, использующих другие физические поля, например, электромагнитные поля радиодиапазона или акустическое излучение объектов.

Пусть зависимости вероятностей обнаружения объектов противника от дальности различными системами (оптическими, инфракрасными, радиосистемами) примерно одинаковы. Тогда совместное их использование позволяет существенно расширить зону уверенного обнаружения противника, а значит и вероятность выживания. К такому же результату (расширению зоны обнаружения противника) может приводить использование дополнительной информации, полученной от других участников сцены.

4. ЭФФЕКТИВНОСТЬ КОМПЛЕКСИРОВАНИЯ СИСТЕМ, ИСПОЛЬЗУЮЩИХ РАЗЛИЧНЫЕ ФИЗИЧЕСКИЕ ПОЛЯ

При обнаружении сигнала со случайной начальной фазой и амплитудой вероятность обнаружения D и ложной тревоги F связаны соотношением [26]:

$$D = F^{\frac{1}{1+\mu}}, \quad (12)$$

где μ – соотношение сигнал-шум.

При обнаружении сигнала на фоне внутренних шумов приемной аппаратуры можно записать:

$$P_r = \frac{P_{Tr} G_{Tr} G_R \lambda^2 \sigma_T}{4\pi^3 R^4} V^4. \quad (13)$$

С учетом того, что:

$$\Pi = \frac{P_{Tr} G_{Tr} G_R \lambda^2 \sigma_T}{4\pi^3 P_N}, \quad (14)$$

где P_{Tr}, P_r – излучаемая и принятая мощности, ЭПР и дальность до цели, $G_{Tr} G_R$ – коэффициенты усиления передающей и приемной антенн, Π, P_N – потенциал РЛС и мощность шума на входе приемника, V – интерференционный множитель ослабления поверхности. Учитывая, что $P_r = \mu P_N$, можно записать соотношение сигнал-шум:

$$\mu = \Pi \frac{\sigma_T}{R^4} V^4. \quad (15)$$

Для высотных целей $V^4 \approx 1$, а для целей располагаемых вблизи поверхности раздела (наземных или надводных), а также вблизи от нее (маловысотных воздушных) $V^4 \approx \frac{1}{R^4}$, причем их высоты: $h_T <<= \frac{\lambda R}{4 h_R}$, где h_T, h_R высота цели и антенны РЛС.

Таким образом, соотношение сигнал /шум прямо пропорционально потенциалу системы, ЭПР цели и обратно пропорционально четвертой степени дальности для высотных объектов и восьмой степени для маловысотных или поверхностно расположенных.

В случае маловысотных или поверхностно расположенных целей чаще всего фактором, лимитирующим дальность их обнаружения, являются не внутренние шумы аппаратуры, а помехи от местных предметов – отражения от участков суши, моря или ясного неба.

Тогда с учетом выражений (12–15) можно записать:

$$D \approx F^{\frac{1}{1+\Pi \frac{\sigma_T}{R^4} V^4}}, \quad (16)$$

а значит, для высотных объектов оно имеет вид:

$$D = F^{\frac{1}{1+\Pi \frac{\sigma_T}{R^4} V^4}} \approx F^{\frac{R^4}{\Pi \sigma_T V^4}} \approx F^{\frac{R^4}{\Pi \sigma_T}}, \quad (17\ а)$$

а для маловысотных:

$$D \approx F^{\frac{R^8}{\Pi \sigma_T}}. \quad (17\ б)$$

Из соотношений (17) можно определить дальности R_0, на которых обеспечиваются заданные вероятности правильного обнаружения D_0 и ложной тревоги F_0 для высотных:

$$R_0 = \left(\Pi \sigma \frac{\ln(D_0)}{\ln(R_0)} \right)^{1/4}, \quad (18\ а)$$

и

$$R_0 = \left(\Pi \sigma \frac{\ln(D_0)}{\ln(R_0)} \right)^{1/8}, \quad (18\ б)$$

соответственно для маловысотных целей.

Тогда соотношения (16) могут быть записаны в виде:

$$D = D_0^{x^{4m}}, \quad (19)$$

где m=1 для высотных целей, m=2, а $x = \frac{R}{R_0}$ – относительная дальность. На рис. 4 показан характер зависимости вероятностей обнаружения от дистанции (рис. 4, а) для двух фиксированных вероятностей обнаружения (=0,5 и 0,9) и дальностей обнаружения от потенциала системы и ЭПР обнаруживаемого объекта (рис. 4, б). Из рис. 4 следует, зависимость вероятности обнаружения является монотонно убывающей функцией дальности и, в большинстве случаев, при практических расчетах можно использовать ее аппроксимацию, в виде ступенчатой функции с постоянным значением от нулевых дальностей до дальностей, когда вероятность обнаружения равна 0,9 и считая ее равной нулю на больших дальностях. Это будет давать при расчетах несколько заниженные данные.

Для реальных систем разведки, а также вооружений, как правило, зависимости вероятностей обнаружения и поражения от дистанции до цели неизвестны.

В лучшем случае, в ходе испытаний могут определяться дальности, на которых реализуются заданные вероятности обнаружения (обычно 0,9 или 0,99) и заданные вероятности поражения объектов системами вооружения.

Соотношение (19) может быть переписано в виде:

$$D = D_0^{\left(\frac{R}{R_0}\right)^{4m}}, \quad (19\ а)$$

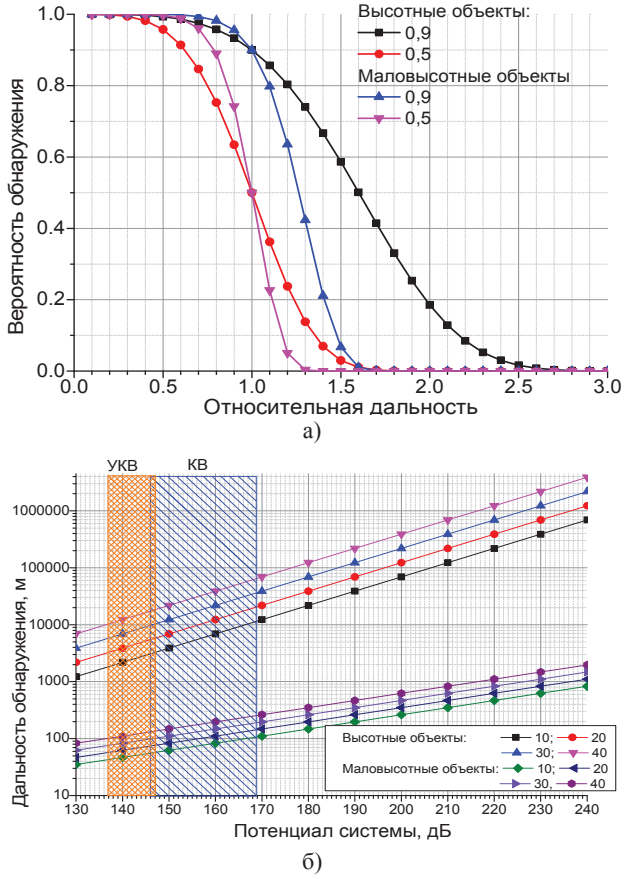


Рис. 4. Зависимости вероятности обнаружения флуктуирующего сигнала от дальности (а) и дальности обнаружения от потенциала системы и ЭПР целей (10дБ/м^2, 20дБ/м^2, 30 дБ/м^2, 40дБ/м^2) для высотных и маловысотных объектов

удобном, для дальнейших расчетов. В него входят заданные вероятности обнаружения D_0 на дальности для высотных m=1 и маловысотных m=2 объектов. Будем полагать, что аналогичным соотношением (19а) описывается и вероятность поражения объекта системой вооружения при m=1. При этом под R_0 дальность поражения противника с вероятностью D_0.

В случае, если используется несколько датчиков контроля обстановки (оптические, радиоволновые, акустические) и несколько систем вооружения (артиллерийская, ракетная), то при статистической независимости получаемых ими результатов, вероятности уничтожения P_d^k и не уничтожения P_d^k k-го противника определяются

$$P_d^k = P_{det}^k P_{dest}^k, \qquad (20\ а)$$

$$P_d^k = 1 - P_{det}^k P_{dest}^k, \qquad (20\ б)$$

через вероятность обнаружения k-го объекта противника датчиками освещения обстановки P_{det}^k и вероятность уничтожения k-го противника системами вооружения P_{dest}^k. Последние определяются

$$P_{det}^k = 1 - \Pi_{i=1}^{i=i_0}\left(1 - P_{det}^{k_i}\right), \qquad (21\ а)$$

$$P_{dest}^k = 1 - \Pi_{j=1}^{j=j_0}\left(1 - P_{dest}^{k_j}\right), \qquad (21\ б)$$

через вероятности обнаружения k-го объекта противника i_0 датчиками освещения обстановки $P_{det}^{k_i}$ и вероятности уничтожения k-го противника j_0 системами вооружения $P_{dest}^{k_j}$.

Соотношения (19–21) позволяют оценить эффективность комплексного использования датчиков освещения обстановки различных типов и систем вооружения.

Вероятность успешного выполнения задачи P_{01} своим объектом, в случае наличия одного объекта противника k=1 будет определяться через произведение вероятностей поражения P_d^1 объекта противника и не поражения P_d^0 им (20):

$$P_{01} = P_d^1 \cdot P_d^0 = P_d^1\left(1 - P_d^0\right), \qquad (22\ а)$$

где индексы 0 и 1 относятся к своему объекту и объекту противника.

Аналогичным образом определиться успешное выполнение задачи объектом противника:

$$P_{10} = P_d^0 \cdot P_d^1 = P_d^0\left(1 - P_d^1\right). \qquad (22\ б)$$

Можно ввести понятие функционала эффективности, характеризующего насколько вероятность уничтожения противника в дуэльной схватке двух объектов, при условии сохранения живучести своего объекта, больше вероятности уничтожения противником вашего объекта, при условии сохранения живучести объектом противника, определится из соотношений (22) как:

$$\Delta = P_{01} - P_{10} = P_d^1 \cdot P_d^0 = P_d^1\left(1 - P_d^0\right) - P_d^0\left(1 - P_d^1\right) =$$

$$= P_d^1 - P_d^0. \qquad (23\ а)$$

И будет равен разности вероятности уничтожения своим объектом объекта противником и вероятности уничтожения противником своего объекта. С использованием (20а) можно записать:

$$\Delta = P_{det}^1 P_{dest}^1 - P_{det}^0 P_{dest}^0 =$$

$$= \left(\Delta_{det} + P_{det}^0\right)\left(\Delta_{dest} + P_{dest}^0\right) - P_{det}^0 P_{dest}^0 =$$

$$= \Delta_{det} P_{dest}^0 + \Delta_{dest} P_{det}^0 + \Delta_{det}\Delta_{dest}, \qquad (23\ б)$$

где $\Delta_{det} = P_{det}^1 - P_{det}^0$, а $\Delta_{dest} = P_{dest}^1 - P_{dest}^0$ разница вероятностей обнаружения датчиков своего объекта и противника, а также разности вероятностей пораже-

ния системами вооружения своего объекта и противника.

Из соотношения (23 б)следует, что обеспечение более высоких вероятностей обнаружения $\Delta_{det} > 0$ датчиками обстановки, чем это достигается противником и больших вероятностей уничтожения $\Delta_{dest} > 0$ его приводит к возрастанию значений функционала качества выполнения задачи $\Delta > 0$.Из соотношений (21) следует, что дополнение системы обнаружения дополнительным датчиком обстановки или системы вооружения дополнительной системой оружия приводит к возрастанию вероятности обнаружения противника и вероятности его уничтожения:

$$P_{det}^{k,i_0+1} - P_{det}^{k,i_0} = \Pi_{i=1}^{i=i_0}\left(1-P_{det}^{k_i}\right) - \Pi_{i=1}^{i=i_0+1}\left(1-P_{det}^{k_i}\right) =$$

$$= P_{det}^{k,i_0+1}\Pi_{i=1}^{i=i_0}\left(1-P_{det}^{k_i}\right), \qquad (24\ а)$$

$$P_{dest}^{k,j_0+1} - P_{dest}^{k,j_0} = \Pi_{j=1}^{j=j_0}\left(1-P_{dest}^{k_j}\right) - \Pi_{j=1}^{j=j_0+1}\left(1-P_{dest}^{k_j}\right) =$$

$$= P_{dest}^{k,j_0+1}\Pi_{j=1}^{j=j_0}\left(1-P_{dest}^{k_j}\right), \qquad (24\ б)$$

на величины пропорциональные вероятностям обнаружения реализуемым добавленным датчиком обстановки и вероятностям поражения противника, реализуемым добавленной системой вооружения.

Таким образом, появление у противника дополнительны датчиков контроля обстановки и новых систем вооружения позволяет ему более успешно решать поставленные задачи. Поэтому для повышения живучести собственных объектов необходимо использование большего, чем у противника количества каналов получения информации о внешней обстановке, и улучшения их характеристик, а также применение дополнительных систем вооружения и увеличение дальности действия старых систем вооружения.

В табл. 5 приведены дальности действия (обнаружения с вероятностями более 0,9) существующих и перспективных датчиков обстановки, а в табл. 6 дальности действия различных систем вооружения и сопряженных с ними систем наведения.

В качестве примера оценены функционалы эффективности при дуэльной схватке танков России Т-90 и США – Абрамс для двух ситуаций:

Танки имеют примерно одинаковое артиллерийское вооружение и средства управления огнем, а также комплексы активной защиты. Отличие состоит в применении различных систем ПТУР («Корнет» и «Джавелин»), причем дальность поражения первого боле чем в 3 раза превышает аналогичную характеристику второго.

В другом варианте будет рассмотрено влияние на эффективность боевого применения Абрамса дополнительно активно-пассивной системы разведки КВ

Таблица 5

Дальности действия датчиков обнаружения

Датчики	Оптические ТПКУ-2Б, ТКН-3 [19]	ИК ТКН-3 [19]	РТС КВ и УКВ диапазонов [14]		Пассивные акустические РТС [21, 22]	
Объекты	день	ночь	Активные	Активно-пассивные	тихо	Ветер, дождь
Наземные (БТТ, автомобили)	3,0км;4,0км	0,4 км	0,4…1,0 км	0,3…0,7км	6,0км	0,5км
Воздушные (самолеты, вертолеты)	-	-	2…20км	1…3км	7.3км	0,7км
Выстрел	-	-	-	-	8км	3,4км
БПЛА	-	-	1...8 км	0,5…1,5 км	6,0 км	-

Таблица 6

Дальность действия систем оружия и прицелов

Название	Страна	Источник	Дальность	Высота	Применение
Верба (Индекс ГРАУ 9К333, ракета 9М336)	Россия	27	≥6км	≥4км	Самолеты, вертолеты, БПЛА, ракеты
FIM-92 «Стингер»	США	28	4,8км	0,18-3,8км	Самолеты. вертолеты
Стрела-10 (SA-13 Gopher)	СССР	29	5км	0,025-3,5км	
«Корнет» (Индекс ГРАУ — 9К135, АТ-14 Spriggan)	СССР	30	10км	9км	БТТ, самолеты, вертолеты со скоростью до 250м/с
ПТРК FGM-148 Javelin	США	31	0,05…2,5км	-	БТТ
Артиллерийские системы танков с прицелами ПП-61 АМ и 1П3-2 с тепловизором «Буран-М» с тепловизором «Эсса»	СССР Россия	 19 32	 2,0км /1,8км /4,0км	-	БТТ
Артиллерийское вооружение танка Абрамс: М1А1 М1А2	США	32	 0,2…4,0км 0,2…5,0км		БТТ

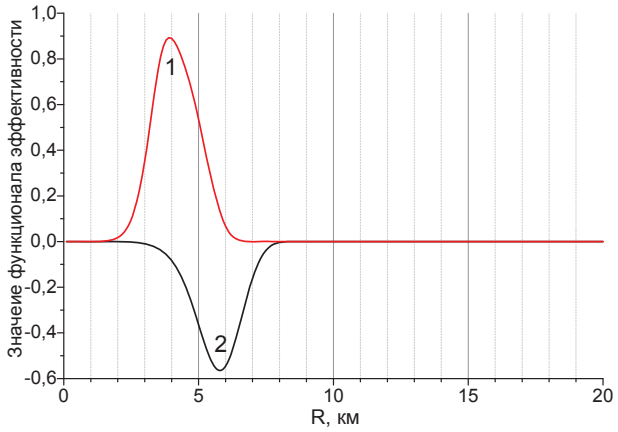


Рис. 5. Влияние на боевую эффективность БТТ Абрамс использования дополнительных каналов освещения обстановки: 1- Т-90 и Абрамс со стандартными системами вооружения и оптическими системами наблюдения и прицеливания; 2- Абрамс с дополнительными системами акустической разведки и целеуказания

диапазона, а также пассивной системы акустической разведки. Оценки для обоих вариантов комплектования объектов БТТ средствами вооружения и анализа обстановки проведены с использованием соотношений (19а, 21–23) и представлены на рис.5.

Видно, что если в первом случае преимущество Т-90 за счет использования более эффективной системы ПТРК является неоспоримым, то появление у Абрамса дополнительного канала акустической разведки и целеуказания, имеющего существенно большие дальности обнаружения объектов в безпомеховой обстановке, приводит к тому, что эффективность Абрамса становится выше, чем Т-90.

Кроме того из рис. 6 видно, что для каждого набора вооружений и датчиков обстановки существуют дальности, на которых их применение дает наибольшие преимущества перед противником. Так, при стандартном наборе Т-90 обладает наибольшими преимуществами перед Абрамсом на дистанциях около 4 км, в то время как Абрамс, с дополнительным набором датчиков обстановки, обладает наибольшими преимуществами перед Т-90 на дистанциях около 6 км.

ЗАКЛЮЧЕНИЕ

1. Для трансформации современных боевых платформ и системы их управления в современную пространственно распределенную интеллектуальную смарт-грид сеть необходимо их объединение автоматизированными системами обмена информацией с указанием приоритетности и степени опасности отдельных элементов обстановки для каждой из платформ. Система передачи телеметрической информации об обстановке может быть построена на основе имеющихся на объектах техники КВ и УКВ радиостанций.

2. Для повышения надежности и живучести распределенной интеллектуальной сети информационные датчики отдельных платформ необходимо строить, используя поля различной физические природы (электромагнитные и акустические), разных диапазонов длин волн (от сотен нанометров для оптического диапазона до десятков метров – для радиодиапазона и акустических волн). Кроме того необходимо применять различные методы зондирования окружающей среды как активные с излучением специальных сигналов, так и активно-пассивные – основанные на приеме вторичных полей создаваемых отражение от объектов техники существующих источников излучения наземного и космического базирования, а также пассивные – основанные на использовании собственных оптических, тепловых и акустических излучений объектов техники. Это позволит повысить информативность каналов поступления информации об обстановке и живучесть самих объектов техники в условиях воздействия на них противной стороны.

3. В дополнение к применяемым на объектах БТТ оптическим и инфракрасным системам, необходимо использовать акустические средства разведки и целеуказания, которые могут обеспечить обнаружение объектов техники (наземной и воздушной) и вооружений противника на удалениях до 10 км.

4. Для получения информации об окружающей обстановке могут использоваться вторичные поля, создаваемые объектами техники противника при отражении сигналов подсветки вещательных станций КВ диапазона, спутниковых и наземных систем телевидения и вещания. Их использование может позволить обнаруживать движущиеся объекты наземной и воздушной техники на удалениях в единицы километров.

5. Необходимо создание автоматизированных каналов обмена информацией между отдельными участниками сцены, а также командованием, и систем отображения информации как собственных датчиков, так и полученной от других участников сцены и командования с указанием потенциальной степени опасности, а также пассивные – основанные на приеме собственного излучения объектов в оптическом, инфракрасном диапазонах электромагнитных волн, а также собственных акустических шумов объектов военной техники.

6. Использование для подсветки обстановки излучений вещательных КВ станций и собственных радиостанций объектов бронетехники может позволить обнаруживать высотные воздушные цели на удалениях свыше 10 км.

7. Комплексирование систем обнаружения, использующих физические поля различных диапазонов и природы позволяет повысить вероятность обнаружения средств противника, а значит и эффективность борьбы с ними.

8. Построение роботизированных комплексов вооружения встроенных в смарт-грид систему распределенного интеллекта позволит повысить их жи-

вучесть и эффективность применения в условиях противодействия противнику.

Литература

[1] *Кравченко В.Ф.* Смарт грид технологии - основа модернизации системы водоснабжения / В.Ф. Кравченко, Е.В. Кривенко, С.А. Левченко, В.И. Луценко, С.В. Плюта // Доклады Национальной Академии Наук Беларуси, Технические Науки 2015, Май-Июнь, Т. 59, №3. – С. 102–108.

[2] *Кравченко В.Ф.* Смарт грид технология - основа модернизации системы водоснабжения для будущего устойчивого развития общества / В.Ф. Кравченко, Е.В. Кри-венко, С.А. Левченко, В.И. Луценко // Физические основы приборостроения 2015. – Т. 4, № 1. – С. 12–29.

[3] NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0. Февраль 2012. Авторы: NIST (Национальный институт технологий и стандартизации, США), Государственный коммерческий департамент США. Концепция и дорожная карта по стандартам взаимодействия для Smart Grid.

[4] Крылатая противокорабельная ракета П-700 Гранит (3М-45) / Информационно - новостная система «Ракетная техника» // Электронный ресурс http://rbase.new-factoria.ru/missile/wobb/granit/granit.shtml.

[5] Противокорабельная ракета Яхонт (Оникс) / Информационно - новостная система «Ракетная техника» // Электронный ресурс http://rbase.new-factoria.ru/missile/wobb/jakhont/jakhont.shtml

[6] Танк Т-14 "Армата" или Т-99 "Приоритет" / Новости ВПК // Электронный ресурс http://vpk.name/library/f/armata.html

[7] *Бирюков И.Ю.* Анализ приоритетов систем наземной разведки по обнаружению объектов вооружения и военной техники / И.Ю. Бирюков, Ю.М. Бусяк, А.В. Шульга // Інженерні, технічні, програмні засоби, комплекси та системи**,** Збірник наукових праць Національної академії Національної гвардії України. 2015. Вип. 2 (26). – С. 81–87.

