О возможности защиты информации в телекоммуникационных OFDM-системах с помощью многопараметрических ортогональных преобразований

С. А. Мартюгин, С. В. Поршнев

***Аннотация*—Обеспечение информационной безопасности является одним из важнейших направлений в области беспроводных систем связи. Традиционные методы защиты информации основаны на верхних уровнях сетевой модели OSI, однако их надёжность значительно снижается для сценариев, где легитимные и нелегитимные пользователи используют общую физическую среду.**

В статье представлена система связи с технологией мультиплексирования с ортогональным частотным разделением каналов (OFDM – orthogonal frequency-division multiplexing), в которой вместо традиционных ортогональных преобразований (ОП), например, преобразования Уолша, Хаара, Фурье, используются их дробные (ДрОП) или многопараметрические (МОП) реализации. Такие преобразования зависят от конечного набора независимых параметров α (в случае дробных ОП) или $\alpha_0 =,...,= \alpha_{N-1}$ (в случае МОП), при изменении которых меняется их облик. При $\alpha = \pi / 2$, или $\alpha_0 =,...,= \alpha_{N-1} = \pi / 2$ преобразования принимают форму классического ОП, а при $\alpha = 0$, или $\alpha_0 =,...,= \alpha_{N-1} = 0$ вырождаются в тождественное преобразование. Для успешного обмена информацией необходимо знать параметры используемого в данный момент ДрОП или МОП, которые могут периодически меняться.

Приведены результаты моделирования несанкционированного доступа к OFDM-системе, в которой используется однопараметрическое преобразование Фурье-Баргманна (ДрПФБ), которые показывают, что такая система позволяет обеспечить лучшую защищённость информации по сравнению с традиционной OFDM-системой.

Предложены походы, призванные повысить защищенность информации, передаваемой в OFDM-системах, основанных на использовании ДрОП и МОП.

***Ключевые слова*— Обработка сигналов, дискретное преобразование Фурье, дробное преобразование Фурье, OFDM.**

Статья получена 11.02.2024

Степан Александрович Мартюгин, Уральский федеральный университет имени первого Президента России Б. Н. Ельцина, stmart2608@gmail.com

Сергей Владимирович Поршнев, д.т.н., профессор, Уральский федеральный университет имени первого Президента России Б. Н. Ельцина, ведущий научный сотрудник, Институт математики и механики им. Н.Н. Красовского Уральского отделения РАН, s.v.porshnev@urfu.ru

I. Введение

Угроза несанкционированного доступа к системе передачи информации (информационной системе (ИС)) по беспроводным каналам связи, включенная под шифром УБИ.083 в Банк данных угроз информации Федеральной службы по техническому и экспортному контролю Российской Федерации [1], заключается в наличии у нарушителя возможности получения доступа к ресурсам всей дискредитируемой ИС, через используемые в ее составе беспроводные каналы передачи данных. Данная угроза обусловлена слабостями протоколов идентификации/аутентификации (таких как WEP, WPA и WPA2, AES), используемых для доступа к беспроводному оборудованию. Ее реализация оказывается возможной при выполнении одновременно следующих условий:

1) наличия у нарушителя специализированного программного обеспечения, реализующего функции эксплуатации уязвимостей протоколов идентификации/аутентификации беспроводных сетей;
2) нахождения в точке приема сигналов дискредитируемой беспроводной сети.

Источником угрозы является нарушитель с низким потенциалом [2]. Объектами воздействия на ИС являются сетевой узел, учётные данные пользователя, сетевой трафик, аппаратное обеспечение. Последствиями реализации угрозы являются нарушения конфиденциальности, целостности и доступности информации, находящейся в ИС.

Одним из возможных способов реализации данной угрозы безопасности информации является подслушивание, организуемое перехватом радиосигнала (анонимное подслушивание). В этой связи разработка и применение соответствующих методов и технических средств противодействия данной угрозе безопасности информации является актуальной.

К обсуждаемому классу ИС относятся системы беспроводной связи, цифрового телевидения, радиовещания, передачи спутниковых данных, навигации, в том числе беспилотных летательных аппаратов, в которых широко используется технология мультиплексирования с ортогональным частотным

разделением каналов – OFDM [3], математическим базисом которой является преобразование Фурье, относящееся к классу ортогональных преобразований [4].

Для обеспечения конфиденциальности передаваемой информации в таких системах обычно используют криптографические средства защиты, что, в свою очередь, уменьшает скорость передачи информации и существенно увеличивает их стоимость. В этой связи был проведен ряд теоретических исследований с целью обоснования возможности создания методов защиты передаваемой информации в OFDM-системах на физическом уровне модели OSI [5, 6, 7].

В статье приведены теоретические обоснования метода защиты информации в системах с OFDM, в которой вместо классического преобразования Фурье могут использоваться различные ДрОП и МОП. Эти преобразования зависят от параметров α и $\alpha_0,...,\alpha_{N-1}$ (для ДрОП и МОП соответственно), которые могут изменяться независимо друг от друга. Параметр α принимает значения от 0 до 2π, а вектор $\boldsymbol{\theta}=\alpha_0,...,\alpha_{N-1}$ принадлежит параметрическому пространству ($(N-1)$-мерному тору) $(\alpha_0,...,\alpha_{N-1})\in \mathbf{Tor}^{N-1}[0,2\pi]=(0,2\pi]^{N-1}$. В качестве ДрОП и МОП могут использоваться дробные (ДрПФ) и многопараметрические (МППФ) преобразования Фурье.

При изменении параметров α или $\alpha_0,...,\alpha_{N-1}$ меняется и форма поднесущих OFDM-системы. Если приёмной стороне неизвестны текущие значения этих параметров (или текущая форма поднесущих), то правильная демодуляция принятого сигнала будет невозможной. Таким образом, параметры α и $\alpha_0,...,\alpha_{N-1}$, известные только легитимным пользователям, можно использовать как дополнительные ключи безопасности. При этом, очевидно, что подбор параметров МОП методом перебора их значений за приемлемое время невозможен. Например, если в системе используется МППФ $\mathsf{F}^{(\alpha_0,...,\alpha_{N-1})}$, размерностью $N=1024$, то для того, чтобы правильно подобрать значения параметров $\alpha_0,...,\alpha_{N-1}$ придётся просканировать пространство $(0,2\pi]^{1023}$. При этом параметры $\boldsymbol{\theta}=\alpha_0,...,\alpha_{N-1}$ могут периодически меняться.

Статья имеет следующую структуру: в секции II проведён краткий обзор теории ДрПФ и МППФ, в секции III описана модель OFDM-системы с ДОП или МОП, в секции IV приведено описание вычислительного эксперимента, проведенного с целью подтверждения возможности защиты передаваемой информации предложенной OFDM-системой, в секции V обсуждаются его результаты.

II. Дробные и многопараметрические преобразования Фурье

Пусть $\mathsf{T}=\left[t(x,y)\right]$ – произвольное дискретное ортогональное (или унитарное) $(N\times N)$-преобразование, λ_n и $\Psi_n(x)$ – его собственные значения и собственные вектора соответственно, где $n=0,\ldots,N-1$. Пусть $\mathbf{U}_N=\left[\Psi_0(x)\,|\,\Psi_1(x)\,|\,\vdots\,|\,\Psi_{N-1}(x)\right]$ – матрица, составленная из собственных векторов T-преобразования. Тогда собственным разложением преобразования $\mathbf{T}$ будет:

$$\begin{aligned}\mathsf{T}&=\left[t(x,y)\right]\\&=\sum_{n=0}^{N-1}\lambda_n\Psi_n(x)\Psi_n(y)\\&=\mathbf{U}\cdot\mathbf{diag}(\lambda_0,...,\lambda_{N-1})\cdot\mathbf{U}^{-1}.\end{aligned}\qquad(1)$$

Определение 1. Для произвольных вещественных чисел $a_0,\ldots,a_{N-1}$ существует следующее многопараметрическое T-преобразование (МОП):

$$\mathsf{T}^{(a_0,\ldots,a_{N-1})}=\mathbf{U}\cdot\mathbf{diag}\left(\lambda_0^{a_0},\ldots,\lambda_{N-1}^{a_{N-1}}\right)\cdot\mathbf{U}^{-1}\qquad(2)$$