[8] Информационные технологии создания пространственно-временных модемов многопозиционных активно-пассивных радиолокационных систем / Ю.Н. Седышев, В.А. Тютюнник // Прикладная радиоэлектроника. – 2015. – Т. 14, № 1. – С. 105–110.

[9] *Лобочко С.Е.* Построение системы обнаружения с использованием излучения УКВ и ТВ–передатчиков / С.Е. Лобочко // Международная научная конференция «Излучение и рассеяние ЭМВ» ИРЭМВ*2003, труды конференции, Таганрог, 2003. – С. 287–290.

[10] *Луценко И.В.* Бистатические РЛС с подсветкой ионосферными сигналами связных станций коротковолнового диапазона / И.В. Луценко, И.В. Попов, В.И. Луценко // Радиофизика и электроника: Сборник научных трудов / НАН Украины. Ин-т радиофизики и электроники им. А. Я. Усикова. – Харьков.- 2007. – Т.12, №1. – С. 193–204.

[11] *Lutsenko I.V.* Illumination of Air Environment Using Radiation of SW Broadcasting stations / I.V. Lutsenko, V.I. Lutsenko, I.V. Popov // The 5-th European Radar Conference, 30–31 October 2008: conf. proceedings.- Amsterdam, 2008. – P. 396–399.

[12] *Попов И.В.* Освещение воздушной обстановки с использованием излучения вещательных станций КВ диапазона / И.В. Попов, В.И. Луценко, И.В. Луценко. // "Современные проблемы радиоэлектроники" Сборник научных трудов. Под редакцией Громыко А. И., Сарафанова А. В. ; М. Радио и связь. 2006. – С. 25–28.

[13] *Вичкань А.В.* Пассивная когерентная радиолокация в коротковолновом диапазоне. Часть 1. Обнаружение воздушных целей. / А.В. Вичкань, П.А. Мельяновский, А.И. Шуть // Радиофизика и электроника. – 2010. – Т. 15, №1. – С. 72–77.

[14] *Луценко В.И.*, Мониторинг воздушной обстановки с использованием излучения вещательных станций коротковолнового диапазона / В.И. Луценко, И.В. Луценко, И.В. Попов// Изв. Вузов Радиофизика. – 2015. – Т. 58, № 1. – С. 10–20

[15] *Лауш А.Г.* Использование излучений глобальных навигационных спутниковых систем для решения задач радиолокации и дистанционного зондирования / А.Г. Лауш, В.И. Луценко, И.В. Луценко, Д.О. Попов // 2014 24th Int. Crimean Conference “Microwave & Telecommunication Technology” (CriMiCo’2014). 7–13 September, Sevastopol, Crimea, Russia P. 1149–1150.

[16] *Лауш А.Г.* Использование излучений глобальных навигационных спутниковых систем для решения задач радиолокации / А.Г. Лауш, В.И. Луценко, И.В. Луценко // Известия высших учебных заведений. Радиоэлектроника, Том 58, № 11 (2015). – С. 14–26

[17] *Красько А.С.* Поддержка принятия решений по обеспечению общественной безопасности на городских территориальных объектах на основе оперативного анализа аудиоинформации: автореф. дис. на соискание научн. степени кандидата технических наук: спец. 05.13.10 – Управление в социальных и экономических системах / А.С. Красько. – Уфа, 2011. – 16 с.

[18] *Смирнов В.* Маскировка подвижных наземных объектов в современных условиях // Электронный ресурс.- http://samlib.ru/s/smirnow_wasilij/masikirovka.shtml. – 2013.

[19] *Мокрушин Д.* Акустические системы обнаружения / Д. Мокрушин // Электронный ресурс. - http://twower.livejournal.com/502014.html?thread=14595326.

[20] *Луценко В.И.* Дальность действия и разрешающая способность пассивных акустических систем разведки / В.И. Луценко, И.В. Луценко, А.В. Соболяк //5-й международный радиоэлектронный форум «Прикладная радиоэлектроника. Состояние и перспективы развития» МРФ-2014 14-17-октября 2014г.: сб. научн. трудов МРФ-2014. – Т.1 «Интегрированные информационные радиоэлектронные системы и технологии».- Харьков. – 2014. – С.41–44.

[21] *Луценко В.И.* Пассивные акустические системы разведки, дальность их действия и разрешающая способность / В.И. Луценко, И.В. Луценко, А.В. Соболяк // Інтегровані технології та енергозбереження, щоквартальний науково-технічний журнал. Харків: НТУ «ХПІ»,. – 2014, № 3. – С. 60–64.

[22] *Луценко В.И.* Дальность действия систем акустической разведки / В.И. Луценко, И.В. Луценко, А.В. Соболяк // Прикладная радиоэлектроника, 2015. – Том 14, № 2. – С. 125–136.

[23] *Кравченко В.Ф.* Рассеяние радиоволн морем и обнаружение объектов на его фоне / В.Ф. Кравченко, В.И. Луценко, И.В. Луценко // М. Физматлит, 2015. – 448 с.

[24] *Луценко В.И.* Об эффектах, которые могут приводить к возрастанию ЭПР малоразмерных объектов в декамет-

ровом диапазоне / В.И. Луценко, И.С. Тургенев, С.И. Хоменко // Радиофизика и электроника: Сборник научных трудов / НАН Украины. Ин-т радиофизики и электроники им. А. Я. Усикова. – Харьков. – 1997. – Т. 2, № 1. – С. 60–63.

[25] *Lutsenko V.I.* Frequency Dependences of Scattering Matrices in the Resonance Domain / V.I. Lutsenko, S.Y. Tolstel. // Telecommunication and Radio Engineering. – 2001. – V. 55, № 4. – P. 33–39.

[26] Теоретические основы радиолокации. / Под ред. Я. Д. Ширмана. – М.: Сов. радио, 1970. – 559 с.

[27] Верба (ПЗРК) [Электронный ресурс] // Википедия — свободная энциклопедия. – Режим доступа: https://ru.wikipedia.org/wiki/%D0%92%D0%B5%D1%80%D0%B1%D0%B0_(%D0%9F%D0%97%D0%A0%D0%9A).

[28] «Верба» против «Стингера»: новейший российский ПЗРК не имеет аналогов в мире [Электронный ресурс] // Медиагруппа «Звезда». – Режим доступа: https://tvzvezda.ru/news/forces/content/201506200927-cnrm.htm.

[29] Стрела-10 [Электронный ресурс] // Википедия — свободная энциклопедия. – Режим доступа: https://ru.wikipedia.org/wiki/%D0%A1%D1%82%D1%80%D0%B5%D0%BB%D0%B0-10.

[30] Корнет (ПТРК) [Электронный ресурс] // Википедия — свободная энциклопедия. – Режим доступа: https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D1%80%D0%BD%D0%B5%D1%82_(%D0%9F%D0%A2%D0%A0%D0%9A).

[31] Противотанковый ракетный комплекс FGM-148 Javelin [Электронный ресурс] // Информационно - новостная система «Ракетная техника». - Режим доступа: http://rbase.new-factoria.ru/missile/wobb/javelin/javelin.shtml.

[32] Танк M1A2 Абрамс ТТХ [Электронный ресурс] // Оружие. Вооружение России и мира. - Режим доступа: http://oruzhie.info/tanki/51-m1a2-abrams.

Поступила в редколлегию 18.12.2017

Луценко Владислав Иванович, доктор физ.-мат. наук, старший научный сотрудник, старший научный сотрудник, Институт радиофизики и электроники им. А.Я. Усикова НАН Украины. Область научных интересов: распространение и рассеяние радиоволн, дистанционное зондирование природных сред, радиолокация.

Луценко Ирина Владиславовна, канд. физ.-мат. наук, старший научный сотрудник, Институт радиофизики и электроники им. А.Я. Усикова НАН Украины. Область научных интересов: дистанционное зондирование тропосферы Земли с использованием излучения наземных и спутниковых радиосистем, исследование обратного рассеяния радиоволн СВЧ и КВЧ подстилающими поверхностями, гидрометеорами и антропогенными образованиями.

Соболяк Александр Васильевич, начальник отдела электрооборудования, Государственное предприятие «Харьковское конструкторское бюро по машиностроению им. А.А. Морозова». Область научных интересов: радиолокация, разработка радиотехнических систем и комплексов в акустическом и радиодиапазонах.

УДК 621.396.96:621.271.029.65

Використання смарт-грід технологій для підвищення ефективності застосування об'єктів наземної техніки / В.І. Луценко, І.В. Луценко, О.В. Соболяк // Прикладна радіоелектроніка: наук.-техн. журнал. – 2017. – Том 16, № 3, 4. – С. 134–146.

Розглянуто можливість побудови інтелектуальних мереж з окремих об'єктів наземної техніки і за рахунок цього підвищення ефективності їх застосування та живучості. Особливе значення має підвищення інформативності каналів отримання інформації про зовнішню обстановку шляхом об'єднання інформаційних потоків каналів, що використовують різні фізичні поля (акустичні, електромагнітні тощо). Оцінені дальності виявлення для різних датчиків і результат, одержуваний від їх комплексування.

Ключові слова: смарт-грід технології, інтелектуальні мережі, об'єкти наземної техніки.

Табл.: 06. Іл.: 05. Бібліогр.: 32 найм.

UDC 621.396.96:621.271.029.65

Using smart grid technologies to improve the efficiency of application of ground-based equipment objects / V.I. Lutsenko, I.V. Lutsenko, A.V. Sobolyak // Applied Radio Electronics: Sci. Journ. – 2017. – Vol. 16, № 3, 4. – P. 134–146.

The possibility of constructing intelligent networks from separate objects of ground-based equipment and at the expense of this increasing the efficiency of their application and survivability is considered. Of particular importance is the increase in the information content of channels for obtaining information about the external situation by combining information flows of channels using different physical fields (acoustic, electromagnetic ones etc.). The detection ranges for various sensors and the result obtained from their integration are estimated.

Keywords: smart grid technologies, intelligent networks, ground-based equipment objects.

Tab.: 06. Fig.: 05. Ref.: 32 items.

УДК 19.66:519.668

ВЫЧИСЛЕНИЕ ЗНАЧЕНИЙ ЭЛЕМЕНТАРНЫХ И СПЕЦИАЛЬНЫХ ФУНКЦИЙ С ИНТЕРВАЛЬНО ЗАДАННЫМ АРГУМЕНТОМ, ОПРЕДЕЛЁННЫМ В СИСТЕМЕ ЦЕНТР-РАДИУС

В. Ю. ДУБНИЦКИЙ, А. М. КОБЫЛИН, О. А. КОБЫЛИН

Предложены алгоритмы для вычисления значений элементарных функций, аргументы которых представлены интервальными числами, определёнными в системе центр-радиус. Алгоритмы реализованы в специализированном программном калькуляторе, позволяющем вычислять интервальные значения степенной, показательной, логарифмической функции, прямых и обратных тригонометрических функций, прямых и обратных гиперболических функций, гамма-функции, неполной гамма-функции, бета-функции и дигамма-функции.

Ключевые слова: элементарные функции, интервальные числа, определенные в системе центр-радиус, специализированный программный калькулятор, степенная функция, показательная функция, логарифмическая функция, прямые и обратные тригонометрические функции, прямые и обратные гиперболические функции, гамма-функция, неполная гамма-функции, бета-функция, дигамма-функция.

ВВЕДЕНИЕ

Задача вычисления значений элементарных функций исторически стала одной из первых задач, решённых на компьютерах [1]. С тех пор и до сегодняшнего дня она остается актуальной так, как методы её решение существенно зависят от непрерывно меняющейся архитектуры компьютеров. Подробно эти методы рассмотрены в работах [2–6]. Главная особенность этих работ, с точки зрения авторов данного сообщения, в том, что в них для вычисления значений элементарных и специальных функций использована традиционная эвклидова арифметика. Использование интервально заданных чисел в указанных работах не рассмотрено.

Понятие интервального числа и теоретические основы интервального анализа для решения прикладных задач рассмотрены в работах [7–10]. В работе [10] введено представление интервального числа в системе центр-радиус и определены правила действий с такими числами.

Следуя этой работе, рассмотрим множество действительных чисел R, на котором определим интервальное число A в виде замкнутого интервала:

$$\mathrm{A}=\left(\underline{a},\overline{a}\right)=(a_1,a_2),\ \underline{a}\le\overline{a};\ a_1\le a_2, \tag{1}$$

и представим в виде:

$$A=\left\langle a,r_a\ \right\rangle, \tag{2}$$

где

$$a=\frac{a_1+a_2}{2},\ r_a=\frac{a_2-a_1}{2},\ a,r_a,\in R. \tag{3}$$

При применении системы центр-радиус действия сложения и вычитания с интервальными числами выполняют по следующим правилам:

$$A+B=\left\langle a+b,r_a+r_b\ \right\rangle; \tag{4}$$

$$A-B=\left\langle a-b,r_a+r_b\ \right\rangle. \tag{5}$$

В рамках данной работы примем, что границы интервалов, которые ограничивают рассматриваемые числа, образованы вычислительными ошибками, погрешностями измерений или неполным знанием области изменения некоторой физической величины. Поэтому в условии (2) должны быть выполнены неравенства:

$$a\ge r_a\ge 0,\ b\ge r_b\ge 0, \tag{6}$$

иначе будем считать, что задача, в рамках наших представлений об исследуемом объекте, физического смысла не имеет. В работе [10] предложены формулы для выполнения операции деления и умножения в системе центр-радиус в виде:

$$\left\langle a,r_a\right\rangle\left\langle b,r_b\right\rangle=\left\langle ab+r_ar_b,ar_b+br_a\right\rangle; \tag{7}$$

$$\frac{\left\langle a,r_a\right\rangle}{\left\langle b,r_b\right\rangle}=\left\langle\frac{ab+r_ar_b}{b^2-r_b^2},\frac{ar_b+br_a}{b^2-r_b^2}\right\rangle. \tag{8}$$

Для возведения в целочисленную степень в работе [10] приведены формулы:

$$A^n=\left\langle a,r_a\right\rangle^n=\left\langle G,R\right\rangle; \tag{9}$$

при условии, что $n\in Z$. Тогда:

$$G=\sum_{k=0}^{n}C_n^{2k}r_a^{2k}a^{n-2k};$$

$$R=\sum_{k=0}^{n}C_n^{2k+1}r_a^{2k+1}|a|^{n-(2k+1)}. \tag{10}$$

Для программирования процесса вычислений условие (9) представим, с учетом условия (10), в виде:

$$A=\langle a;r_a\ \rangle^n=\left\langle a^2+r_a^2;2|a|r_a\right\rangle\underbrace{\left(\left(a;r_a\right)\ldots\left(a;r_a\right)\right)}_{n-2}. \quad (11)$$

В работе [9] модуль интервального числа $A=\left(\underline{a},\overline{a}\right)$ определён так:

$$\mathrm{mod}(A)=\max\left\{\left(a-r_a\right),\left(a+r_a\right)\right\}. \quad (12)$$

Для определения значений элементарных функций с интервально заданным аргументом в работах [9, 10, 11] применено их разложение в ряд Тейлора. Такой подход, по нашему мнению, требует отсутствующего в настоящее время строгого обоснования понятий предельного перехода и сходимости для функциональных рядов, численные значения аргументов которых заданы в интервальном виде.

1. ПОСТАНОВКА ЗАДАЧИ

Разработка и программная реализация методов вычисления значений элементарных и специальных функций на основе их многочленных и рациональных аппроксимаций, при условии, что численные значения аргументов есть интервальные числа, заданные в системе центр-радиус. В рамках данной работы к элементарным функциям отнесены степенная функция, логарифмическая функция, прямые и обратные тригонометрические функции, прямые и обратные гиперболические функции. К специальным функциям отнесены гамма-функция, неполная гамма-функция, бета-функция и дигамма-функция.

2. ВЫЧИСЛЕНИЯ ЭЛЕМЕНТАРНЫХ ФУНКЦИЙ

Рассмотрим процедуры вычисления элементарных функций при условии, что численные значения аргументов есть интервальные числа, заданные в системе центр-радиус.

Рассмотрим основные арифметические операции в том случае, когда один из операндов – постоянное число. В системе центр-радиус, используя условия (2, 3), постоянное число C представим в виде $C=\langle c,\ 0\rangle$. Примем, что $A=\langle a,r_a\rangle$ и $B=\langle b,0\rangle$. Тогда операции сложения и вычитания представим в виде:

$$A+B=\langle a+b,r_a\ \rangle; \quad (13)$$

$$A-B=\langle a-b,r_a\ \rangle. \quad (14)$$

Для умножения интервального числа, представленного в системе центр-радиус, на постоянную величину примем, что:

$$AB=\begin{cases}\langle a,0\rangle\langle b,r_b\rangle, A=const, B\neq consn;\\ \langle a,r_a\rangle\langle b,0\rangle, A\neq const, B=const.\end{cases} \quad (15)$$

При операции деления интервального числа на постоянное число получим, что:

$$\frac{A}{B}=\frac{\langle a,r_a\rangle}{\langle b,0\rangle}=\left\langle\frac{ab}{b^2},\frac{br_a}{b^2}\right\rangle=\left\langle\frac{a}{b},\frac{r_a}{b}\right\rangle; \quad (16)$$

или

$$\frac{A}{B}=\frac{\langle a,0\rangle}{\langle b,r_b\rangle}=\frac{\langle ab,ar_b\rangle}{b^2-r_b^2}=\left\langle\frac{ab}{b^2-r_b^2},\frac{ar_b}{b^2-r_b^2}\right\rangle. \quad (17)$$

Следуя работе [3, С.78], и принимая во внимание ранее введенные обозначения, представим логарифмическую функцию в виде:

$$\ln\langle x,r_x\rangle=$$

$$=\sum_{i=1}^{6}\langle a_i,0\rangle\left[\langle -1;0\rangle^{i-1}+\frac{\langle 1;0\rangle}{\langle x,r_x\rangle^i}\right]\frac{\left(\langle x,r_x\rangle-\langle 1;0\rangle\right)^i}{\langle i;0\rangle}. \quad (18)$$

Далее при описании вычислительных алгоритмов, во избежание недоразумений, связанных с использованием десятичных дробей, вместо символа $\langle a,r_a\rangle$ будем использовать символ $\langle a;r_a\rangle$.

Коэффициенты a_i, необходимые для вычисления величины $\ln\langle x,r_x\rangle$, приведены в табл.1.

Таблица 1

Значение коэффициентов для приближения функции $\ln(x)$

a_1	0,500000	a_4	0,030303
a_2	0,227273	a_5	0,007576
a_3	0,090909	a_6	0,0001082

Произвольную показательную функцию, используя работу [3, С. 49], представим в виде:

$$a^x=\sum_{k=0}^{\infty}\frac{(x\ln a)^k}{k!}. \quad (19)$$

Тогда, с учетом условия (18), её интервальным расширением будет функция вида:

$$\langle a;r_a\rangle^{\langle x;r_x\rangle}=\sum_{k=0}^{6}\frac{\left(\langle x;r_x\rangle\ln\langle a;r_a\rangle\right)^k}{k!}. \quad (20)$$

Экспоненту с отрицательным показателем, точнее её рациональное приближение, следуя работе [3, С. 63], представим в виде

$$e^{-x}=\left[\sum_{k=0}^{6}a_k x^k\right]^{-4},\ \text{при}\ 0\le x\le 16. \quad (21)$$

Значения коэффициентов a_k, используемых для приближения величины e^{-x}, приведены в табл.2.

Таблица 2

Значение интерполяционных коэффициентов для приближения величины e^{-x}

a_0	1
a_1	0,2499986842
a_2	0,0312575832
a_3	0,00259137121
a_4	0,0001715620
a_5	0,0000054302
a_6	0,0000006906

Интервальное расширение функции (20) примет вид:

$$e^{-\langle x,r_x\rangle}=\left[\sum_{k=0}^{6}\langle a,r_a\rangle_k\langle x,r_x\rangle^k\right]^{-4},\ 0\le x\le 16. \quad (22)$$

Экспоненту с положительным показателем представим в виде:

$$e^{\langle x,r_x\rangle}=1\ /\ \left[\sum_{k=0}^{6}\langle a,r_a\rangle_k\langle x,r_x\rangle^k\right]^{-4}. \quad (23)$$

Это позволяет осуществлять действия с числами в диапазоне $[1{,}12\cdot10^{-7};8{,}88\cdot10^{6}]$.

При выбранных методах вычисления значений тригонометрических и гиперболических функций потребуется выполнение операций сравнения интервальных чисел, представленных в системе центр-радиус.

Будем считать, что интервальное число A_1 меньше интервального числа A_2 если:

$$(A_1=\langle a_1;r_{a1}\rangle)<(A_2=\langle a_2;r_{a2}\rangle)\Rightarrow a_1+r_{a1}<a_2-r_{a2}. \quad (24)$$

В работе [9] модулем интервального числа $A=\left(\underline{a},\overline{a}\right)$ называют величину

$$\mathrm{mod}(A)=\max\left\{(a-r_a),(a+r_a)\right\}. \quad (25)$$

Условие, противоположное условию (25), назовем дополнительным модулем интервального числа $A=\left(\underline{a},\overline{a}\right)$, обозначим его выражением $Co\,\mathrm{mod}(A)$ от латинского «complimenti module»:

$$Co\,\mathrm{mod}(A)=\min\left\{(a-r_a),(a+r_a)\right\}. \quad (26)$$

Пусть V некоторое интервальное число и K некоторое неинтервальное число. Тогда условие $|V|\le K$ можно представить в виде:

$$\left(|V|\le K\right)\Rightarrow\left(co\,\mathrm{mod}\left\langle k,r_k\ge\langle 1;0\rangle\right\rangle\right)\&\ \mathrm{mod}\left(k;r_k\right)\le 1. \quad (27)$$

Условие $|V|\ge K$ представим в виде:

$$\left(|V|\ge K\right)\Rightarrow\left(co\,\mathrm{mod}\left\langle k,r_k\ge\langle 1;0\rangle\right\rangle\right)\&\ \mathrm{mod}\left(k;r_k\right)\le 1. \quad (28)$$

Для вычисления значений тригонометрических функций с интервально заданным аргументом используем методику, описанную в работе [4, С. 232].

Пусть $X=\langle x;r_x\rangle$, тогда:

$$Z=\frac{X}{2}=\frac{\langle x;r_x\rangle}{\langle 2;0\rangle}=\left\langle\frac{x}{2};\frac{r_x}{2}\right\rangle. \quad (29)$$

Функцию tgZ представим в виде:

$$tgZ=Z+\frac{1}{3}Z^3+\frac{2}{15}Z^5+\frac{17}{315}Z^7+\frac{62}{2835}Z^9,$$

$$\mathrm{mod}(Z)<\frac{\pi}{2}. \quad (30)$$

Используя условие (29) и основную тригонометрическую подстановку, получим выражения для вычисления основных тригонометрических функций, которые приведены в табл. 3.

Таблица 3

Значения основных тригонометрических функций, выраженных с использованием тангенса половинного угла

Функция	Подстановка	Ограничения
$\sin X$	$\frac{2tgZ}{1+tg^2Z}$	$\mathrm{mod}(Z)\ne\pi(1+2Z)$
$\cos X$	$\frac{1-tg^2Z}{1+tg^2Z}$	$\mathrm{mod}(Z)\ne\pi(1+2Z)$
tgX	$\frac{2tgZ}{1-tg^2Z}$	$\mathrm{mod}(Z)\ne\pi(1+2Z)$ $\mathrm{mod}(Z)\ne\pi\left(\frac{1}{2}+Z\right)$
$ctgX$	$\frac{1-tg^2Z}{2tgZ}$	$\mathrm{mod}(Z)\ne\pi(1+2Z)$ $\mathrm{mod}(Z)\ne\pi\left(\frac{1}{2}+Z\right)$

При использовании формул, приведенных в этой таблице, следует помнить, что их применять следует, только используя правила действия с интервальными числами, описанными ранее.

Для вычисления значений обратных тригонометрических функции используем выражения, приведенные в работе [9, С. 115, 119]. Тогда получим, что:

$$\arcsin\langle x;r_x\rangle=$$

$$=\ln\left(\langle 1;0\rangle+\langle x;r_x\rangle+\frac{\langle x;r_x\rangle^{\langle 2;0\rangle}}{2!}+\frac{\langle 5\rangle\langle x;r_x\rangle^{\langle 4;0\rangle}}{4!}\right); \quad (31)$$

$$ark\cos\langle x;r_x\rangle=\frac{\langle\pi;0\rangle}{\langle 2;0\rangle}-ark\sin\langle x;r_x\rangle; \quad (32)$$

$$arctg\langle x;r_x\rangle = \ln\left(\langle 1;0\rangle + \langle x;r_x\rangle + \frac{\langle x;r_x\rangle^{\langle 2;0\rangle}}{2!} - \right.$$

$$\left. - \frac{\langle x;r_x\rangle^{\langle 3;0\rangle}}{3!} + \frac{\langle 7;0\rangle\langle x;r_x\rangle^{\langle 4;0\rangle}}{4!}\right); \quad (33)$$

$$arkctg\langle x;r_x\rangle = \frac{\langle \pi;0\rangle}{\langle 2;0\rangle} - arktg\langle x;r_x\rangle. \quad (34)$$

Для вычисления значений гиперболических функций с интервально заданным аргументом используем методику, описанную в работах [3, С. 133; 4, С. 264]. Примем, что:

$$d\langle x;r_x\rangle = \exp\left(\langle x;r_x\rangle - 1\right). \quad (35)$$

Тогда основные гиперболические функции представим в виде:

$$sh(\langle x;r_x\rangle) = \langle 0.5;0\rangle\left(d\langle x;r_x\rangle + \frac{d\langle x;r_x\rangle}{d\langle x;r_x\rangle + \langle 1;0\rangle}\right); \quad (36)$$

$$ch\left(\langle x;r_x\rangle\right) = \left(sh^2\langle x;r_x\rangle + 1\right)^{\langle 0.5;0\rangle}; \quad (37)$$

$$th\left(\langle x;r_x\rangle\right) = \frac{sh\langle x;r_x\rangle}{\left(sh^2\langle x;r_x\rangle + 1\right)^{\langle 0.5;0\rangle}}; \quad (38)$$

$$cth\left(\langle x;r_x\rangle\right) = \frac{\left(sh^2\langle x;r_x\rangle + 1\right)^{0,5}}{sh\langle x;r_x\rangle}. \quad (39)$$

Для вычисления значений обратных гиперболических функций используем методику, описанную в работе [12, С. 28].

Значения арксинуса гиперболического вычислим по формуле:

$$Arsh\left(\langle x;r_x\rangle\right) =$$

$$\ln\left(\langle x;r_x\rangle + \left(\langle x;r_x\rangle^2 + \langle 1;0)\rangle\right)^{\langle 0,5;0\rangle}\right). \quad (40)$$

С учетом двузначности ареакосинуса гиперболического для вычисления его значений используем формулы:

$$Arch\left(\langle x;r_x\rangle_1\right) = \ln\left(\langle x;r_x\rangle + \left(\langle x;r_x\rangle^2 - \langle 1;0)\rangle\right)^{\langle 0,5;0\rangle}\right)$$

$$co\,\mathrm{mod}(X = \langle x;r_x\rangle) \geq \langle 1;0\rangle; \quad (41)$$

$$Arch\left(\langle x;r_x\rangle_2\right) = -\ln\left(\langle x;r_x\rangle + \left(\langle x;r_x\rangle^2 - \langle 1;0)\rangle\right)^{\langle 0,5;0\rangle}\right)$$

$$co\,\mathrm{mod}(X = \langle x;r_x\rangle) \geq \langle 1;0\rangle. \quad (42)$$

Значения арктангенса гиперболического и арккотангенса гиперболического вычислим по формулам:

$$Arth\langle x;r_x\rangle = \langle 0,5;0\rangle \ln\frac{\langle 1;0\rangle + \langle x;r_x\rangle}{\langle 1;0\rangle - \langle x;r_x\rangle},$$

$$-1 < co\,\mathrm{mod}\left(X = \langle x;r_x\rangle\right),\ \mathrm{mod}\left(X = \langle x;r_x\rangle\right) < 1. \quad (43)$$

$$Arcth\langle x;r_x\rangle = \langle 0,5;0\rangle \ln\frac{\langle 1;0\rangle + \langle x;r_x\rangle}{\langle x,r_x\rangle - \langle 1;0_x\rangle},$$

$$co\,\mathrm{mod}\left(X = \langle x;r_x\rangle\right) \geq -1,\ \mathrm{mod}\left(X = \langle x;r_x\rangle\right) < 1. \quad (44)$$

Далее, используя условия (13)…(44), вычислим значения гамма-функции, неполной гамма-функции, бета-функции и дигамма-функции при условии задания аргументов в виде интервальных чисел, определённых в системе центр-радиус.

В работе [2] приведены методы вычисления названных специальных функций аппроксимациями, использующими элементарные функции.

Для гамма-функции:

$$\Gamma(\alpha) = \int_0^\infty x^{\alpha-1}e^{-x}dx; \quad (45)$$

известно приближение вида:

$$\Gamma(\alpha) \approx \sqrt{\frac{2\pi}{\alpha}}e^{-\alpha}\alpha^{\alpha} \cdot \cdot\left(1 + \frac{1}{12\alpha} + \frac{1}{288\alpha^2} - \frac{139}{51840\alpha^3} - \frac{571}{2488320\alpha^4}\right). \quad (46)$$

Для неполной гамма-функции:

$$\Gamma(\alpha, x) = \int_x^\infty e^{-t}t^{\alpha-1}dt; \quad (47)$$

известно приближение вида:

$$\Gamma(\alpha, x) \approx e^{-x}x^{\alpha-1}\left[1 + \frac{\alpha-1}{x} + \frac{(\alpha-1)(\alpha-2)}{x^2}\right]. \quad (48)$$

Бета-функция может быть представлена в виде отношения гамма-функций:

$$B(u,v) = \int_0^1 x^{u-1}(1-x)^{v-1}dx = \frac{\Gamma(u)\Gamma(v)}{\Gamma(u+v)}. \quad (49)$$

Для дигамма-функции:

$$\psi(\alpha) = \frac{d}{d\alpha}\ln\Gamma(\alpha); \quad (50)$$

известно приближение вида:

$$\psi(\alpha) \approx \ln\alpha - \frac{1}{2\alpha} - \frac{1}{12\alpha^2} + \frac{1}{120\alpha^4} - \frac{1}{252\alpha^6}. \quad (51)$$

Совмещение методов интервальных вычислений с методами вычисления значений специальных функций позволяют найти решение задачи, сформулированной в заголовке данного сообщения.

В работе [13] для вычисления значений гамма-функции предложено упрощённое, в сравнении с условием (46), выражение вида:

$$\Gamma(\alpha) \approx \sqrt{\frac{2\pi}{\alpha}} e^{-\alpha} \alpha^{\alpha} \left(1 + \frac{1}{12\alpha} + \frac{1}{288\alpha^2}\right). \quad (52)$$

В табл.4 приведены значения функций Γ(2)=1 и Γ(6)=120 вычисленные по условиям (46) и (52).

Таблица 4

Значения функций Γ(2) и Γ(6)

Точное значение гамма-функции	Приближенное значение, вычисленное по условию (46)	Приближенное значение, вычисленное по условию (52)
Γ(2) =1	1,0003	0,999
Γ(6) =120	120,001	119,999

Хотя условие (46) кажется более точным, однако при выполнении вычислений в интервальном виде предпочтительнее оказалось условие (52), дающее меньший радиус интервала так, как количество операций с интервальными числами в нём меньше, чем в условии (46). В интервальном виде сомножитель $\sqrt{2\pi/\alpha}$ представим в виде:

$$A_1 = \frac{\langle 2{,}5066;0\rangle}{\langle \alpha; r_\alpha \rangle^{1/2}}. \quad (53)$$

Для определения его интервального значения выполним действия в такой последовательности.

1) Вычислим, используя условие (18), величину:

$$\ln\langle \alpha, r_\alpha \rangle = \sum_{i=1}^{6} \langle a_i, 0\rangle \left[\langle -1;0\rangle^{i-1} + \frac{\langle 1;0\rangle}{\langle \alpha, r_\alpha\rangle^i} \right] \frac{\left(\langle \alpha, r_\alpha\rangle - \langle 1;0\rangle\right)^i}{\langle i;0\rangle} = \langle a_1; r_{a1}\rangle. \quad (54)$$

2) Вычислим, используя условие (20), величину:

$$\langle \alpha; r_\alpha \rangle^{1/2} = \langle \alpha; r_\alpha \rangle^{\langle 0{,}5\rangle} = \sum_{k=0}^{6} \frac{\left(\langle \alpha; r_\alpha\rangle \langle a_1; r_{a1}\rangle\right)^{=k}}{k!} = \langle a_2; r_{a2}\rangle. \quad (55)$$

3) Тогда численное значение условия (53), используя условие (17), получим в виде:

$$A_1 = \frac{\langle 2{,}5066;0\rangle}{\langle \alpha; r_\alpha \rangle^{1/2}} = \left\langle \frac{2{,}5066 a_2}{a_2^2 - r_a^2}; \frac{2{,}5066 r_{a2}}{a_2^2 - r_a^2} \right\rangle. \quad (56)$$

4) Вычислим, используя условие (22), величину:

$$A_2 = e^{-\langle \alpha, r_\alpha\rangle} = \left[\sum_{k=0}^{6} \langle a, r_a\rangle_k \langle \alpha, r_\alpha\rangle^k \right]^{-4}. \quad (57)$$

5) Вычислим, используя условия (18) и (20), величину:

$$A_3 = \langle \alpha; r_\alpha \rangle^{\langle \alpha; r_\alpha\rangle} = \sum_{k=0}^{6} \frac{\left(\langle \alpha; r_\alpha\rangle \ln\langle \alpha_1; r_{\alpha 1}\rangle\right)^k}{k!}. \quad (58)$$

Интервальное значение сомножителя, стоящего в круглых скобках в условии (52) вычислим, используя условия (18) и (20), таким образом:

$$A_4 = \langle 1;0\rangle + \frac{\langle 0.0833;0\rangle}{\langle a; r_a\rangle} + \frac{\langle 0.00347;0\rangle}{\langle a; r_a\rangle^2} = \langle 1;0\rangle + \frac{\langle 0.0833;0\rangle}{\langle a; r_a\rangle} + \frac{\langle 0.00347;0\rangle}{\left\langle a^2 + r_a^2; 2|a| r_a \right\rangle} = \langle 1;0\rangle + \left\langle \frac{0.0833a}{a^2 - r_a^2}; \frac{0.0833 r_a}{a^2 - r_a^2} \right\rangle + \left\langle \frac{0.00347a}{\left[\left(a^2 + r_a^2\right)^2 - 4a^2 r_a^2\right]} + \frac{0.00347 r_a}{\left[\left(a^2 + r_q^2\right)^2 - 4a^2 r_a^2\right]} \right\rangle. \quad (59)$$

Следовательно, интервальное расширение гамма-функции, вычисленное в системе центр-радиус $\left[\Gamma(\alpha)\right]$, можно определить так:

$$\left[\Gamma(\alpha)\right] = \prod_{i=1}^{4} A_i = \left\langle g(\alpha); r_{g(\alpha)} \right\rangle. \quad (60)$$

Условие (60) получают последовательным выполнением действий по условию (7).

Рассмотрим более подробно процедуру вычисления интервальных значений неполной гамма-функции. Интервальное расширение выражения e^{-x} получено в условии (36) и равно A_5. Интервальное расширение выражения $x^{\alpha-1}$, используя условия (6), (18), (37), примет следующий вид:

$$A_5 = \langle x-1; r_x \rangle^{\langle \alpha - 1; r_\alpha\rangle} = \sum_{k=0}^{6} \frac{\left(\langle \alpha - 1; r_\alpha\rangle \ln\langle x-1; r_x\rangle\right)^k}{k!}. \quad (61)$$

Далее, используя условия (5), (7), (8) и (11) получим следующее:

$$A_6 = \left\langle \left[1 + \frac{\alpha - 1}{x} + \frac{(\alpha-1)(\alpha-2)}{x^2} \right] \right\rangle =$$

$$= \left[\langle 1;0 \rangle + \frac{\langle \alpha - 1; r_\alpha \rangle}{\langle x; r_x \rangle} + \frac{\langle \alpha - 1; r_\alpha \rangle \langle \alpha - 2; r_\alpha \rangle}{\langle x; r_x \rangle} \right] =$$

$$= \left[\begin{array}{l} \langle 1;0 \rangle + \left\langle \frac{(\alpha-1)x + r_\alpha r_x}{x^2 - r_x^2}; \frac{(\alpha-1) r_x + x r_\alpha}{x^2 - r_x^2} \right\rangle + \\ + \frac{\left\langle (\alpha-1)^2 - \alpha + 1; r_\alpha (2\alpha - 3) \right\rangle}{\left\langle x^2 + r_x^2; 2|x| r_x \right\rangle} \end{array} \right]. \quad (62)$$

Следовательно, интервальное расширение неполной гамма-функции, вычисленное в системе центр-радиус, $\left[\Gamma(\alpha, x)\right]$ можно определить так:

$$\left[\Gamma(\alpha, x)\right] = A_2 A_5 A_6 . \quad (63)$$

Рассмотрим более подробно процедуру вычисления интервальных значений бета-функции. Из условия (28) следует, что основной элемент вычислительного процесса – вычисление функции $\left[\Gamma(\alpha)\right]$, реализуемое условиями (33,…39)

$$A_7 = \left[\Gamma(u)\right] \cdot \left[\Gamma(v)\right] = \left\langle g(u); r_{g(u)} \right\rangle \left\langle g(v); r_{g(v)} \right\rangle =$$

$$= \left\langle g(u) g(v) + r_{g(u)} r_{g(v)}; g(u) r_{g(v)} + g(v) r_{g(u)} \right\rangle . \quad (64)$$

Используя условие (5) получим, что:

$$\left\langle z; r_z = \right\rangle \left\langle u; r_u \right\rangle + \left\langle v; r_v \right\rangle = \left\langle u + v; r_u + r_v \right\rangle . \quad (65)$$

Следовательно:

$$\left[\mathrm{B}(u, v\right] = \frac{A_7}{\left\langle g(z); r_{g(z)} \right\rangle} . \quad (66)$$

Интервальное расширение дигамма–функции, используя условия (11), (18), (30), представим в виде:

$$\left[\psi(\alpha)\right] = \sum_{i=1}^{6} \langle a_i, 0 \rangle \left[\langle -1;0 \rangle^{i-1} + \frac{\langle 1;0 \rangle}{\langle \alpha, r_\alpha \rangle^i} \right] \times$$

$$\times \frac{\left(\langle \alpha, r_\alpha \rangle - \langle 1;0 \rangle \right)^i}{\langle i;0 \rangle} - \frac{\langle 0{,}08333;0 \rangle}{\left\langle a^2 + r_a^2; 2|a| r_a \right\rangle} +$$

$$+ \frac{0{,}00833}{\left\langle a^2 + r_a^2; 2|a| r_a \right\rangle \underbrace{\left((a; r_a) \ldots (a; r_a) \right)}_{2}} -$$

$$- \frac{0{,}00397}{\left\langle a^2 + r_a^2; 2|a| r_a \right\rangle \underbrace{\left((a; r_a) \ldots (a; r_a) \right)}_{4}} . \quad (67)$$

В табл.5 приведены результаты сравнения предложенных методов вычисления значений гамма-функции, неполной гамма-функции, бета-функции и дигамма-функции с их табличными значениями, приведенными в работах [2, 14].

Таблица 5

Табличные и интервальные значения гамма-функции, неполной гамма-функции, бета-функции и дигамма-функции

Вид функции	Табличное значения	Интервальные расширения	
		Система центр-радиус	Классическое представление
Γ(1,5)	0,8862	$\left\langle 0{,}88685; 9 \cdot 10^{-5} \right\rangle$	*[0,88676; 0,88694]*
Γ(2;3)	0,19914	$\left\langle 0{,}19915; 11 \cdot 10^{-3} \right\rangle$	*[0,19904; 0,19926]*
B(1,5; 1,2)	0,51488	$\left\langle 0{,}51488; 2988 \cdot 10^{-2} \right\rangle$	*[0,51476; 0,51500]*
Ψ(1;5)	*0,03648*	$\left\langle 0{,}36380; 155 \cdot 10^{-3} \right\rangle$	*[0,36365; 0,36396]*

Сопоставляя табличные значения функций и их интервальные расширения можно сделать вывод о том, что применение интервальных вычислений позволяет получать не только значения функций с достаточной для практического применения точностью, но и одновременно оценивать погрешность получаемых результатов вычислений. Последнее обстоятельство, по мнению авторов данного сообщения, делает их применение целесообразным в тех случаях, когда аргументы функций получают в результате экспериментальных наблюдений.

Для проведения вычислительных экспериментов разработана программная система на языке программирования C# в среде программирования Visual Studio. Главная форма предлагаемой программной системы показана на рис.1.

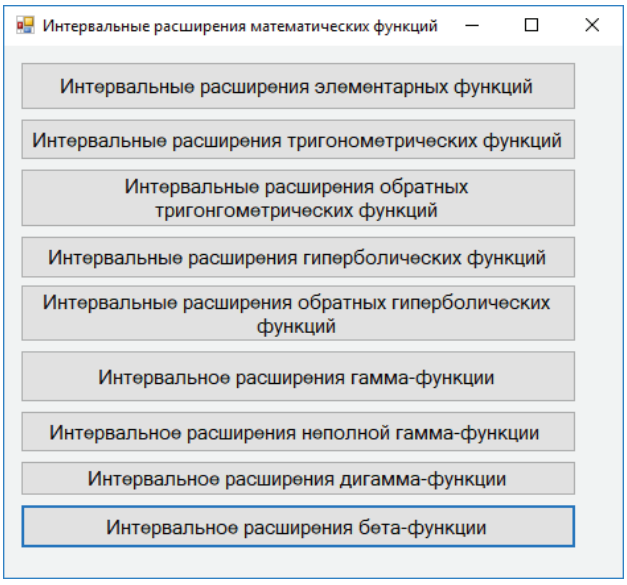


Рис.1. Главное окно программной системы для программного обеспечения

«Интервальные расширения математических функций».

Примеры расчетов по интервальным расширениям элементарных функций показаны на рис.2,…6.

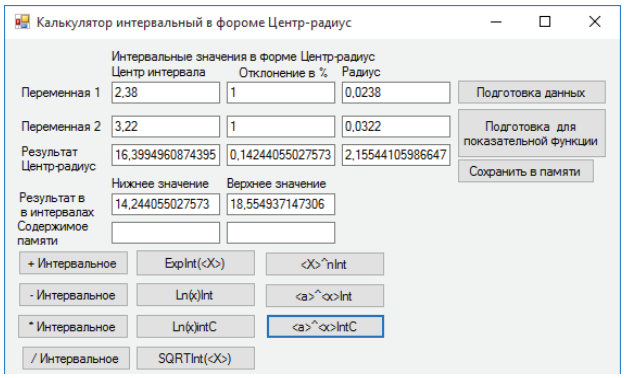


Рис.2. Пример расчета значений степенной функции

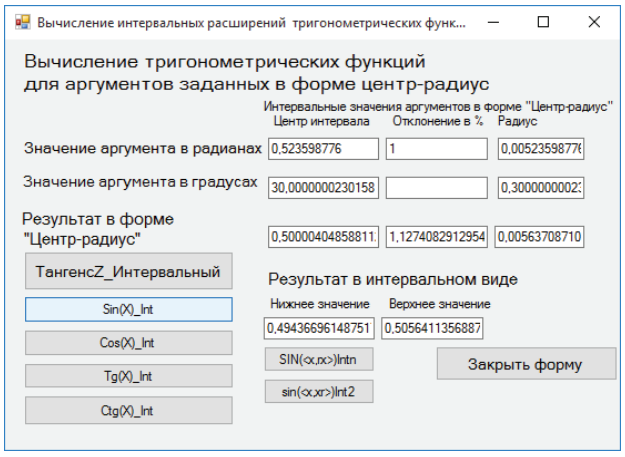


Рис.3. Пример расчета значений тригонометрической функции

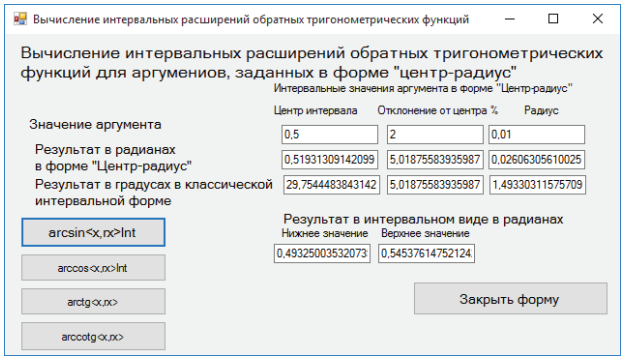


Рис.4. Пример расчета значений обратной тригонометрической функции

В программной системе предусмотрено ее дальнейшее расширение, для решения прикладных задач с использованием интервальных расширений математических функций.

Областью применения полученных результатов могут быть вычисления значений элементарных и специальных функций в тех случаях, когда аргументы функций получают в результате экспериментальных наблюдений.

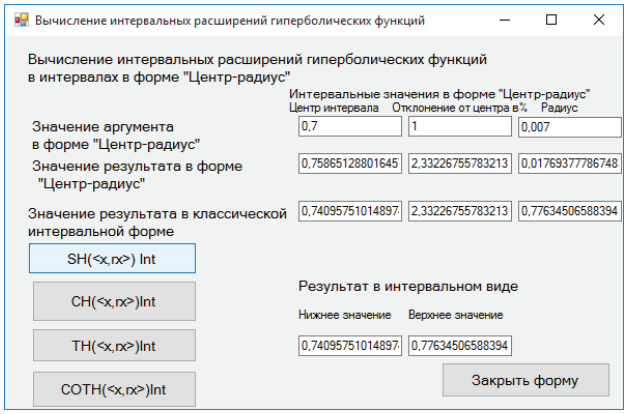


Рис.5. Пример расчета значений гиперболической функции

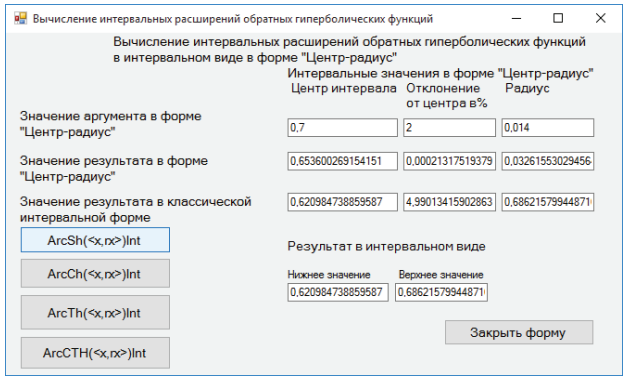


Рис.6. Пример расчета значений обратных гиперболической функции

ЗАКЛЮЧЕНИЕ

Предложены алгоритмы для вычисления значений элементарных функций, аргументы которых представлены интервальными числами, определёнными в системе центр-радиус.

Алгоритмы реализованы в специализированном программном калькуляторе, позволяющем вычислять интервальные значения степенной, показательной, логарифмической функции, прямых и обратных тригонометрических функций, прямых и обратных гиперболических функций.

Для гамма-функции, неполной гамма-функции, бета-функции и дигамма-функции предложены алгоритмы вычисления их значений при условии определения их аргументов в виде интервальных чисел, заданных в системе центр-радиус.

Результаты численного эксперимента показали, что применение интервальных вычислений позволяет получать значения функций с достаточной для практического применения точностью и одновременно оценивать погрешность получаемых результатов вычислений.

Областью применения полученных результатов могут быть вычисления значений элементарных и специальных функций в тех случаях, когда аргументы функций получают в результате экспериментальных наблюдений.

Литература

[1] *Carlson B., Goldstein M.* Rational approximation of functions. / Los Alamos Scientific Laboratory LA-1943, 1955.

[2] Справочник по специальным функциям с формулами, графиками и математическими таблицами. / Под ред. М. Абрамовица и И. Стигана. – М. : Наука, 1979. – 832 с.

[3] *Люстерник, Л.А.* Математический анализ: Вычисление элементарных функций / Л.А. Люстерник, О.А. Червоненкис, А.Р. Янпольский. – М., 1963. – 248 с.

[4] *Попов Б. А., Теслер Г.А.* Вычисление функций на ЭВМ. / Б.А. Попов, Г.А. Теслер. – К.: «Наукова думка», 1984. – 599с.

[5] *Кошаровский А.Н.* Разработка и исследование алгоритмов и процессоров вычисления значений элементарных функций: дис. канд. техн. наук: 05.13.05 / Кошаровский Андрей Николаевич. – Москва, Московский энергетический институт, 2000 г. – 179 с.

[6] *Сальников М.С.* Рекурсивный алгоритм вычисления логарифма. /С. Сальников // Информационные процессы. – 2012. – Т.12, № 3. – С. 248–252.

[7] *Алефельд Г.* Введение в интервальные вычисления / Г. Алефельд, Ю. Херцбергер. – М.: Мир, 1987. – 360 с.

[8] *Алтунин А.Е.* Модели и алгоритмы принятия решений в нечетких условиях /А.Е. Алтунин, М.В. Семухин. – Тюмень: Изд. ТГУ, 2000. – 352 с.

[9] *Шарый, С.П.* Конечномерный интервальный анализ / С.П. Шарый. – М.:Изд-во «XYZ», 2012. – 606 с.

[10] *Жуковська, О.А.* Основи інтервального аналізу: навч. посібник / О.А. Жуковська. – К.: Освіта України, 2009. – 136 с.

[11] *Стоян Ю.Г.* Введення в інтервальну геометрію: навч. посіб. /Ю.Г. Стоян -Харків. ХІРЕ, 2006. – 98с.

[12] *Янпольский А.Р.* Гиперболические функции. / А.Р. Японьский.-М.: Физматгиз, 1960. – 195 с.

[13] *Кобзарь А.И.* Прикладная математическая статистика. Для научных работников и инженеров. / А.И. Кобзарь. – Москва: ФИЗМАТЛИТ, 2006. – 816 с.

[14] Calculates the Incomplete gamma functions of the first and second kind γ(a, x) and Γ(a, x). / Режим доступа: http://keisan.casio.com/exec/ system/1180573447.

Поступила в редколлегию 31.10.2017

Дубницкий Валерий Юрьевич, канд. техн. наук, ст. научн. сотр, Харьковский учебно-научный институт ГВУЗ Университета банковского дела. Область научных интересов – интервальные вычисления, моделирование финансовых процессов.

Кобылин Анатолий Михайлович, канд. техн. наук, доцент, доцент кафедры информационных технологий, Харьковский учебно-научный институт ГВУЗ Университета банковского дела. Область научных интересов – интервальные вычисления, моделирование финансовых процессов.

Кобылин Олег Анатольевич, канд. техн. наук, доцент, доцент кафедры Информатики, Харьковский национальный университет радиоэлектроники. Область научных интересов – обработка изображений, распознавание образов, спектральный анализ изображений.

УДК 19.66:519.668

Обчислення значень елементарних та спеціальних функцій з інтервально заданим аргументом, визначеним в системі центр-радіус / В.Ю. Дубницький, А.М. Кобилін, О.А. Кобилін // Прикладна радіоелектроніка: наук. – техн. журнал. – 2017. – Том 16, № 3, 4. – С. 147–154.

Запропоновано алгоритми для обчислення значень елементарних функцій, аргументи яких подано інтервальними числами, визначеними в системі центр-радіус.

Алгоритми реалізовано в спеціалізованому програмному калькуляторі, що дозволяє обчислювати інтервальні значення степеневої, показникової, логарифмічної функції, прямих і зворотних тригонометричних функцій, прямих і зворотних гіперболічних функцій, гамма-функції, неповної гамма-функції, бета-функції і дігамма-функції.

Ключові слова: елементарні функції, інтервальні числа, які визначено в системі центр-радіус, спеціалізований програмний калькулятор, степенева функція, показникова функція, логарифмічна функція, прямі і зворотні тригонометричні функції, прямі і зворотні гіперболічні функції, гамма-функція, неповна гамма-функції, бета-функція, дігамма-функція.

Табл.: 05. Іл.: 06. Бібліогр.: 14 найм.

UDC 19.66:519.668

Calculation of elementary and special functions values with interval stated argument determined in a center-radius system / V.Yu. Dubnitskiy, A.M. Kobylin, O.A. Kobylin // Applied Radio Electronics: Sci. Journ. – 2017. – Vol. 16, № 3, 4. – P. 147–154.

Algorithms are proposed to calculate the values of elementary functions whose arguments are represented by interval numbers determined in a center-radius system. The arguments are realized in a specialized programmable calculator, which enables to calculate interval values of power, exponential and logarithmic functions, direct and inverse trigonometric functions, direct and inverse hyperbolic functions. For calculating gamma, incomplete gamma, beta and digamma functions algorithms of their values are proposed under the proviso that their arguments are defined in the form of interval numbers set in the center-radius system.

Keywords: elementary functions, interval numbers determined in a center-radius system, specialized programmable calculator, power function, exponential function, logarithmic function, direct and inverse trigonometric functions, direct and inverse hyperbolic functions, gamma function, incomplete gamma function, beta function, digamma function, interval calculations, center-radius system.

Tab. 05. Fig. 06. Ref.: 14 items.

УДК 681.3.06:006.354

ОЦІНКИ ПРАКТИЧНОЇ СТІЙКОСТІ МОДИФІКОВАНИХ СТАНДАРТІВ БЛОКОВОГО ШИФРУВАННЯ УКРАЇНИ ТА РОСІЇ ВІДНОСНО ЦІЛОЧИСЕЛЬНОГО РІЗНИЦЕВОГО КРИПТОАНАЛІЗУ

Л. В. КОВАЛЬЧУК, Н. В. КУЧИНСЬКА

Розглянуто одну з актуальних модифікацій різницевого криптоаналізу, а саме цілочисельний різницевий криптоаналіз. Отримано науково обґрунтовані оцінки практичної стійкості до цілочисельного різницевого криптоаналізу модифікованих стандартів блокового шифрування України та Росії. Показано від яких саме параметрів, що характеризують s-блоки, залежать ці оцінки. Проведено порівняльний аналіз значень цих параметрів для всіх алгоритмів, розглянутих у цій роботі. Також наведено статистичний розподіл отриманих параметрів за випадковою вибіркою з 100000 s-блоків.

Ключові слова: різницевий криптоаналіз, стандарти блокового шифрування, s-блоки.

ВСТУП

Сьогодні симетричні блокові алгоритми шифрування є основним криптографічним засобом забезпечення конфіденційності під час обробки інформації в сучасних інформаційно-телекомунікаційних системах. Тривалий час у країнах СНД широко використовувався радянський алгоритм блокового шифрування ГОСТ 28147-89. Але питання його удосконалення та побудови нових ефективних алгоритмів шифрування з обґрунтованою стійкістю залишилось актуальним. В результаті за останні кілька років в країнах СНД було прийнято низку власних стандартів блокових шифрів:

- СТБ 34.101.31-2011 (Білорусь) [1];
- ГОСТ Р 34.12 2015 (РФ) [2];
- ДСТУ 7624:2014 «Калина» (Україна) [3].

Слід зауважити, що в стандарті ГОСТ Р 34.12 2015 визначено два алгоритми блокового шифрування: один алгоритм для довжини блока 128 біт, на який можна посилатись, як на «Кузнєчік», другий алгоритм з довжиною блока 64 біт, на який можна посилатись, як на «Магму». Другий алгоритм є за своєю структурою аналогічним алгоритму, визначеному в ГОСТ 28147-89 [2]. Крім того, український («Калина») та російський («Кузнєчік») стандарти схожі за своєю будовою, оскільки за основу обох алгоритмів було взято стандарт AES. У цьому розумінні алгоритм ГОСТ Р 34.12 2015 «Кузнєчік» можна вважати «Калина»–подібним алгоритмом.

Переважну більшість сучасних блокових SPN-шифрів спроектовано схожим чином: їх раундові функції є композицією ключового суматора, блоку підстановки і оператора перестановки, лінійного над полем F_2 або його деяким розширенням. Тому задача оцінювання стійкості таких шифрів до різницевого криптоаналізу та його можливих модифікацій або зводиться до задачі побудови верхніх оцінок середніх ймовірностей диференціалів таких композицій, або містить її як підзадачу [4–15].

Вперше цілочисельні диференціали згадуються у роботах, що стосуються криптоаналізу та обґрунтування стійкості геш-функцій. Зокрема, з використанням цілочисельних диференціалів були побудовані колізії як до багатьох функцій класу MD, так і до окремих вузлів таких функцій. Досить повний перелік посилань на такі роботи, а також обґрунтування використання саме цілочисельних диференціалів можна знайти в [8–10]. Зауважимо, що аналітичні складнощі, які виникають в цьому випадку у зв'язку з наявністю біта переносу при модульному додаванні, посилюються тим, що оператор перестановки, який є одним з перетворень хеш-функції, не є лінійним відносно модульного додавання. Виходячи з отриманих у роботах [8–10] результатів, можна зробити висновок, що використання цілочисельних диференціалів є виправданим при криптоаналізі таких блокових шифрів або хеш-функцій, які містять суматор за модулем 2^n, причому як правило n=32 або 64.

Слід зазначити, що у всіх попередніх роботах, у яких розглядались немарковські та узагальнено марковські блокові шифри, або будувались оцінки практичної стійкості алгоритмів відносно побітового різницевого криптоаналізу, або будувались оцінки стійкості раундових функцій до цілочисельного криптоаналізу. Питання побудови оцінок стійкості блокових алгоритмів до цілочисельного різницевого криптоаналізу у цій роботі розглянуто вперше.

Основні означення, що стосуються марковських, узагальнено марковських блокових алгоритмів та такі, що використовуватимемо в даній статті, можна знайти в [5, 13].

1. ОСНОВНІ ТЕРМІНИ ТА ПОЗНАЧЕННЯ

Розглянемо $\Im$ – r-раундовий блоковий шифр, який перетворює відкритий текст $x \in V_n$ у шифрований текст $y \in V_n$ при ключі шифрування $k = (k_1, k_2, \ldots, k_r) \in (V_m)^r$ за таким правилом:

$$y = \Im_k(x) = f_{k_r} \circ f_{k_{r-1}} \circ \cdots \circ f_{k_1}(x), \qquad (1)$$

де $k_i \in V_m$, $i = \overline{1, r}$ – раундові ключі, $f_\lambda(\cdot) : V_n \to V_n$, $\lambda \in V_m$ – раундова функція шифрування. Також припускатимемо, що раундові ключі незалежні в сукупності рівноімовірно розподілені на V_m випадкові величини.

Для раундової функції $f_k : V_n \to V_n, k \in V_m$, яка фігурує в (1), *диференціалом (різницею) цієї функції відносно операцій* (μ_1, μ_2) називатимемо пару (α, β), для яких існує $x \in V_n$ таке, що виконується співвідношення:

$$f_k(x \circ_1 \alpha) \circ_2 f_k(x)^{-1} = \beta,$$

де $\alpha, \beta \in V_n$, а під $f_k(x)^{-1}$ розуміють елемент множини V_n, обернений до $f_k(x)$ відносно операції μ_2 [13]. У такому випадку двійковий вектор α називають вхідною різницею, а β - вихідною.

Величину

$$d^f_{\mu_1,\mu_2}(x; \alpha, \beta) = 2^{-n} \sum_{k \in V_n} \delta(f_k(x \circ_1 \alpha) \circ_2 f_k(x)^{-1}, \beta), \quad (2)$$

називають *середньою* (*за ключами*) *ймовірністю раундового диференціалу* (α, β) *в точці* x відносно операцій μ_1, μ_2 на множині V_n, де $x, \alpha, \beta \in V_n$.

Величину

$$d^f_{\mu_1,\mu_2}(\alpha, \beta) = 2^{-n} \sum_{x \in V_n} d^f_{\mu_1,\mu_2}(x; \alpha, \beta) \quad (3)$$

називають *середньою* (*за ключами*) *ймовірністю раундового диференціалу* (α, β) відносно операцій μ_1, μ_2 [13]. Якщо $\mu_1 = \mu_2 = \mu$, також використовуватимемо позначення $d^f_\mu(x; \alpha, \beta)$ і $d^f_\mu(\alpha, \beta)$, якщо це не викликає непорозумінь.

За означенням, шифр є марковським, якщо $\forall\ x, \alpha, \beta \in V_n$: $d^f_{\mu_1,\mu_2}(x; \alpha, \beta) = d^f_{\mu_1,\mu_2}(0; \alpha, \beta)$.

З (3) випливає, що в цьому випадку також правильно

$$\forall\ x, \alpha, \beta \in V_n : d^f_{\mu_1,\mu_2}(x; \alpha, \beta) = d^f_{\mu_1,\mu_2}(\alpha, \beta).$$

Різницевою характеристикою шифру (1) назвемо послідовність $\Omega = (\omega_0, \omega_1, \ldots, \omega_{r+1})$, де $\omega_i \in V_n \setminus \{0\}$, $i = \overline{1, r}$. [5]

Середньою (за ключами) ймовірністю різницевої характеристики назвемо величину

$$EDP(\Omega) =$$

$$= \frac{1}{2^n} \sum_{x_0 \in V_m} \frac{1}{2^{mr}} \sum_{k_1, \ldots, k_r \in V_n} \prod_{i=1}^{r} \delta(f_{k_i}(x_{i-1} \circ \omega_{i-1}) \circ f_{k_1}^{-1}(x_{i-1}), \omega_i) \cdot$$

Ми розглядатимемо лише такі Ω, для яких $EDP(\Omega) \neq 0$. Зауважимо, що введена таким чином величина $EDP(\Omega)$ дійсно є імовірністю (за всіма $K \in (V_m)^r$ та $x_0 \in V_n$) події, яка полягає у тому, що вхідна різниця ω_0 після першого раунду перейшла у різницю ω_1, після другого – у ω_2 і т. д., а після r-го – у ω_r. Величина $\max_\Omega EDP(\Omega)$ є обернено пропорційною до кількості матеріалу, необхідного для атаки на алгоритм, тобто вона характеризує *практичну стійкість блокового алгоритму шифрування*.

Оскільки дослідження стійкості марковських та немарковських блокових шифрів суттєво відрізняється, то в ході аналізу будь-якого блокового шифру на першому етапі завжди потрібно визначити, чи є він марковським.

У наших позначеннях марковський шифр має такі властивості:

1) величина (2) не залежить від x і дорівнює середній (за ключами) імовірності раундового диференціалу у точці 0;

2) для величини (3) виконується така рівність:
$\forall \alpha, \beta \in V_m\ \forall x \in V_m$:

$$d^f_{\mu_1,\mu_2}(\alpha, \beta) = d^f_{\mu_1,\mu_2}(x; \alpha, \beta) = d^f_{\mu_1,\mu_2}(0; \alpha, \beta),$$

тобто середня за ключами імовірність раундового диференціалу дорівнює середній за ключами імовірності раундового диференціалу у точці 0.

Основною властивістю марковських шифрів, яка водночас є їхньою суттєвою перевагою в ході побудови оцінок практичної стійкості до різницевого криптоаналізу, є виконання такого співвідношення:

$$EDP(\Omega) = \prod_{i=0}^{r-1} d^f_{\mu_1,\mu_2}(0; \omega_i, \omega_{i+1}) = \prod_{i=0}^{r-1} d^f_{\mu_1,\mu_2}(\omega_i, \omega_{i+1}),$$

тобто імовірність різницевої характеристики марковського шифру дорівнює добутку імовірностей його раундових диференціалів у точці 0.

2. ПОБУДОВА ОЦІНОК ПРАКТИЧНОЇ СТІЙКОСТІ МОДИФІКОВАНОГО ГОСТ-ПОДІБНОГО АЛГОРИТМУ

Означення 1. Називатимемо блоковий алгоритм шифрування (1) *модифікованим ГОСТ-подібним алгоритмом*, якщо його раундова функція має такий вигляд:

$$f_k(u, v) = (v, u + \varphi(v + k)), \quad (4)$$

де $x = (u, v) \in V_n$, $n = 2m$, $u, v, k \in V_m$, k – раундовий ключ, $\varphi : V_m \times V_m \to V_m$ – раундове перетворення алгоритму (4), а під операцією "+" розуміють додавання за модулем 2^m.

Довжина блоку алгоритму визначається як $n = pu$, $p \geq 2$, а блок підстановки є відображенням, визначеним таким чином:

$$\forall x \in V_n : \quad S(x) = (s^{(p)}(x^{(p)}), \ldots, s^{(1)}(x^{(1)})),$$

$$x^{(i)} \in V_u, i = \overline{1, p},$$

де s-блоки $s^{(i)}: V_u \to V_u$, $i = \overline{1, p}$ – бієктивні відображення.

Відображення зсуву вліво на t біт вектора з V_m позначимо $L_t: V_m \to V_m$.

В наших позначеннях раундове перетворення $\varphi: V_m \times V_m \to V_m$, яке задано в (4), можна подати таким чином:

$$\varphi(x,k) = L_t\big(S(x+k)\big). \qquad (5)$$

Для модифікованого за таким правилом алгоритму справедливі наступні леми.

Лема 1. Блоковий алгоритм шифрування з раундовою функцією (4) є марковським шифром відносно операції додавання за модулем 2^m.

Доведення леми 1 виконується заміною змінної $k+v$ на k під час обчислення (2).

Лема 2. Для модифікованого ГОСТ-подібного алгоритму справедлива така оцінка практичної стійкості:

$$\max_{\Omega} EDP(\Omega) \le \left(\max_{\alpha,\beta \in V_n \setminus \{0\}} d_+^{\varphi}(0;\alpha,\beta) \right)^{\left\lfloor \frac{2r}{3} \right\rfloor}.$$

Доведення леми 2 є аналогічним до доведення відповідного результату у роботі [9] для класичного різницевого криптоаналізу.

Для побудови верхньої оцінки величини $\max\limits_{\alpha,\beta \in V_n \setminus \{0\}} d_+^{\varphi}(0;\alpha,\beta)$ скористаємось результатами, отриманими в [15, 16]. Далі ми коротко наведемо ці результати.

Введемо необхідні позначення.

Для довільного блоку заміни s покладемо

$$\Delta_+^s = \max_{\alpha,\beta \in V_u \setminus \{0\}} 2^{-u} \sum_{k \in V_u} \delta(s(k+\alpha) - s(k), \beta), \quad (6)$$

$$\delta_+^s = \max_{\substack{\alpha \in V_u \setminus \{0\} \\ \beta \in V_u \setminus \{0\}}} \frac{1}{2^u} \sum_{k \in V_u} (\delta(s(k+\alpha) - s(k), \beta) +$$

$$+ \delta(s(k+\alpha) - s(k), \beta + 1)). \qquad (7)$$

Таким чином верхні оцінки середніх імовірностей цілочисельних диференціалів відображення (5) визначає наступна теорема [15].

Теорема 1. Нехай $t \ge u, p \ge 2$. Якщо раундова функція має вигляд (5), то справедлива така нерівність:

$$\forall \alpha, \beta \in V_n \setminus \{0\}: \quad d_+^{\varphi}(\alpha,\beta) \le \max\left\{ \delta_+^s,\ 2\Delta_+ \right\}.$$

Тому шукане найбільше значення γ відповідно буде

$$d_+^{\varphi}(\alpha,\beta) \le \gamma = \max\left\{ \delta_+^s,\ 2\Delta_+ \right\}. \qquad (8)$$

Зауважимо, що час обчислення параметра (8) для довжини входу $n = pu$ (розмір входу s-блоку дорівнює u) становить $O(pu^3 \log u)$ бітових операцій.

Використовуючи результати лем 1, 2 та теореми 1 можна довести справедливість оцінки практичної стійкості модифікованого ГОСТ-подібного алгоритму до цілочисельного різницевого криптоаналізу. Для введеного ГОСТ-подібного алгоритму справедливим є наступний результат.

Теорема 2. Для модифікованого ГОСТ-подібного алгоритму справедлива оцінка практичної стійкості:

$$\max_{\Omega} EDP(\Omega) \le \left(\max\left\{ \delta_+^s,\ 2\Delta_+ \right\} \right)^{21}.$$

Нижче наведено статистичний розподіл параметрів (6), (7) для вузлів заміни алгоритму ГОСТ, рекомендованих згідно з [17].

Таблиця 1

Значення параметрів (6), (7) для рекомендованих вузлів заміни алгоритму ГОСТ

Номер ДКЕ	*вузол заміни*	*значення вузла заміни*	$2^4 \cdot d_+^s$	$2^4\ \delta_+^s$
dke1	K0	a9d6eb45f13c7082	4	7
dke1	K1	80c4967b231f5ead	4	5
dke1	K2	f658eba4c037291d	5	6
dke1	K3	38d96bf025ca4e17	4	7
dke1	K4	f8e9720dc615b43a	4	6
dke1	K5	28975f0bc1dea364	5	7
dke1	K6	38b564ea2c179fd0	5	5
dke1	K7	123e6db8fac57904	5	6
dke2	K0	e937f4cb6ad10582	4	7
dke2	K1	adc76e81f3b40952	4	6
dke2	K2	4b1f92ec6a87350d	4	6
dke2	K3	451c7e92afbd0863	4	5
dke2	K4	cb39f04572ed1a86	4	5
dke2	K5	873a96e5d04c12fb	4	6
dke2	K6	f0e68d59a31c4b72	3	5
dke2	K7	43ed502b1a769f8c	4	6
dke3	K0	d91e72c54b6f38a0	5	7
dke3	K1	786b034d95feac21	3	5
dke3	K2	a53c98d64fe02b17	5	5
dke3	K3	bac1569e2df70438	4	6
dke3	K4	5b30f9e41c862a7d	4	5
dke3	K5	43bd1f827ec9a065	3	5
dke3	K6	378b1e50d4ca29f6	5	6
dke3	K7	6dcab793fe120845	4	5
dke4	K0	9c3d76e1a2048f5b	3	5
dke4	K1	a5be760c28f4d391	5	6
dke4	K2	4c30d2eb7f5918a6	5	6
dke4	K3	3945e786d02fbca1	5	7
dke4	K4	29cfdb41753e68a0	4	6
dke4	K5	e5db1942f8703ca6	4	7
dke4	K6	e65a9d48bc0371f2	4	7
dke4	K7	19cb76832fe05a4d	4	7

Номер ДКЕ	*вузол заміни*	*значення вузла заміни*	$2^4 \cdot d_+^s$	$2^4\ \delta_+^s$
dke5	K0	34d8c7a20e9fb156	3	5
dke5	K1	c76938b5fa0d421e	5	5
dke5	K2	e487b3ac1269df05	5	6
dke5	K3	396d8fa27ec0b415	6	8
dke5	K4	5ca721fde3b40896	4	6
dke5	K5	18be74a0c35d9f62	6	7
dke5	K6	9bad5e23064cf178	4	5
dke5	K7	e9185fb062c7a4d3	4	6
dke6	K0	fc96e21b0d4a7835	5	6
dke6	K1	ec5074a3261d9bf8	3	6
dke6	K2	56d9bea3f281407c	4	6
dke6	K3	1f742ec36b9805ad	4	6
dke6	K4	f9e6d158423cab07	6	6
dke6	K5	b0d7ce142368a5f9	5	7
dke6	K6	7ef8d0b3a1429c65	4	6
dke6	K7	15eb2c38a097f64d	5	8
dke7	K0	fda5c01692e73b48	5	6
dke7	K1	25a0691fd47eb38c	4	6
dke7	K2	3e4b5912f68d70ac	6	6
dke7	K3	4ab9f2e5d13607c8	4	6
dke7	K4	f65897cb0a3124de	4	6
dke7	K5	cbf451e908d2a736	4	6
dke7	K6	d248bc13a59e7f06	4	6
dke7	K7	150f6a3e72cdb894	4	5
dke8	K0	e4b2875c9d031f6a	5	7
dke8	K1	3eca62d198740f5b	5	6
dke8	K2	52871fe64db0a3c9	4	5
dke8	K3	ca7de3029516b4f8	4	7
dke8	K4	63f709a8bc4152de	4	6
dke8	K5	6df15380bae49c27	4	5
dke8	K6	2fc5b13e06da7948	4	6
dke8	K7	305c8fdeb629714a	5	6
dke9	K0	90bc243fd6e1a758	4	6
dke9	K1	350f87ecda16b249	5	6
dke9	K2	845aebd6cf793120	4	6
dke9	K3	54f0cba91e8632d7	5	7
dke9	K4	7c3068eb1fda9524	4	6
dke9	K5	743b6a819ced0f25	4	6
dke9	K6	7e9f1483bd026a5c	4	6
dke9	K7	e28f307cbd15649a	5	7
dke10	K0	8469bc1237e0daf5	4	6
dke10	K1	7d18ae4f90632cb5	4	6
dke10	K2	c8d1a29634e75f0b	3	5
dke10	K3	2b34c79df8501ea6	4	6
dke10	K4	83daef5147bc2069	6	7
dke10	K5	4c9bea76350f128d	5	6
dke10	K6	58e7301da692fbc4	7	7
dke10	K7	a3590d78c416bf2e	5	9

Нижче наведено статистичний розподіл параметрів для чотирьох та восьми бітових вузлів заміни, згенерованих випадково та рівноймовірно.

Аналізуючи результати статистичного дослідження розподілу параметрів для чотирьохбітових та восьмибітових s-блоків, зокрема, було знайдено підстановки з найменшими можливими значеннями параметрів (6) та (7), використання яких дозволить підвищити стійкість раундових перетворень по відношенню до цілочисельного різницевого криптоаналізу. Виходячи з отриманих результатів, верхні оцінки імовірностей цілочисельного раундового диференціалу для відображення (5) при відповідному виборі s-блоків можуть приймати значення $d_+^{\varphi}(\alpha,\beta) \le 0{,}04$.

Таблиця 2

Зведені значення параметрів (6)–(7) для вузлів заміни алгоритму ГОСТ

Значення δ_+^s	Кількість вузлів заміни	Значення Δ_+	Кількість вузлів заміни
0,1875	7	0,3125	18
0,25	43	0,375	42
0,3125	24	0,4375	17
0,375	5	0,5	2
0,4375	1	0,5625	1

Таблиця 3

Статистичний розподіл параметрів (6)–(7) для чотирьохбітових вузлів заміни (вибірка з 10000 підстановок)

Значення $d_+^{s(j)}$	Кількість підстановок	Значення $\delta_+^{s(j)}$	Кількість підстановок
0,1875	816	0,25	39
0,25	5305	0,3125	2254
0,3125	2920	0,375	4578
0,375	790	0,4375	2302
0,4375	131	0,5	668
0,375	37	0,5625	134
0,4375	1	0,625	20
		0,6875	5

Таблиця 4

Статистичний розподіл параметрів (6)–(7) восьмибітових вузлів заміни (вибірка з 10000 підстановок)

Значення $d_+^{s(j)}$	Кількість підстановок	Значення $\delta_+^{s(j)}$	Кількість підстановок
0.0195315	13	0,03125	8
0.0234375	4744	0,03515625	2520
0.0273438	4458	0,0390625	5235
0.03125	724	0,04296875	1836
0.0351563	57	0,046875	340
0.0390625	3	0,05078125	54
0.0429688	1	0,0546875	7

У такому випадку, якщо чотирибітові вузли заміни обрані з рекомендованих [17], але з найменшими значеннями параметрів (dke2 або dke7) такими, що $\max\limits_{\alpha,\beta \in V_n \setminus \{0\}} d^{\varphi}(\omega_i, \omega_{i+1}) \le 2 \cdot 0{,}375$, тоді може бути отримана оцінка виду $\max\limits_{\Omega} EDP(\Omega) \le 0{,}0024 \approx 2^{-9}$.

Звичайно, ця оцінка стійкості є надзвичайно

низькою. Але вона суттєво покращиться, якщо обрати чотирибітові вузли заміни так щоб $\max\limits_{\alpha,\beta\in V_n\setminus\{0\}} d^{\varphi}(\omega_i,\omega_{i+1}) \le 2\cdot 0{,}1875$. Тоді буде справедливою оцінка $\max\limits_{\Omega} EDP(\Omega) \le 1{,}13\cdot 10^{-9} \approx 2^{-29}$.

Нижче наведено приклади s-блоків (представлені у різному вигляді), які мають найменше значення відповідного параметра (8):

1)	11 15 14 7 8 12 3 1 13 10 4 5 0 9 6 2	bfe78c31da450962
2)	2 13 11 7 10 1 9 12 5 3 14 4 0 6 15 8	2db7a19c53e406f8
3)	7 0 9 2 3 11 1 13 10 8 5 4 6 14 15 12	70923b1da8546efc
4)	15 7 9 2 0 12 4 6 10 11 3 13 8 5 14 1	f7920c46ab3d85e1

Якщо ж у модифіканому алгоритмі ГОСТ використовувати 8-бітових вузлів заміни і обрати їх так, щоб $\max\limits_{\alpha,\beta\in V_n\setminus\{0\}} d^{\varphi}(\omega_i,\omega_{i+1}) \le 2\cdot 0{,}0195,$ то $\max\limits_{\Omega} EDP(\Omega) \le 2{,}58\cdot 10^{-30} \approx 2^{-98}$, що є дуже гарною оцінкою для алгоритму з 64-бітовим блоком.

Нижче наведено приклади s-блоків, які мають найменше значення відповідного параметра (8):

150 162 116 70 253 232 248 182 24 32 106 27 240 84 138 203 62 202 155 213 40 176 114 143 151 113 228 217 88 178 140 8 223 205 225 243 141 14 55 210 112 128 255 42 110 9 144 72 187 177 197 237 86 87 28 224 100 115 11 7 53 75 132 241 66 164 49 41 77 5 59 130 199 63 179 50 221 149 21 35 65 124 126 137 191 67 93 198 222 148 215 61 163 82 108 171 250 211 229 6 73 239 109 233 201 90 244 71 218 10 242 168 254 204 251 165 74 235 107 159 120 188 104 105 167 136 44 207 180 194 20 216 2 238 152 60 154 31 46 0 47 166 122 36 175 54 234 125 34 135 80 226 153 169 15 26 193 101 146 127 68 1 64 56 156 118 48 246 57 103 209 89 134 196 3 247 123 4 157 102 38 81 99 186 173 18 161 129 119 208 58 17 236 22 227 98 96 190 13 43 195 172 139 214 192 212 189 51 94 25 19 37 29 117 16 76 174 79 230 33 131 245 231 91 145 23 206 95 249 147 78 97 111 158 121 185 69 133 184 219 160 85 183 30 92 170 252 181 142 220 45 200 83 52 39 12

251 84 128 186 236 221 168 132 198 115 119 210 143 66 110 73 19 96 27 38 30 140 196 92 120 56 60 1 62 237 239 46 26 75 188 32 226 136 72 156 145 78 70 170 36 202 21 241 243 55 109 6 0 4 209 50 183 116 101 105 51 125 144 67 181 11 222 53 74 164 134 79 98 249 227 147 107 108 180 28 246 200 154 152 174 254 102 248 161 214 160 117 151 225 139 69 166 148 121 190 250 178 171 9 61 252 135 233 234 142 94 16 89 218 34 219 217 12 64 155 68 29 58 187 17 127 216 157 167 82 182 54 13 201 76 95 137 106 113 203 103 71 123 81 146 104 215 90 229 42 194 93 83 191 5 195 213 208 176 138 245 10 207 173 8 158 230 87 2 255 228 63 99 244 52 165 131 126 24 3 118 206 57 232 184 39 77 122 35 197 15 48 43 129 111 59 45 44 220 235 49 179 40 85 224 189 65 20 162 130 149 7 37 153 112 25 150 100 169 242 240 177 41 247 31 47 86 212 141 253 114 33 159 193 231 124 91 238 192 204 14 223 163 211 22 172 205 80 23 185 175 18 199 97 88 133

21 192 199 134 128 248 112 175 1 144 85 203 181 163 73 189 170 67 206 60 174 253 178 51 46 99 240 61 148 244 146 149 2 162 9 43 98 235 38 165 105 116 81 160 236 230 86 138 216 197 62 114 23 218 19 252 221 157 182 79 54 122 93 65 49 229 215 92 75 202 129 242 187 241 22 123 72 191 117 223 176 195 151 226 237 7 219 198 90 124 246 100 8 196 210 97 193 17 211 168 50 250 30 78 205 222 80 183 121 69 156 251 245 201 66 131 239 24 34 16 106 180 76 83 190 130 108 44 255 249 152 10 126 166 217 47 140 228 159 161 53 188 139 143 167 109 213 59 40 234 102 15 145 186 45 74 142 150 71 172 232 89 70 14 94 169 84 207 185 25 11 173 200 31 135 209 57 0 154 26 18 184 27 39 254 243 208 119 6 153 104 194 179 3 158 48 35 64 58 136 225 55 68 141 37 212 87 125 238 63 77 29 137 5 231 204 214 247 113 227 91 88 33 20 13 133 110 32 171 127 147 103 120 4 155 107 28 96 82 233 132 41 12 101 224 115 164 42 95 177 56 52 36 118 111 220

48 149 75 141 241 252 180 153 128 184 247 62 136 54 181 129 82 56 131 33 161 101 107 63 5 251 227 183 171 37 90 239 228 250 218 150 59 23 12 179 2 145 115 219 203 211 49 106 111 126 213 0 215 249 159 209 204 123 60 135 89 142 199 8 73 221 160 248 164 80 91 88 173 214 143 98 86 127 232 156 19 166 193 139 185 122 114 109 169 95 216 104 125 176 225 24 220 240 100 110 175 144 27 116 163 217 229 105 255 22 40 78 174 92 197 50 200 157 238 113 67 20 34 36 76 120 177 230 25 162 93 108 134 47 190 9 235 158 155 178 26 189 70 28 130 87 226 31 187 233 245 236 196 16 55 1 79 42 77 97 212 152 52 186 46 254 231 210 118 119 138 165 207 14 253 223 44 112 84 65 10 151 198 45 71 53 148 172 246 99 4 117 17 132 66 237 121 29 182 43 195 15 96 83 85 102 146 3 201 194 7 30 147 57 222 137 206 64 188 124 13 39 234 41 224 72 32 69 58 191

103 18 74 244 61 242 94 140 21 51 81 11 68
133 202 208 6 35 167 168 205 154 192 170 38
243

145 38 250 181 173 130 111 157 95 97
198 47 210 238 131 120 221 77 124 90 3 193
217 12 154 234 23 236 64 192 21 36 24 244
107 172 72 13 70 79 218 117 220 61 179 92
253 51 49 116 200 165 87 101 18 186 170 249
54 137 33 209 205 134 140 41 188 46 7 65
232 5 161 183 223 91 103 60 224 214 6 88
168 123 81 99 164 229 248 82 68 151 167 149
171 146 102 85 55 121 28 74 128 251 246 174
129 86 178 166 194 255 30 132 4 62 201 254
20 66 212 94 184 22 240 189 1 233 10 242
182 98 135 96 235 32 219 8 163 144 222 204
17 80 191 206 228 225 215 158 76 50 147 19
125 208 160 143 190 48 185 73 37 42 45 115
58 177 100 63 11 227 226 136 199 247 187 84
35 40 197 142 207 75 29 83 239 105 69 153
106 109 31 119 169 27 216 211 122 133 110 114
175 152 11

3. ПОБУДОВА ОЦІНОК ПРАКТИЧНОЇ СТІЙКОСТІ КАЛИНА-ПОДІБНИХ АЛГОРИТМІВ

Введемо необхідні позначення. Лінійний (над кільцем Z_{2^u}) оператор $A:(V_u)^p \to (V_u)^p$ задамо за допомогою матриці

$$A=\left(a_{ij}\right)_{i,j=1}^{p},\ a_{ij}\in V_u,$$

де для будь-якого $x=(x^{(p)},...,x^{(1)})\in V_n$:

$$A\,x^T=y^T=\left(y^{(p)},...,y^{(1)}\right)^T,\ y^{(i)}=\sum_{j=1}^{p}a_{ij}x^{(j)},$$

а операції множення та додавання виконуються у кільці Z_{2^u}. Позначимо $A_i=\left(a_{ip},...,a_{i1}\right)$. Тоді, в наших позначеннях, $y^{(i)}=A_i x^T$, тобто

$$A\,x^T=\left(A_p x^T,...,A_1 x^T\right)^T,$$

де під скалярним множенням розуміємо множення векторів з $\left(Z_{2^u}\right)^p$.

Аналогічно позначимо для оберненого оператора $A^{-1}=\left(A'_p,...,A'_1\right)$, де $A'_i,\ \ i=\overline{1,p}$ – рядки матриці A^{-1} (також пронумеровані у зворотному порядку, відповідно до нумерації координат вектора x). Тоді

$$A^{-1}x^T=\left(A'_p x^T,...,A'_1 x^T\right)^T.$$

Надалі розглядається лише такий оператор A, що для деякого фіксованого $l\in\mathbf{N}$: $wt\left(A'_j\right)\le l,\quad j=\overline{1,p}$.

Означення 2. В наших позначеннях називатимемо блоковий алгоритм шифрування (1) *модифікованим Калина-подібним алгоритмом,* якщо його раундова функція має вигляд:

$$f_k(x)=A\circ S(x*k),\qquad (9)$$

де $x\in V_n$ – відкритий текст, $n=pu,\ \ p\ge 2$, $x=(x_p,....,x_1)$, $x_i:V_u\to V_u$, $i=\overline{1,p}$, $k\in V_n$ – раундовий ключ, $*$ – операція побітового або модульного додавання, $S:V_n\to V_n$ – блок підстановки такий, що $S=(s^{(p)},...,s^{(1)})$, де $s^{(i)}:V_u\to V_u$.

Зазначимо, що модифікований зазначеним чином Калина-подібний алгоритм може містити:

1*) побітовий ключовий суматор;

2*) модульний ключовий суматор;

3*) операції модульного та побітового додавання чергуються в залежності від раунду.

Операція в ключовому суматорі і визначатиме властивості такого алгоритму.

Наступне твердження визначає для зазначених модифікованих Калина-подібних алгоритмів, чи є вони марковськими.

Лема 3. Залежно від ключового суматора модифікований Калина-подібний алгоритм з раундовою функцією (9) та ключовим суматором згідно з 1*)-3*) буде:

1*) марковським відносно операції побітового додавання $\oplus$ та узагальнено марковським відносно операції модульного додавання;

2*) марковським відносно операції модульного додавання + та узагальнено марковським відносно операції побітового додавання $\oplus$;

3*) узагальнено марковським відносно модульного і побітового додавання.

Доведення наведемо лише для 3*), оскільки інші пункти твердження доводяться безпосередньо, виходячи з аналогічних міркувань.

Розглянемо раундову функцію (9), позначимо її

$$f_k(x)=\varphi(x*k).$$

Для фіксованого $x\in V_n$ розглянемо вираз

$$2^{-n}\sum_{k\in V_n}\delta(f_k(x\circ_1\omega)\circ_2 f_k(x)^{-1},\omega')=$$

$$=2^{-n}\sum_{k\in V_n}\delta(\varphi((x\circ_1\omega)*k)\circ_2\varphi(x*k)^{-1},\omega').$$

Запишемо $x\circ_1\omega$ у такому вигляді: $x\circ_1\omega=\nu(x,\omega)*\omega*x$, де $\nu(x,\omega)=(x\circ_1\omega)*x^{-1}*\omega^{-1}$.

Зазначимо, що відображення $\omega\to\omega_0=\nu(x,\omega)*\omega$ при фіксованому $x\in V_n$ є перестановкою на V_n. Дійсно, якщо $\nu(x,\omega_1)*\omega_1=\nu(x,\omega_2)*\omega_2$, то

$$(x\circ_1\omega_1)*x^{-1}*\omega_1^{-1}*\omega_1=(x\circ_1\omega_2)*x^{-1}*\omega_2^{-1}*\omega_2,$$

звідки $x\circ_1\omega_1=x\circ_1\omega_2$, $\omega_1=\omega_2$.

Позначимо перестановку $\omega \to \nu(x,\omega) * \omega$ через $\sigma_x(\omega)$. З наведених вище міркувань випливає, що $\forall x \in V_n$:

$$2^{-n} \sum_{k \in V_n} \delta(\varphi((x \circ_1 \omega) * k) \circ_2 \varphi(x * k)^{-1}, \omega') =$$

$$= 2^{-n} \sum_{k \in V_n} \delta(\varphi(\nu(x,\omega) * x * \omega * k) \circ_2 \varphi(x * k)^{-1}, \omega') =$$

$$= 2^{-n} \sum_{k \in V_n} \delta(\varphi(\sigma_x(\omega) * k) \circ_2 \varphi_k(k)^{-1}, \omega'),$$

що й завершує доведення леми 3.

Твердження Леми 3 справедливе і у більш загальному випадку, а саме для такого шифру, у якого раундові функції мають вигляд $f_k(x) = \varphi(x * k)$, але є різними: наприклад, відрізняються операцією "*" у ключовому суматорі. У цьому випадку в твердження необхідно внести відповідні зміни щодо операції у ключовому суматорі.

Наступну лему можна вважати наслідком з Леми 3.

Лема 4. Для модифікованого Калина-подібного алгоритму з модульним ключовим суматором, справедлива така оцінка практичної стійкості до цілочисельного криптоаналізу:

$$EDP(\Omega) = \prod_{i=0}^{r-1} d_+^f(\omega_i, \omega_{i+1}).$$

Для побудови оцінок практичної стійкості модифікованих Калина-подібних алгоритмів відносно цілочисельного різницевого криптоаналізу скористаємось наступними результатами з [16].

Теорема 3 ([16]) Нехай раундова функція має вигляд $f_k(x) = A \circ S(x+k)$. Тоді справедлива така нерівність:

$$\forall \alpha, \beta \in V_n \setminus \{0\} \quad d_+^f(\alpha, \beta) \le \Delta_+,$$

де для кожного $i = \overline{1, p}$ покладемо

$$\Delta_+^{(i)} = \max_{\alpha, \gamma \in V_u \setminus \{0\}} \frac{1}{2^u} \sum_{k \in V_u} \left(\sum_{z=0}^{l+1} \delta\left(s^{(i)}(k+\alpha) - s^{(i)}(k), \gamma + z\right) \right) \quad (10)$$

та

$$\Delta_+ = \max\left\{\Delta_+^{(i)}, i = \overline{1, p}\right\}. \quad (11)$$

Теорема 4 ([16]) Нехай раундова функція має вигляд $f_k(x) = A \circ S(x \oplus k)$. Тоді справедлива наступна нерівність:

$$\forall \alpha, \beta \in V_n \setminus \{0\} \quad d_+^G(\alpha, \beta) \le \Delta_{\oplus +},$$

де для кожного $l = \overline{1, p}$ визначено

$$\Delta_{\oplus +}^{(i)} = \max_{\alpha, \gamma \in V_n \setminus \{0\}} \frac{1}{2^u} \sum_{k \in V_u} \left(\sum_{z=0}^{l+1} \delta\left(S^{(i)}(k \oplus \alpha) - S^{(i)}(k), \gamma + z\right) \right) \quad (12)$$

та

$$\Delta_{\oplus +} = \max\left\{\Delta_{\oplus +}^{(i)}, i = \overline{1, p}\right\}. \quad (13)$$

Наведені теореми встановлюють верхні оцінки стійкості раундових функцій, визначених у (9). Зауважимо, що час обчислення величин $\Delta_{\oplus +}$ та Δ_+ для довжини входу k (розмір одного s-блоку) становить $O(lpk^3 \log k)$ бітових операцій.

Використовуючи результати лем 3 та 4, а також теорем 4 і 5, можна побудувати оцінки практичної стійкості для модифікованих алгоритмів «Калина» та «Кузнєчик» відносно цілочисельного різницевого криптоаналізу.

Теорема 5.

1) для модифікованого Калина-подібного алгоритму, верхні оцінки імовірності узагальненої диференціальної характеристики алгоритму визначаються як:

$$EDP(\Omega) \le \max_{\alpha, \beta \in V_n \setminus \{0\}} d_{+,+}^f(\alpha, \beta) \cdot \left(\max_{\alpha, \beta \in V_n \setminus \{0\}} d_{\oplus,+}^f(\alpha, \beta) \right)^{N-1},$$

де N – кількість раундів блокового алгоритму;

2) для модифікованого алгоритму «Кузнєчик», верхні оцінки імовірності узагальненої диференціальної характеристики алгоритму визначаються як:

$$EDP(\Omega) \le \max_{\alpha, \beta \in V_n \setminus \{0\}} d_{\oplus,+}^f(\alpha, \beta)^{N-1},$$

де N – кількість раундів блокового алгоритму.

Нижче наведено статистичний розподіл параметрів для 100000 вузлів заміни згенерованих випадковим чином.

Таблиця 5

Статистичний розподіл параметру (10) при $l = 8$ (вибірка з 100000 випадкових 8-бітових s-блоків)

Значення Δ_+	Значення $2^8 \cdot \Delta_+$	Кількість
0,08203125	21	19
0,0859375	22	2632
0,08984375	23	19230
0,09375	24	32814
0,09765625	25	24959
0,1015625	26	12627
0,10546875	27	4999
0,109375	28	1804
0,11328125	29	595
0,1171875	30	241
0,12109375	31	52
0,125	32	15
0,12890625	33	11
0,1328125	34	2

Таблиця 6

Статистичний розподіл параметру (12) при $l = 8$ (вибірка з 100000 випадкових 8-бітових s-блоків)

Значення $\Delta_{\oplus+}$	Значення $2^8 \cdot \Delta_{\oplus+}$	Кількість
0,08203125	21	5
0,0859375	22	789
0,08984375	23	8671
0,09375	24	22491
0,09765625	25	24806
0,1015625	26	18980
0,10546875	27	11004
0,109375	28	6396
0,11328125	29	3261
0,1171875	30	1807
0,12109375	31	862
0,125	32	465
0,12890625	33	230
0,1328125	34	126
0,13671875	35	61
0,140625	36	20
0,14453125	37	16
0,1484375	38	6
0,15234375	39	3
0,15625	40	1

На рисунку 1 подано значення з таблиці 6 у вигляді діаграми. Як бачимо, основна кількість s-блоків мають значення параметра (12) у межах від 0,08203125 до 0,16015625, причому найбільше s-блоків характеризуються значеннями 0,09765625, 0,09375 та 0,1015625. Отриманий розподіл параметру (12) зберігається і на 100 000 інших випадкових блоків нелінійної підстановки.

Отримані дані статистичних розподілів параметрів (10) та (12) дозволяють сприймати оцінки цих параметрів для s-блоків, визначених у національних стандартах для алгоритмів «Калина» та «Кузнєчик», у контексті загальної картини, характерної для s-блоків такого розміру.

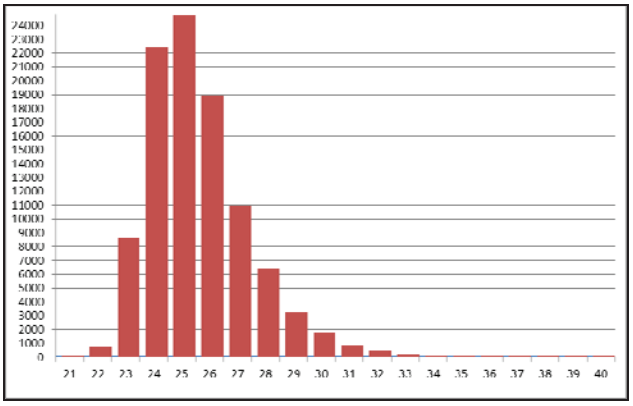


Рис.1

Використовуючи результати статистичного розподілу параметрів для $l = 8$ та восьмибітових s-блоків, зокрема, було знайдено підстановки з найменшими можливими значеннями цих параметрів, використання яких дозволить підвищити стійкість раундових перетворень по відношенню до цілочисельного різницевого криптоаналізу. Виходячи з отриманних результатів, верхні оцінки імовірностей цілочисельного раундового диференціалу для раундової функції (9) при відповідному виборі s-блоків, може приймати значення не більше 0,04 у випадку модульного ключового суматора та 0,05 побітового ключового суматора.

В таблиці 7 наведено статистичний розподіл параметрів для вузлів заміни, що рекомендовані в стандарті ДСТУ 7624:2014.

Таблиця 7

Статистичний розподіл параметрів (10), (11) восьмибітових вузлів заміни шифру ДСТУ 7624 («Калина»)

Підстановка	$\Delta_{+,+}$	$2^8 \cdot \Delta_{+}$
π_0	0,09765625	25
π_1	0,08984375	23
π_2	0,10546875	27
π_3	0,09375	24
${}_{-1}\pi_0$	0,11328125	29
${}_{-1}\pi_1$	0,08984375	23
${}_{-1}\pi_2$	0,10546875	27
${}_{-1}\pi_3$	0,09765625	25
max	0,11328125	29

Таблиця 8

Статистичний розподіл параметрів (12), та (13) восьмибітових вузлів заміни шифру ДСТУ 7624 («Калина»)

Підстановка	$\Delta_{\oplus+}$	$2^8 \cdot \Delta_{\oplus+}$
π_0	0,08984375	23
π_1	0,09375	24
π_2	0,0859375	22
π_3	0,09375	24
${}_{-1}\pi_0$	0,09375	24
${}_{-1}\pi_1$	0,08984375	23
${}_{-1}\pi_2$	0,09375	24
${}_{-1}\pi_3$	0,09375	24
max	0,09375	24

Використовуючи отримані дані, подані в таблицях 5–6, слід зауважити, що існує можливість обирати вузли заміни з такими значеннями параметрів, які забезпечуватимуть більшу стійкість Калина-подібних алгоритмів відносно цілочисельного різницевого криптоаналізу.

В такому випадку, якщо вузли заміни обрані з рекомендованих в стандарті ДСТУ7624:2014 (див. таблиці 7 та 8), тоді $\max\limits_{\alpha,\beta\in V_n\setminus\{0\}} d^f_{\oplus,+}(\alpha,\beta)\le 0{,}09375$ і $\max\limits_{\alpha,\beta\in V_n\setminus\{0\}} d^f_{+,+}(\alpha,\beta)\le 0{,}10546875$. Звідки, з урахуванням оцінки імовірності узагальненої диференціальної характеристики алгоритму з теореми 3 для 10 раундів зашифрування

$$EDP(\Omega)\le 5{,}9\cdot 10^{-11}\approx 2^{-34},$$

для 14 раундів зашифрування.

$$EDP(\Omega)\le 4{,}578\cdot 10^{-15}\approx 2^{-48},$$

для 18 раундів зашифрування

$$EDP(\Omega)\le 3{,}521\cdot 10^{-19}\approx 2^{-61}.$$

Якщо обрати вузли заміни, так щоб вони відповідали найменшим значенням параметрів (див. табл. 6) $\max\limits_{\alpha,\beta\in V_n\setminus\{0\}} d^f_{+,+}(\alpha,\beta)\le 0{,}08203125$ і $\max\limits_{\alpha,\beta\in V_n\setminus\{0\}} d^f_{+,+}(\alpha,\beta)\le 0{,}08203125$, у такому випадку для 10 раундів зашифрування отримали б $EDP(\Omega)\le 1{,}38\cdot 10^{-11}\approx 2^{-36}$ для 14 раундів зашифрування $EDP(\Omega)\le 6{,}248\cdot 10^{-16}\approx 2^{-51}$ і для 18 раундів зашифрування $EDP(\Omega)\le 2{,}829\cdot 10^{-20}\approx 2^{-65}$.

Для модифікованого алгоритму (з модульним ключовим суматором), при оптимальному виборі значень параметрів (див. таблицю 7) справедлива аналогічна оцінка.

В такому випадку, якщо використано вузол заміни із стандарту ГОСТ Р 34.12 2015, тоді для модифікованого алгоритму із побітовим додаванням у ключовому суматорі $\max\limits_{\alpha,\beta\in V_n\setminus\{0\}} d^f_{\oplus,+}(\alpha,\beta)\le 0{,}0898437$, звідки за теоремою 3 для 10 раундів зашифрування (враховуючи, що останній раунд не використовує нелінійну заміну, а лише побітове додавання ключа), отримаємо $EDP(\Omega)\le 3{,}814\cdot 10^{-10}\approx 2^{-31}$.

Якщо розглянути модифікований алгоритм із операцією модульного додавання у ключовому суматорі, його практична стійкість оцінюється величинами $\max\limits_{\alpha,\beta\in V_n\setminus\{0\}} d^f_{+,+}(\alpha,\beta)\le 0{,}0898437$, для одного раунду зашифрування та за теоремою 3

$$EDP(\Omega)\le 3{,}814\cdot 10^{-10}\approx 2^{-31}$$

для 10 раундів шифрування.

ВИСНОВКИ

В даній статті отримано оцінки верхніх меж практичної стійкості модифікованого ГОСТ-подібного алгоритму та модифікованих алгоритмів «Кузнєчік» та «Калина» до цілочисельного різницевого криптоаналізу у двох випадках: коли у ключовому суматорі реалізована операція модульного додавання або побітового додавання. Наведені результати дозволяють оцінити практичну стійкість алгоритмів блокового шифрування визначених у стандартах України та Росії відносно цілочисельного різницевого криптоаналізу.

Порівняння значень отриманих параметрів зі статистичними розподілами випадкових параметрів дає привід припускати, що під час проектування шифру «Кузнєчік», окрім стійкості до класичного побітового різницевого криптоаналізу, могла бути врахована необхідність практичної стійкості і до цілочисельного різницевого криптоаналізу. Неможливо стверджувати напевно, чи був такий тип атаки розглянутий авторами шифру під час проектування його s-блоку. Слід зазначити, щодо інших сучасних алгоритмів, стійкість до цілочисельного різницевого криптоаналізу не розглядалася ні при побудові шифру AES, ні шифру «Калина». Якщо припущення – вірне, то «Кузнєчік» стає першим алгоритмом шифрування, який би використовував нелінійні вузли заміни за замовчуванням із близькими до практично досяжних найменших значень параметрів, тобто тих, що забезпечують йому практичну стійкість раундових перетворень до цілочисельного різницевого криптоаналізу. До того ж показники «Калини», хоч не на багато, але гірші, ніж «Кузнєчіка». Найгіршу стійкість до цілочисельного різницевого криптоаналізу з операцією побітового додавання в ключовому суматорі має третій s-блок «Калини», а до цілочисельного різницевого криптоаналізу з операцією модульного додавання в ключовому суматорі – другий. Але цей недолік було вирішено за допомогою збільшення кількості раундів шифрування.

Література

[1] СТБ 34.101-31.2011 Информационные технологии и безопасность. Защита информации. Криптографические алгоритмы шифрования и контроля целостности [Електронний ресурс] // Режим доступу: – http://apmi.bsu.by/assets/files/std/belt-spec27.pdf- Назва з екрану.

[2] ГОСТ Р 34.12-2015 Информационная технология. Криптографическая защита информации. Блочные шифры.захисту інформації [Електронний ресурс] // Режим доступу: – http://tc26.ru/standard/gost/GOST_R_3412-2015.pdf - Назва з екрану.

[3] ДСТУ 7624:2014 «Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення [Електронний ресурс] // Режим доступу: – https://eprint.iacr.org/2015/650.pdf - Назва з екрану.

[4] *Олексійчук А.М., Ковальчук Л.В., Пальченко С.В.* Криптографічні параметри вузлів заміни, що характеризу-

ють стійкість ГОСТ-подібних блокових шифрів відносно методів лінійного та різницевого криптоаналізу. Захист інформації. – 2007, № 2. – С. 12 – 23.

[5] *Ковальчук Л. В., Пальченко С. В., Скрипник Л.В.* Застосування теорії узагальнених марковських шифрів для оцінювання стійкості сучасних блокових алгоритмів до методів різницевого криптоаналізу. – Науково-технічний збірник «Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні». – 2007, № 2 (16). – С. 70–84.

[6] *Ковальчук Л.* Обобщёные марковские шифры: оценка практической стойкости к методу дифференциального криптоанализа. Труды Пятой Общероссийской научной Конференции “Математика и безопасность информационных технологий” – (МаБИТ-06), 25-27 октября 2006. – С. 595–599.

[7] *Алексейчук А., Ковальчук Л., Шевцов А., Скрыпник Л.* Оценки практической стойкости блочного шифра «Калина» относительно разностного, линейного билинейного методов криптоанализа. Труды Седьмой Общероссийской научной Конференции “Математика и безопасность информационных технологий” – (МаБИТ-08), 30 октября – 2 ноября 2008. – С. 15–20.

[8] *X. Wang, H. Yu.* How to Break MD5 and Other Hash Functions. Advances in Cryptology EUROCRYPT'05, Lectures Notes in Computer Science 3494, Springer-Verlag, 2005, P. 19–35.

[9] *S. Cotini, R.L. Riverst, M.J.B. Robshaw, Y. Lisa Yin.* Security of the RC6^{TM} Block Cipher, Режим доступу: – https://people.csail.mit.edu/rivest/ContiniRivestRobshawYin-TheSecurityOfTheRC6BlockCipher.pdf - Назва з екрану.

[10] *Tomas A.* Berson Differential cryptanalysis mod 2^{32} with applications to MD5. Advanced in Cryptology. – CRYPTO’98 (LNCS 372). – 1999. – P. 95–103.

[11] *Ковальчук Л.* Построение верхних оценок средних вероятностей целочисленных дифференциалов композиции ключевого сумматора, блока подстановки и оператора сдвига. «Кибернетика и системный анализ» – 2010, №6, С. 89–96.

[12] *Ковальчук Л., Кучинская Н.* Построение верхних оценок средних вероятностей целочисленных дифференциалов раундовых функций блочных шифров определенной структуры. «Кибернетика и системный анализ» – 2012, №5, С. 71–81.

[13] *Lai X.* Markov ciphers and differential cryptanalysis / X. Lai, J.L. Massey, S. Murphy. Advances in Cryptology – EUROCRYPT’91, Proceedings. – Springer Verlag, 1991. – pp. 17–38.

[14] *Алексейчук А. Н. Ковальчук Л.В.* Верхние границы максимальных значений вероятностей дифференциальных и линейных характеристик шифра Фейстеля, содержащего сумматор по модулю 2^m . Прикладная радиоэлектроника. – 2006. – Т. 5, № 1. – С. 74–82.

[15] *Кучинская Н. В., Скрипник Л.В* Построение верхних оценок средних вероятностей целочисленных дифференциалов композиции ключевого сумматора, блока подстановки и произвольного оператора циклического сдвига. Спеціальні телекомунікаційні системи та захист інформації. – 2013. – Вип. 2(24). – С.26–32.

[16] *Ковальчук Л., Кучинська Н., Скрипник Л.* Побудова верхніх оцінок середніх імовірностей цілочисельних диференціалів композицій ключового суматора, блока підстановки та лінійного (над деяким кільцем) оператора . Науково-технічний збірник «Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні». – 2015. – №1(29). – С.33–45.

[17] Наказ Адміністрації Держспецзв'язку №114 Про затвердження Інструкції про порядок постачання і використання ключів до засобів криптографічного захисту інформації Редакція від 27.06.2013 [Електронний ресурс] // Режим доступу: – http://zakon3.rada.gov.ua/laws/show/z0729-07 - Назва з екрану.

Надійшла до редколегії 29.12.2017

Ковальчук Людмила Василівна, доктор технічних наук, професор, професор кафедри математичних методів захисту інформації, Фізико-технічний інститут НТУУ КПІ ім. Ігоря Сікорського, область наукових інтересів: сучасні методи криптоаналізу блокових алгоритмів шифрування, методи аналізу якості псевдовипадкових послідовностей, сучасні асиметричні криптосистеми та методи їх криптоаналізу, криптовалюти.

Кучинська Наталія Вікторівна, кандидат технічних наук, доцент кафедри інформаційної безпеки, Фізико-технічний інститут НТУУ КПІ ім. Ігоря Сікорського, область наукових інтересів: сучасні методи криптоаналізу блокових алгоритмів шифрування, методи аналізу якості псевдовипадкових послідовностей.

УДК 681.3.06:006.354

Оценки практической стойкости модифицированных стандартов блокового шифрования Украины и России относительно целочисленного разностного криптоанализа / Л.В. Ковальчук, Н.В. Кучинская // Прикладная радиоэлектроника: науч.-техн. журнал. – 2017. – Том 16, № 3, 4 – С. 155–165.

Рассмотрено одну из модификаций разностного криптоанализа, а именно целочисленный разностный криптоанализ. В статье получены научно-обоснованные оценки практической стойкости к целочисленному разностному криптоанализу модифицированных стандартов блочного шифрования Украины и России. Представлено зависимость полученных оценок от параметров, которые характеризуют s-блоки. Проведено сравнительный анализ значений этих параметров для всех алгоритмов, рассмотренных в работе. Также представлено статистическое распределение полученных параметров по случайной выборке из 100000 s-блоков.

Ключевые слова: разностный криптоанализ, стандарты блочного шифрования, s-блоки.

Табл.: 08. Рис.: 01. Библиогр.: 17 наим.

UDC 681.3.06:006.354

Estimates of the practical stability of the modified block encryption standards of Ukraine and Russia with respect to integer difference cryptanalysis / L.V. Kovalchuk, N.V. Kuchinska // Applied Radio Electronics: Sci. Journ. – 2017. – Vol. 16, № 3, 4. – P. 155–165.

One of the differential cryptanalysis modifications is considered, namely, the integer differential cryptanalysis. The paper provides scientifically grounded estimates of practical security to integer differential cryptanalysis of the block encryption modified standards of Ukraine and Russia. The dependence of the obtained estimates on the parameters that characterize s-blocks is presented. A comparative analysis of values of these parameters for all the algorithms considered in the work is carried out. A statistical distribution of the obtained parameters is also presented for a random sample of 100,000 s-blocks

Keywords: difference cryptanalysis, block encryption standards, s-blocks.

Tab.: 08. Fig.: 01. Ref.: 17 items.

ЛОКАЦИЯ И НАВИГАЦИЯ

УДК 621.382.2.029.64

ЧИСЛЕННО-АНАЛИТИЧЕСКИЙ МЕТОД РЕШЕНИЯ ЗАДАЧ ЛУЧЕВОЙ РАДИОТОМОГРАФИИ

А. Е. ПОЕДИНЧУК, К. А. ЛУКИН, С. К. ЛУКИН

В работе предлагается численно-аналитический метод решения задач фазовой томографии прозрачных неоднородных сред. Входной информацией для этого класса задач является измерение фазы волны, прошедшей через неоднородную среду. В геометрическом приближении фаза прошедшей волны выражается в виде интеграла от показателя преломления среды вдоль луча, соединяющего передатчик и приемник. В том случае, когда можно пренебречь рефракцией (характерные размеры неоднородностей превышают радиус Френеля), луч представляет собой прямую линию, соединяющую передатчик и приемник. Значения таких интегралов при различных положениях передатчика (приемника) используются в фазовой томографии для восстановления пространственной структуры крупномасштабных неоднородностей среды [1–4].

Ключевые слова: лучевая томография, обратные задачи электродинамики.

ВВЕДЕНИЕ

В данной работе на примере задач лучевой радиотомографии ионосферы Земли апробируется новый метод решения обратных задач для восстановления пространственной структуры крупномасштабных неоднородностей среды [1–4]. Рассматривается вариант спутниковой лучевой радиотомографии, реализуемой с помощью низкоорбитальных или высокоорбитальных искусственных спутников Земли (ИСЗ) [2]. Теоретической основой лучевой радиотомографии [2] является интегральное уравнение, связывающее разность фаз $\Delta\varphi = \varphi_0 - \varphi$ (φ_0 – фаза зондирующей волны, φ – фаза прошедшей волны через атмосферу) и распределение электронов концентрации N

$$\lambda r_e \int N ds = \Delta\varphi, \qquad (1)$$

где λ – длина зондирующей волны, r_e – классический радиус электрона.

Интегрирование в (1) осуществляется вдоль луча, соединяющего передатчик на ИСЗ, и приемник, расположенный на поверхности Земли. Таким образом, задача состоит в определении электронной концентрации N как функции пространственных переменных по известной (измеренной) разности фаз $\Delta\varphi$ при различных положениях ИСЗ и приемника.

Для решения такой задачи были предложены различные методы. Мы не будем анализировать достоинства и недостатки этих методов (достаточно подробный анализ которых изложен в [2]). Отметим только, что, в основном, эти методы используют аппроксимацию интегрального оператора, задаваемого уравнением (1), конечномерными операторами. Такая аппроксимация сводит уравнение (1) к конечной системе линейных алгебраических уравнений, которая, как правило, является недоопределенной. Эти системы уравнений имеют неединственное решение (проблемы неоднозначности и неполноты входных данных) [2]. Кроме того, точность восстановления функции N на прямую зависит от точности аппроксимации интегрального оператора (1). Поэтому повышение точности с необходимостью приводит к системам линейных алгебраических уравнений большой размерности. Численные построения решений таких систем уравнений требует разработки специальных методов [5].

Предлагаемый ниже метод решения уравнения (1) лишен этих недостатков. В частности, система линейных алгебраических уравнений, с помощью которой определятся функция N, имеет положительную полуопределенную симметричную квадратную матрицу. Это свойство позволяет для построения решения использовать хорошо известный метод α – регуляции Лаврентьева [6].

1. АЛГОРИТМ РЕШЕНИЯ ЗАДАЧ ЛУЧЕВОЙ РАДИОТОМОГРАФИИ

Прежде чем излагать основные этапы построения метода решения уравнения (1), следуя [2], введем параметры, характеризующие геометрию схемы регистрации входных данных задачи лучевой радиотомографии. Будем предполагать, не ограничивая общности, что ИСЗ движется по круговой орбите. Введем

полярную систему координат в плоскости, проходящей через центр Земли и орбиту ИСЗ. Тогда (r_0,α_0) – координаты ИСЗ, (R,α_i) – координаты приемника, расположенного на поверхности Земли (R – радиус Земли), β – угол места ИСЗ, 0 – центр Земли, $00'$ – ось полярной системы координат.

Используя результаты, полученные в [2], уравнение (1) можно представить в следующем виде

$$\lambda r_e R \int_0^{h_0} \frac{N(h,\tau)dh}{\sqrt{1-\frac{cos^2\beta}{(1+h)^2}}} = \Delta\varphi(\beta). \qquad (2)$$

Здесь

$$h=\frac{r}{R}-1,\ \tau=\alpha_i+\beta-arccos\left(\frac{\cos\beta}{1+h}\right),\ h_0=\frac{r_0}{R}-1.$$

Задача состоит в построении решения уравнения (2) по известной функции $\Delta\varphi(\beta)$. Суть предлагаемого метода построения решения такова. Предположим, что функцию $N(h,\tau)$ можно представить в виде

$$N(h,\tau)=\sum_{m=0}^{M} N_m(h)(\tau-\tau_i)^m, \qquad (3)$$

где коэффициенты $N_m(h)$ – некоторые неизвестные функции, подлежащие определению.

Подставим (3) в (2), тогда будем иметь

$$\Delta\varphi(\beta)=\lambda r_e R\sum_{m=0}^{M}\int_0^{h_0} N_m(h)Q_m(h,\beta)dh, \qquad (4)$$

где

$$Q_m(h,\beta)=\frac{\left(\beta-arccos\left(\frac{\cos\beta}{1+h}\right)\right)^m}{\sqrt{1-\frac{cos^2\beta}{(1+h)^2}}}. \qquad (5)$$

В задачах лучевой радиотомографии имеет место ситуация, когда функция $\Delta\varphi(\beta)$ задана (измерена) лишь для конечного множества углов места ИСЗ – β_p, $p=1,\ldots,P$

$$\varphi_p=\Delta\varphi(\beta_p). \qquad (6)$$

По этим значениям требуется найти все функции $N_m(h)$, $m=1,\ldots,M$. Понятно, что такая задача является типичной некорректной задачей [7]. Следуя работе [8], заменим ее следующей условной вариационной задачей

$$\sum_{m=0}^{M}\int_0^{h_0} N_m{}^2(h)dh=min. \qquad (7)$$

$$N_m(h),\ \eta\le m\le M,$$

$$\varphi_p=\sum_{m=0}^{M}\int_0^{h_0} N_m(h)Q_m{}^p(h)dh,\ p=1,\ldots,P. \qquad (8)$$

Здесь

$$Q_m^p(h)=\lambda r_e R Q_m(h,\beta_p). \qquad (9)$$

Для решения задачи (7), (8) воспользуемся методом множителей Лагранжа [9]. Для этого условно вариационной задаче (7) (8) ставится в соответствие семейство безусловных вариационных задач

$$\Phi(N_1(h),\ldots,N_m(h),\eta_1,\ldots,\eta_p)=min, \qquad (10)$$

$$N_m(h),\ 0\le m\le M.$$

Здесь функционал $\Phi(N_1(h),\ldots,N_m(h),\eta_1,\ldots,\eta_p)$ имеет вид

$$\Phi(N_1(h),\ldots,N_m(h),\eta_1,\ldots,\eta_p)=$$

$$=\sum_{m=0}^{M}\int_0^{h_0} N_m{}^2(h)dh+$$

$$+2\sum_{p=1}^{p}\eta_p\left(\varphi_p-\sum_{m=0}^{M}\int_0^{h_0} N_m(h)Q_m{}^p dh\right), \qquad (11)$$

η_p $p=1,\ldots,P$ – множители Лагранжа, с помощью которых учтены условия (8) исходной задачи (4).

Для нахождения функций $N_m(h)$, $m=0,\ldots,M$, доставляющих минимальное значение функционалу (11) необходимо вычислить производную Фреше и приравнять ее нулю. Опуская подробности вычисления, приведем окончательный результат. Функции $N_m(h)$, $m=0,\ldots,M$, при которых функционал (10) принимает минимальное значение, можно представить в следующем виде

$$N_m(h)=\sum_{p=1}^{P}\eta_p Q_m^p(h),\ m=0,\ldots,M. \qquad (12)$$

Множители Лагранжа η_p, $p=1,\ldots,P$ в формуле (12) являются решением системы линейных алгебраических уравнений.

$$\sum_{q=1}^{P} Q_{pq}\eta_q=\varphi_p,\ p=1,\ldots,P. \qquad (13)$$

Матричные элементы Q_{pq} выражаются через функции $Q_m^p(h)$ и имеют вид

$$Q_{pq} = \sum_{m=0}^{M} \int_0^{h_0} Q_m{}^p(h) Q_m{}^q(h) dh, \qquad (14)$$

$$p,q = 1,\ldots,P.$$

Как следует из (14), матрица $Q = \left(Q_{pq}\right)_{p,q=1}^{P}$ является симметричной и положительно полуопределенной матрицей, а ее размерность совпадает с количеством отсчетов угла места ИСЗ.

Таким образом, исходная задача лучевой радиотомографии сведена к решению системы линейных алгебраических уравнений (13).

Поскольку величины φ_p, $p = 1,\ldots,P$ получаются в результате измерений, то они известны с некоторой погрешностью $б_p$

$$\varphi_p^{б} = \varphi_p + б_p, \ p = 1,\ldots,P. \qquad (15)$$

Следовательно, при построении решения уравнений (13) следует находить устойчивые приближения решения системы уравнений

$$\sum_{q=1}^{P} Q_{pq}\eta_q = \varphi_p{}^{б}, \ p = 1,\ldots,P. \qquad (16)$$

Как было указано выше, матрица системы уравнений (16) является симметричной и положительно полуопределенной. Поэтому для ее решения можно воспользоваться методом α регуляции Лаврентьева [7]. Суть метода в следующем. Представим систему (16) в матричной форме

$$Q\eta = \varphi_{б}. \qquad (17)$$

Здесь $\eta = \left(\eta_p\right)_{p=1}$, $\varphi_{б} = (\varphi_p + б_p)_{p=1}^{P}$.

В соответствии с методом Лаврентьева уравнение (17) заменяется на регуляризованное уравнение

$$\alpha\eta_\alpha + Q\eta_\alpha = \varphi_{б}. \qquad (18)$$

где $\alpha > 0$ – параметр регуляризации.

Как легко видеть, уравнение (18) при любом $\alpha > 0$ имеет единственное решение

$$\eta_\alpha = \left(\alpha I + Q\right)^{-1}\varphi_{б}. \qquad (19)$$

Здесь I – единичная матрица, $\left(\alpha I + Q\right)^{-1}$ – обратная матрица.

Выбор параметра α осуществляется по невязке

$$\left\|\varphi_{б} - Q\eta_\alpha\right\|^2 = б^2, \qquad (20)$$

где $\|...\|$ – обозначает норму вектора в конечномерном пространстве,

$$б^2 = \sum_{p=1}^{P} б_p^2.$$

Обратную матрицу в (19) можно находить, например, с помощью разложения Холецкого [10].

ЗАКЛЮЧЕНИЕ

Таким образом, исходная задача лучевой томографии сведена к решению системы уравнений (18) с помощью которого функция электронной концентрации $N(h,\tau)$ выражается в следующем виде

$$N(h,\tau) = \sum_{p=1}^{P} \eta_p^{\alpha} \sum_{m=0}^{M} Q_m^p(h)\left(\tau - \tau_i\right)^m, \qquad (21)$$

$$Q_m^p(h) = \lambda r_e R \frac{\left(\beta_p - arccos\left(\frac{\cos\beta_p}{1+h}\right)\right)^m}{\sqrt{1 - \frac{cos^2\beta_p}{(1+h)^2}}}. \qquad (22)$$

где $\left(\eta_p^{\alpha}\right)_{p=1}^{P}$ – решение системы уравнений (18).

Отметим, что разработанный подход к решению задач лучевой томографии легко обобщается на случай, когда имеется несколько приемников. Кроме того, в представлении (3) для функции электронной концентрации были выбраны полиномиальные функции $\left(\tau - \tau_i\right)^m$, $m = 0,\ldots,M$, которые без особого труда могут быть заменены на любую систему линейно независимых функций.

Литература

[1] *Kak A., Sney M.* Principles of Computerized Tomography Imaging. N.Y. IEEE Press, 1988.

[2] *Куницын В.Е., Терещенко Е.Д., Андреева Е.С.* Радиотомография ионосферы. М.: Наука. 2007. – 336 с.

[3] *Кравцов Ю.А., Орлов Ю И.* Геометрическая оптика неоднородных сред. М.: Наука, 1980. – 304 с.

[4] *Кравцов Ю.А., Тинин М.В., Книжин С. И.* Дифракционная томография неоднородной среды при сильных вариациях фазы. Радиотехника и Электроника. – 2011. – Т 26, №7. – С. 816–822.

[5] *Страхов В.Я, Страхов А.В.* Аппроксимационный подход к решению задач гравиметрии и магнитометрии. II. Новые методы нахождения устойчивых приближенных решений систем линейных алгебраических уравнений с приближенно заданной правой частью: Российский журнал наук о Земле, 1999. – Т. 1, 5. – С. 353–400.

[6] *Лаврентьев М.М.* О некоторых некорректных задачах математической физики. Новосибирск: Изд-во Сибирского отделения АН СССР; 1962. – 82 с.

[7] *Иванов В.К., Васин В.В., Танана В.П.* Теория линейных некорректных задач и ее приложения. М. Наука, 1978. – 226 с.

[8] *Страхов В.Н.* Каким методом георфизики должны заменить метод Лаврентьева нахождения устойчивых приближенных решений систем линейных алгебраических уравнений с симмметричными положительно определенными матрицами и приближенно заданными векторами правых частей. Вычислительные технологии. 2007. – Т. 12, № 6. – С. 109–123.

[9] *Васильев В.В.* Численные методы решения экстремальных задач. М. Наука, 1980. – 518 с.

[10] *Воеводин В.В., Кузнецов Ю.А.* Матрицы и вычисления. М. Наука, 1984. – 318 с.

Поступила в редколлегию 15.11.2017

Поединчук Анатолий Ефимович, канд. физ.-мат. наук, старший научный сотрудник, зав. отдела дифракции и дифракционной электроники Института радиофизики и электроники им. А. Я. Усикова НАН Украины. Научные интересы: численные методы решения дифференциальных уравнений в частных производных, прямые и обратные задачи электродинамики.

Лукин Константин Александрович, фото и сведенья об авторе см. на стр. 128.

Лукин Сергей Константинович, окончил Харьковский Национальный Аэрокосмический ун-т «ХАИ» в 2008. С 2009 г. – мл. научный сотрудник отдела нелинейной динамики электронных систем в Институте радиофизики и Электроники им. О.Я. Усикова НАН Украины. Область интересов: цифровая обработка сигналов, в том числе в FPGA; программируемые шумовые радары; формирование когерентных изображений в наземных шумовых РСА; методы сжатых выборок (compressive sensing).

УДК 621.382.2.029.64

Чисельно-аналітичний метод вирішення проблем променевої томографії / А.Ю. Поединчук, К.О. Лукін, С.К. Лукін // Прикладна радіоелектроніка: наук.-техн. журнал. – 2017. – Том 16, № 3, 4. – С. 166–169.

У роботі пропонується чисельно-аналітичний метод вирішення проблем променевої томографії прозорих неоднорідних середовищ. Вхідною інформацією для цього класу задач є вимір фази хвилі, що пройшла через неоднорідне середовище. У геометричному наближенні фаза хвилі, що пройшла, виражається у вигляді інтеграла від показника заломлення середовища уздовж променя, що з'єднує передавач і приймач. У цьому випадку, коли можна знехтувати рефракцією (характерні розміри неоднорідностей перевищують радіус Френеля), промінь є прямою лінією, що з'єднує передавач і приймач. Значення таких інтегралів при різних положеннях передавача (приймача) використовуються у фазовій томографії для відновлення просторової структури великомасштабних неоднорідностей середовища.

Ключові слова: променева томографія, обернені задачі електродинаміки.

Бібліогр.: 10 найм.

UDC 621.382.2.029.64

Numerical-analytical method for solving the problems of radiotomography / A.Yu. Poedinchuk, K.A. Lukin, S.K. Lukin.// Applied Radio Electronics: Sci. Journ. – 2017. – Vol. The paper proposes a numeric-analytical method for solving the problems of phase tomography of transparent inhomogeneous media. The input information for this class of problems is the measurement of the phase of waves passing through an inhomogeneous medium. In the geometric approximation, the phase of the transmitted wave grows in the form of an integral of the refractive index of the medium along the beam connecting a transmitter and a receiver. In the case where the refraction can be neglected (the characteristic dimensions of the inhomogeneity exceed the Fresnel radius), the ray is a straight line connecting the transmitter and the receiver. The values of such integrals at different positions of the transmitter (receiver) are used in phase tomography to reconstruct the spatial structure of large-scale medium inhomogeneities.

Keywords: ray tomography, inverse problems of electrodynamics.

Ref.: 10 items.

УДК 681.3.06

КРИВА ЕДВАРДСА НАД КІЛЬЦЕМ ЛИШКІВ ЯК ДЕКАРТІВ ДОБУТОК КРИВИХ ЕДВАРДСА НАД СКІНЧЕНИМИ ПОЛЯМИ

О. Ю. БЕСПАЛОВ, Н. В. КУЧИНСЬКА

Розглядається крива, що є узагальненням кривої Едвардса над кільцем лишків; показано, що за певних умов множина її точок утворює групу відносно визначеної операції; ця група ізоморфна декартовому добутку відповідних кривих Едвардса над скінченими полями.

Ключові слова: еліптичні криві, еліптичні криві Едвардса, криптосистеми на еліптичних кривих, група точок еліптичної кривої.

ВСТУП

Еліптичні криві над кільцем лишків Z_n є цікавим об'єктом як з точки зору криптології, так і з точки зору алгебри. Особливістю таких кривих є подвійна можливість їх використання: як для побудови RSA-подібних криптосистем [1, 2], так і для криптоаналізу класичних криптосистем, що базуються на важкорозв'язуваності задачі факторизації, таких як криптосистеми RSA та Рабіна [3,4].

Вперше RSA-подібні еліптичні алгоритми були запропоновані у роботі [1], після чого тема продовжувала активно обговорюватися як у напрямку удосконалення таких криптосистем, наприклад, [2], так і у напрямку їх криптоаналізу [5,6]. Також вдосконалювались і алгоритми факторизації на еліптичних кривих, наприклад, [7,8].

Що стосується RSA-подібних криптосистем на еліптичних кривих, то їх основними перевагами є такі:

- для побудови такої криптосистеми можна використовувати еліптичні криві з довільними параметрами;
- можна будувати як алгоритми шифрування, так і цифрового підпису;
- можна будувати цифрові підписи довільної довжини, зокрема такої довжини, як і повідомлення;
- на відміну від класичної криптосистеми RSA, її еліптичний аналог є стійким до атаки гомоморфізмів;
- інструментарій, що використовується в ході побудови цих криптосистем, може бути використаний для побудови еліптичних аналогів ρ-методу Поларда.

З появою в 2007 році такої форми подання еліптичних кривих, як форма Едвардса [9–11], визначення закону точок додавання такої кривої та доведення ізоморфізму з кривою у формі Вейєрштрасса, було виявлено перспективність її застосування в криптографії. Особливими перевагами еліптичних кривих у формі Едвардса є:

- наявність одного параметра замість двох для кривої у формі Вайєрштрасса;
- відсутність точки на нескінченності, оскільки як нейтральний елемент групи точок кривої Едвардса використовується точка кривої зі скінченими координатами;
- вища швидкість виконання операції додавання та подвоєння точок порівняно з аналогічними операціями для кривих у формі Вайєрштрасса;
- однаковий закон додавання та подвоєння точок кривої, що унеможливлює проведення таймінгової та ємнісної атаки для відновлення бітового запису скаляру.

Тому природним є питання можливості застосування еліптичних кривих Едвардса у зазначених вище напрямках замість класичних еліптичних кривих у формі Вейєрштраса. При цьому слід зазначити, що перенесення криптосистем і методів з еліптичних кривих у формі Вейєрштраса на еліптичні криві у формі Едвардса не є тривіальним.

1. ОСНОВНІ РЕЗУЛЬТАТИ

Під час дослідження узагальнення кривої Едвардса над кільцями лишків Z_n виявилась ще одна її цікава властивість, яку також можна віднести до переваг кривої у формі Едвардса порівняно з кривою у формі Вейєрштрасса. Ця властивість полягає у тому, що, за певних умов, крива Едвардса над кільцем Z_n, де $n = p \cdot q$ (p, q – різні прості числа), утворює групу відносно "стандартної" операції додавання точок. Далі, ця група є ізоморфною декартовому добутку груп, утворених точками відповідних кривих Едвардса над полями F_p та F_q.

Властивості кривих Едвардса над простими полями досить добре вивчені, і, внаслідок зазначеного ізоморфізму, відповідні результати можна використати під час дослідження властивостей таких кривих над кільцями.

Зазначимо, що аналогічний ізоморфізм для кривих у формі Вайєрштрасса побудувати неможливо, внаслідок існування так званої "нескінченно віддаленої точки" кривої, в якої не існує афінних координат.

Результати цієї роботи саме і стосуються побудови ізоморфізму між зазначеними групами точок кри-

вих Едвардса. Ці результати можна застосовувати як для побудови відповідних криптосистем, так і для побудови аналогів методу Лєнстра [7].

Нехай $n \in Z$. Позначимо через $Q_n = \left\{ x \in Z_n^* \mid \exists y \in Z_n^* : x \equiv y (\mathrm{mod}\, n) \right\}$ множину всіх квадратичних лишків за модулем n і $\tilde{Q}_n = \left\{ x \in Z_n^* \mid x \notin Q_n \wedge \left(\frac{x}{n} \right) = 1) \right\}$ множину всіх псевдоквадратів за модулем n. Зазначимо, що якщо $n = p \cdot q$, де p, q – різні прості числа, то

$$\forall x \in Q_n \cup \tilde{Q}_n : \left(\frac{x}{n} \right) = \left(\frac{x}{p} \right) \left(\frac{x}{q} \right) = 1,$$

$$\forall x \notin Q_n \cup \tilde{Q}_n : \left(\frac{x}{n} \right) = -1.$$

Для будь-яких $n \in Z$ та $d \in Z_n^*$ позначимо

$$E_n = \left\{ (x, y) \in Z_n \times Z_n \mid x^2 + y^2 = 1 + dx^2 y^2) \right\}, \quad (1)$$

де операції додавання та множення виконуються за модулем n.

Якщо n – просте число, $d \in Z_n^* \setminus Q_n$, тоді (1) задає деяку криву Едвардса над простим скінченним полем F_n. Але в даній статті розглянемо більш загальний випадок – коли n є добутком двох різних простих чисел. Тому надалі p, q – різні прості числа, $n = p \cdot q$.

Мета даної роботи полягає в тому, щоб звести дослідження кривої E_n, визначеної в (1), до більш відомих та досліджених об'єктів – кривих Едвардса E_p та E_q над простими скінченими полями F_p та F_q, відповідно.

В цій роботі розглянемо найпростіший випадок, коли крива E_n не містить «особливих» точок (тобто точок з нескінченими координатами). Такі криві, згідно з [12], називатимемо повними кривими Едвардса. Авторами роботи буде показано, що в такому випадку E_n утворює групу відносно деякої операції додавання її точок та, більше того, ця група ізоморфна декартовому добутку груп, утвореному кривими Едвардса E_p та E_q.

На множині E_n, визначеній у (1), задамо операцію, яка співпадає зі стандартною операцією додавання точок кривої Едвардса [12], а саме

$$\forall (x_1, y_1), (x_2, y_2) \in E_n : (x_1, y_1) + (x_2, y_2) = (x_3, y_3),$$

де

$$x_3 = \frac{x_1 x_2 - y_1 y_2}{1 - d x_1 x_2 y_1 y_2}, \; y_3 = \frac{x_1 y_2 + x_2 y_1}{1 + d x_1 x_2 y_1 y_2}. \quad (2)$$

Це так званий «модифікований універсальний закон додавання», визначений у [12]. Тут під операціями додавання та множення розуміємо відповідні операції за модулем n, а під операцією ділення – множення на обернений елемент за модулем n.

Сформулюємо відповідні результати у вигляді наступних лем, які доводять, що операція (2) задана коректно.

Для кривої E_n, визначеної в (1) та простого p, $p \mid n$, визначимо множину $\left(E_n\right) \mathrm{mod}\, p$, що є підмножиною $Z_p \times Z_p$, за таким правилом:

$$\left(E_n\right) \mathrm{mod}\, p = \left\{ \left(x \,\mathrm{mod}\, p, y \,\mathrm{mod}\, p \right) \mid (x, y) \in E_n \right\}. \quad (3)$$

Аналогічно, для кожної точки $P = (x, y) \in E_n$ визначимо точку

$$P \,\mathrm{mod}\, p = \left(x \,\mathrm{mod}\, p, y \,\mathrm{mod}\, p \right). \quad (4)$$

Лема 1. Множина $\left(E_n\right) \mathrm{mod}\, p$, визначена згідно з (3), співпадає з множиною точок еліптичної кривої E_p, визначеною в (1), де замість параметра d використовується $d \,\mathrm{mod}\, p$.

Доведення. Нехай $P = (x, y) \in E_n$, тоді $P \,\mathrm{mod}\, p \in \left(E_n\right) \mathrm{mod}\, p$.

Покажемо, що $P \,\mathrm{mod}\, p \in E_p$. Для цього достатньо довести, що для її координат $\left(x \,\mathrm{mod}\, p, y \,\mathrm{mod}\, p \right)$ виконується рівність (1):

$$\left(x \,\mathrm{mod}\, p \right)^2 + \left(y \,\mathrm{mod}\, p \right)^2 =$$

$$= 1 + \left(d \,\mathrm{mod}\, p \right) \left(x \,\mathrm{mod}\, p \right)^2 \left(y \,\mathrm{mod}\, p \right)^2, \quad (5)$$

де всі операції у лівій та правій частині виконуються за модулем числа p.

Оскільки $P = (x, y) \in E_n$, то відповідно до (1), виконується конгруенція

$$x^2 + y^2 = 1 + dx^2 y^2 \left(\mathrm{mod}\, n \right). \quad (6)$$

Але, оскільки $p \mid n$, то за властивістю конгруенцій [13,14]

$$x^2 + y^2 = 1 + dx^2 y^2 \left(\mathrm{mod}\, p \right),$$

що еквівалентно виконанню рівності (5), звідки і отримаємо $P \,\mathrm{mod}\, p \in E_p$.

Нехай тепер деяка точка $P' = (x', y') \in E_p$, тобто

$$\left(x' \right)^2 + \left(y' \right)^2 = 1 + \left(d \,\mathrm{mod}\, p \right) \left(x' \right)^2 \left(y' \right)^2 \left(\mathrm{mod}\, p \right). \quad (7)$$

Покажемо, що $P' \in E_n \bmod p$, тобто що

$$\exists P = (x, y) \in E_n : \begin{cases} x \bmod p = x'; \\ y \bmod p = y'. \end{cases}$$

Визначимо криву E_q згідно з (1) з параметром $d \pmod q$ та виберемо на ній довільну точку $P'' = (x'', y'') \in E_q$. Тоді для координат цієї точки виконується рівність

$$(x'')^2 + (y'')^2 = 1 + (d \bmod q)(x'')^2 (y'')^2, \quad (8)$$

де всі операції виконуються за $\bmod q$.

Тепер визначимо точку $P = (x, y)$ з таких умов:

$$\begin{cases} x = x' \pmod p; \\ x = x'' \pmod q, \end{cases} \qquad \begin{cases} y = y' \pmod p; \\ y = y'' \pmod q. \end{cases} \quad (9)$$

Для завершення доведення достатньо показати, що $P = (x, y) \in E_n$, тобто що для (x, y) виконується рівність (1).

Дійсно, з рівностей (7) та (8) отримуємо:

$$\begin{cases} x^2 + y^2 = 1 + dx^2 y^2 \pmod p; \\ x^2 + y^2 = 1 + dx^2 y^2 \pmod q, \end{cases}$$

звідки, за властивостями конгруенцій та, враховуючи, що НСД$(p, q) = 1$, отримаємо

$$x^2 + y^2 = 1 + dx^2 y^2 \pmod n,$$

тобто $P = (x, y) \in E_n$. Крім того, згідно з (9), $P \bmod p = (x \bmod p, y \bmod p) = P' = (x', y')$ і лему доведено.

Наступна Лема доводить, що за умови $d \in \tilde{Q}_n$ крива E_n не має особливих точок та операція на ній задана коректно.

Лема 2. Нехай $P = (x_1, y_1), Q = (x_2, y_2) \in E_n$, $n = p \cdot q$, де p, q - прості, $d \in \tilde{Q}_n$. Тоді:

1) $dx_1 x_2 y_1 y_2 \neq \pm 1 (\bmod n)$; (10)

2) множина E_n, задана співвідношенням (1), замкнена відносно операції, визначеної в (2).

Доведення. 1) Спершу зазначимо, що якщо $d \in \tilde{Q}_n$, то $\left(\frac{d}{p}\right) = \left(\frac{d}{q}\right) = -1$. Дійсно, оскільки $d \in \tilde{Q}_n$, то $\left(\frac{d}{n}\right) = 1$, звідки $\left(\frac{d}{p}\right) = \left(\frac{d}{q}\right)$. Але при цьому рівність $\left(\frac{d}{p}\right) = \left(\frac{d}{q}\right) = 1$ не може виконуватися, оскільки $d \notin Q_n$. Тому $\left(\frac{d}{p}\right) = \left(\frac{d}{q}\right) = -1$.

У цьому випадку, очевидно, $d \bmod p \notin Q_p$, $d \bmod q \notin Q_q$, а, отже, згідно з [12]

$$\begin{cases} dx_1 x_2 y_1 y_2 \bmod p \neq \pm 1, \\ dx_1 x_2 y_1 y_2 \bmod q \neq \pm 1. \end{cases} \quad (11)$$

Доведемо, від супротивного, що тоді виконується і умова (10). Припустимо, що (10) не виконується. Тоді $\exists\, x_1, x_2, y_1, y_2$ такі, що $(x_1, y_1), (x_2, y_2) \in E_n$ та

$$dx_1 x_2 y_1 y_2 \equiv 1 (\bmod n) \text{ або } dx_1 x_2 y_1 y_2 \equiv -1 (\bmod n). \quad (12)$$

Але в цьому випадку виконуватиметься також одна з рівностей

$$(d \bmod p)(x_1 \bmod p)(x_2 \bmod p)(y_1 \bmod p)(y_2 \bmod p) \equiv$$

$$\equiv 1 (\bmod p)$$

або

$$(d \bmod p)(x_1 \bmod p)(x_2 \bmod p)(y_1 \bmod p)(y_2 \bmod p) \equiv$$

$$\equiv -1 (\bmod p). \quad (13)$$

За лемою 1, це, зокрема, означає, що на кривій E_p, яка задається згідно з (2) з параметром $d \bmod p$, існують такі точки $P = (x_1 \bmod p, y_1 \bmod p)$ та $Q = (x_2 \bmod p, y_2 \bmod p)$, для координат яких виконується одна з рівностей (13). Але, оскільки $d \in \tilde{Q}_n$, то як було зазначено раніше, $\left(\frac{d \bmod p}{p}\right) = \left(\frac{d}{p}\right) = -1$, і згідно з [12] існування точок P та Q, для координат яких виконується (13) у цьому випадку неможливе. Оскільки прийшли до суперечності, то перше твердження леми доведено.

2) Оскільки за умови $d \in \tilde{Q}_n$ криві Едвардса E_p та E_q, визначені відповідно до (1) з параметрами $d \bmod p$ та $d \bmod q$, утворюють групи (без особливих точок) відносно відповідних операцій, то їх декартовий добуток $E_p \times E_q$ з компонентними операціями є групою.

У пункті 1) цієї леми було показано, що вирази (2) є коректними у сенсі, що їх знаменники не перетворюються в 0. Тепер покажемо, що результатом операції (2) також є точка кривої E_n.

Нехай P, $Q \in E_n$. $P = (x_1, y_1)$ та $Q = (x_2, y_2)$. Позначимо, $Z = P + Q = (x_3, y_3)$, де x_3, y_3 визначено згідно з (3). Потрібно довести, що $Z \in E_n$, тобто, що для її координат (x_3, y_3) виконується рівняння (1).

Розглянемо відповідні точки

$$P_p = P \bmod p, \; Q_p = Q \bmod p,$$

$$P_q = P \bmod q\,,\quad Q_q = Q \bmod q\,.$$

За лемою 1, $P_p, Q_p \in E_p$ та $P_q, Q_q \in E_q$, де криві E_p та E_q задаються згідно з (1) з параметрами $d \bmod p$ та $d \bmod q$, відповідно.

За властивостями конгруенцій та за лемою 1,

$$P_p + Q_p = Z \bmod p = Z_p \in E_p\,,$$

$$P_q + Q_q = Z \bmod q = Z_q \in E_q\,.$$

Отже, для координат точок Z_p та Z_q виконується рівняння (1) з параметрами $d \bmod p$ та $d \bmod q$, відповідно. Але для їх координат також виконуються конгруенції

$$\begin{cases} x_3 \equiv x_3 \bmod p \pmod p; \\ y_3 \equiv y_3 \bmod p \pmod p; \\ x_3 \equiv x_3 \bmod q \pmod q; \\ y_3 \equiv y_3 \bmod q \pmod q; \\ d \equiv d \bmod p \pmod p; \\ d \equiv d \bmod q \pmod q. \end{cases}$$

Тому, за властивостями конгруенцій, також виконуватимуться конгруенції

$$\begin{cases} x_3^2 + y_3^2 = 1 + dx_3^2 y_3^2 \pmod p, \\ x_3^2 + y_3^2 = 1 + dx_3^2 y_3^2 \pmod q. \end{cases} \qquad (14)$$

Оскільки НСД $(p,q) = 1$, то з (14) випливає виконання конгруенції

$$x_3^2 + y_3^2 = 1 + dx_3^2 y_3^2 \pmod n\,,$$

тобто для точки $Z = (x_3, y_3)$ виконується рівність (1), звідки $Z \in E_n$.

Лему повністю доведено.

Тепер сформулюємо теорему про структуру алгебраїчної системи E_n з операцією, визначеною в (2).

Теорема 1. Нехай p, q – різні прості числа, $n = p \cdot q$, $d \in \tilde{Q}_n$. Тоді :

1) множина E_n з операцією (2) утворює абелеву групу;

2) $E_n \cong E_p \times E_q$, де E_p та E_q – криві Едвардса, визначені згідно з (1) з параметрами $d \bmod p$ та $d \bmod q$, відповідно.

Доведення. Як було зазначено раніше, з умови $d \in \tilde{Q}_n$ випливає $d \bmod p \notin Q_n$ та $d \bmod q \notin Q_q$, тому відповідні еліптичні криві E_p та E_q є повними кривими Едвардса [12]. Отже, E_p та E_q, відносно відповідних операцій (згідно з (2)) є абелевими групами, тому їх декартовий добуток $E_p \times E_q$ також є абелевою групою відносно відповідної (покомпонентної) операції. Побудуємо відображення $\phi : E_n \to E_p \times E_q$ таким чином:

$\forall P = (x, y) \in E_n$:

$$\phi(P) = \left(P \bmod p, P \bmod q\right) =$$

$$= \left(\left(x \bmod p, y \bmod p\right), \left(x \bmod q, y \bmod q\right)\right).$$

Для доведення теореми необхідно довести такі властивості цього відображення:

1) ϕ – бієкція;

2) $\forall P, Q \in E_n : \phi(P+Q) = \phi(P) + \phi(Q)$.

Доведемо бієктивність відображення ϕ. Нагадаємо, що згідно з лемою 1, криві $(E_n) \bmod p$ та $(E_n) \bmod q$ співпадають з кривими E_p та E_q, заданими згідно з (1). Покажемо, що для будь-якої пари точок $P_1 = (x_1, y_1) \in E_p$, $P_2 = (x_2, y_2) \in E_q$, $\exists! P = (x, y) \in E_n : \phi(P) = (P_1, P_2)$.

Обчислимо x та y за системами конгруенцій

$$\begin{cases} x \equiv x_1 \pmod p, \\ x \equiv x_2 \pmod q, \end{cases} \quad \begin{cases} y \equiv y_1 \pmod p, \\ y \equiv y_2 \pmod q. \end{cases} \qquad (15)$$

За китайською теоремою про лишки $\exists! x \in Z_n$ та $\exists! y \in Z_n$ для яких виконуються системи (15). Таким чином залишається зазначити, що за властивістю конгруенцій, для x та y справедлива рівність (1), де операції виконуються за модулем n. Звідси $P = (x, y) \in E_n$ і бієктивність відображення доведено.

Доведемо, що це відображення зберігає операцію. Для цього потрібно переконатись у виконанні рівності

$$\forall P, Q \in E_n : \phi(P+Q) = \phi(P) + \phi(Q)\,. \qquad (18)$$

За побудовою відображення ϕ, ліва частина рівності (18) дорівнює

$$\phi(P+Q) = \left(\left(P+Q\right) \pmod p, \left(P+Q\right) \pmod q\right) =$$

$$= \left(\frac{x_1 x_2 - y_1 y_2}{1 - dx_1 x_2 y_1 y_2} \pmod p, \frac{x_1 y_2 - x_2 y_1}{1 + dx_1 x_2 y_1 y_2} \pmod q \right) =$$

$$= \left(\frac{(x_1 \bmod p)(x_2 \bmod p) - (y_1 \bmod p)(y_2 \bmod p)}{1 - d(x_1 \bmod p)(x_2 \bmod p)(y_1 \bmod p)(y_2 \bmod p)} \pmod p, \right.$$

$$\left. \frac{(x_1 \bmod q)(y_2 \bmod q) - (x_2 \bmod q)(y_1 \bmod q)}{1 + d(x_1 \bmod q)(x_2 \bmod q)(y_1 \bmod pq)(y_2 \bmod q)} \pmod q \right) =$$

$$= \left(P \bmod p + Q \bmod p, P \bmod q + Q \bmod q\right) =$$

$$= \left(P \bmod p, P \bmod q\right) + \left(Q \bmod p, Q \bmod q\right) =$$

$$\phi(P) + \phi(Q),$$

і рівність (18) доведена.

ВИСНОВКИ

Таким чином, у роботі повністю описано структуру кривої Едвардса над кільцем лишків Z_n для випадку, коли проекції цієї кривої на поля Z_p та Z_q є повними кривими.

Зазначимо, що у випадку $d \notin \tilde{Q}_n$ проекції кривої E_n на вказані поля не будуть повними, там з'являться «особливі точки» [12], тобто точки з нескінченними координатами. Тому в цьому випадку ізоморфізм $E_n \cong E_p \times E_q$ не може бути доведений за аналогією до теореми 1. Тому наведене питання є темою подальших досліджень.

В даній роботі також показано, що множина точок кривої утворює групу відносно операції додавання точок, яка визначається подібно до операції на кривій Едвардса над F_p. Встановлено ізоморфізм групи точок кривої Едвардса над Z_n, де $n = p \cdot q$, а p, q – різні прості числа, декартовому добутку груп $Z_p \times Z_q$, утворених точками кривих Едвардса над відповідними полями. Ці результати дозволяють звести дослідження властивостей нового об'єкта – кривої E_n над кільцем Z_n, $n = p \cdot q$, до дослідження властивостей «проекцій» цієї кривої на Z_p та Z_q, які є досить добре дослідженими.

Детальніше про практичне значення отриманих тут результатів, а саме про їхнє застосування до методів факторизації, мова йтиме у наступних роботах. Зокрема, буде показано, що з їхнім використанням обґрунтування методу Лєнстра та оцінка часу його роботи виконується суттєво простіше, ніж це зроблено у [7,13].

Література

[1] *K. Koyama, U.M. Maurer, T. Okamoto and S.A. Vanstone*, "New Public-Key Schemes Based on Elliptic Curves over the Ring Zn", CRYPTO' 91 Abstracts, Santa Barbara, CA, pp. 6-1 to 6-7, August 11–15, 1991.

[2] *N. Demytko.* A new elliptic curve based analogue of RSA. In T. Helleseth, edit., Advances in Cryptology – EUROCRYPT '93 , vol.765 of Lect. Notes in Comp.Science, p.40–49. Springer-Verlag, 1994.

[3] *A.K. Lenstra and H.W. Lenstra,* Jnr. "Algorithms in Number theory", University of Chicago, Department of computer Science, Technical Report # 87-008, 1987.

[4] *D.M. Bressoud*, Factorisation and Primality Testing, Springer-Verlag, New York, 1989.

[5] *B.S. Kaliski* Jr. A chosen message attack on Demytko's elliptic curve cryptosystem. Journal of Cryptology, 10(1):71–72, 1997.

[6] *D. Bleichenbacher, M. Joye, J.-J. Quisquarter,* A new and optimal chosen-message attack on RSA-type cryptosystems, LNCS 1334, Proc. Information and Communications Security – ICICS'97, Springer-Verlag, (1997), pp.302-313.

[7] *H.W. Lenstra,* Jr. Factoring integers with elliptic curves. Annuals of Mathematics, 126: 649-673, 1987.

[8] *Беспалов О.Ю., Панасюк І.І.* Метод Лєнстра та особливості його застосування на кривих Едвардса. Перспективні напрями захисту інформації: матеріали третьої всеукраїнської наук.-пр.конф. – м.Одеса, 02-06 вересня 2017р. – Одеса:ОНАЗ, 2017. – с. 4-6

[9] *Edwards H.M.* A normal form for elliptic curves. Bulletin of the American Society, Volume 44, Number 3, July 2007, PP.393-422.

[10] *Bernstein D.J., Lange T.* Faster Addition and Doubling on Elliptic Curves. Advances in Cryptology - ASIACRYPT'2007 (Proc. 13th Int.Conf. On the Theory and Application of Cryptology and Information Security. Kuching, Malaysia. December 2-6, 2007). Lect. Notes Comp. Sci. V.4833, Berlin: Springer, 2007. P.29-50.

[11] *Bernstein Daniel J., Lange Tanja, Farashahi Reza Rezaeian.* Binary Edwards curves. Cryptographic hardware and embedded systems - CHES 2008, 10th international workshop, Washington, D.C.

[12] *Бессалов А.В.* Эллиптические кривые в форме Эдвардса в криптографии: монография. – Киев. Изд-во «Политехника», 2017.-272 с.

[13] *Коблиц Н.* Курс теории чисел и криптографии. – М.: Научное изд-во ТВП, 2001. – 254 с.

[14] *Ковальчук Л.В., Кучинська Н.В.* Теоретична криптологія-2: теорія чисел та її застосування в криптоаналізі. – Київ: ІСЗЗІ «КПІ ім. Ігоря Сікорського», 2016. – 106с.

Поступила в редколлегию 29.12.2017

Беспалов Олексій Юрійович, аспірант, Фізико-технічний інститут НТУУ КПІ ім. Ігоря Сікорського. Область наукових інтересів: алгебра, асиметрична криптологія, еліптичні криві, криві Едвардса, програмування, блокчейн, старт-контракти.

Кучинська Наталія Вікторівна, фото та відомості про автора див. на стор. 164.

УДК 681.3.06:006.354

Структура группы точек кривой Эдвардса над кольцом вычетов и ее применение в криптологии / А.Ю. Беспалов, Н.В. Кучинская, // Прикладная радиоэлектроника: науч.-техн. журнал. – 2017. – Том 16, № 3, 4 – С. 170–175.

Рассматривается эллиптическая кривая, которая является обобщением кривой Эдвардса над кольцом вычетов; в работе показано, что при определенных условиях, множество ее точек образует группу относительно определенной операции; данная группа изоморфна декортовому произведению соответствующих кривых Эдвардса над конечными полями.

Ключевые слова: эллиптические кривые, эллиптические кривые Эдвардса, криптосистемы на эллиптических кривых, группа точек эллиптической кривой.

Библиогр.: 14 наим.

UDC 681.3.06:006.354

Edwards curve group of points structure over a residue ring and its application in cryptology / O. Yu. Bespalov, N. V. Kuchinska // Applied Radio Electronics: Sci. Journ. – 2017. – Vol. 16, № 3, 4. – P. 170–175.

The curve is considered which is the generation of Edward's curve over the residue ring. It is shown that under some conditions, the set of its points forms a group with respect to some definite operation. This group is isomorphic to the Decart product of correspondent Edward's curves over the prime fields.

Keywords: elliptic curves, Edwards elliptic curves, elliptic curve cryptosystems, group of elliptic curve points.

Ref.: 14 items.