Определение 2. Если $a_0=\ldots=a_{N-1}=a$, то преобразование (2) называется дробным T-преобразованием (ДОП):

$$\mathsf{T}^{a}=\mathbf{U}\cdot\mathbf{diag}\left(\lambda_0^{a},\ldots,\lambda_{N-1}^{a}\right)\cdot\mathbf{U}^{-1}=\mathbf{U}\cdot\mathbf{\Lambda}^{a}\cdot\mathbf{U}^{-1}\qquad(3)$$

При $a=1$ имеем исходное преобразование $\mathsf{T}^1=\mathbf{U}\mathbf{\Lambda}\mathbf{U}^{-1}$, а при $a=0$ преобразование вырождается в тождественное: $\mathsf{T}^0=\mathbf{U}\mathbf{\Lambda}^0\mathbf{U}^{-1}=\mathbf{I}$. Семейства $\left\{\mathsf{T}^{(a_0,\ldots,a_{N-1})}\right\}_{(a_0,\ldots,a_{N-1})\in\mathbb{R}}$ и $\left\{\mathsf{T}^{a}\right\}_{a\in\mathbb{R}}$ формируют, соответственно, многопараметрическую и однопараметрическую строго непрерывные унитарные группы, где умножение выполняется следующим образом: $\mathsf{T}^{(a_0,\ldots,a_{N-1})}\cdot\mathsf{T}^{(b_0,\ldots,b_{N-1})}=\mathsf{T}^{(a_0+b_0,\ldots,a_{N-1}+b_{N-1})}$ и $\mathsf{T}^{a}\cdot\mathsf{T}^{b}=\mathsf{T}^{a+b}$.

Пусть $\mathsf{F}=\left[e^{-j\frac{2\pi}{N}t\omega}\right]$ – дискретное $(N\times N)$–преобразование Фурье (ДПФ). Собственными функциями оператора преобразования Фурье являются функции Эрмита [8]:

$$\Psi_n(x)=\frac{1}{\sqrt{2^n n!\sqrt{\pi}}}H_n(x)e^{-x^2/2},\qquad(4)$$

где $H_n(x)=(-1)^n e^{x^2}\frac{d^n}{dx^n}e^{x^2}$ – многочлен Эрмита порядка $n\in\mathbb{N}$, и

$$\begin{aligned}\mathsf{F}\left[\Psi_n(x)\right]&=\frac{1}{2\pi}\int_{-\infty}^{+\infty}\Psi_n(x)e^{-2\pi jyx}dx\\&=\lambda_n\Psi_n(y)=e^{-j\frac{\pi}{2}n}\Psi_n(y),\end{aligned}\qquad(5)$$

где $\lambda_n=(-j)^n=e^{-j\frac{\pi}{2}n}$ является собственным числом, соответствующим n-ой собственной функции. Тогда оператор ДПФ имеет следующее собственное разложение:

$$\begin{aligned}\mathsf{F} &= \mathbf{U}\left\{\mathbf{diag}\left(e^{-j\frac{\pi}{2}n}\right)\right\}\mathbf{U}^{-1}\\ &= \sum_{n=0}^{\infty} e^{-j\frac{\pi}{2}n}\Psi_n(x)\Psi_n(y),\end{aligned} \tag{6}$$

где $\mathbf{U} = \left[\Psi_0(i)\,|\,\Psi_1(i)|,...\right]$ – матрица, составленная из собственных векторов оператора ДПФ.

Определение 3. Дискретным дробным преобразованием Фурье является следующее преобразование:

$$\begin{aligned}\mathsf{F}^{a} &= \left[be^{a}(x,y)\right]\\ &= \mathbf{U}\left\{\mathbf{diag}\left(e^{-j\frac{\pi}{2}na}\right)\right\}\mathbf{U}^{-1}\\ &= \sum_{n=0}^{N-1} e^{-j\frac{\pi}{2}na}\Psi_n(x)\Psi_n(y),\end{aligned} \tag{7}$$

где, $a \in \mathbb{R}$. Существует также и α -параметризация, где $\alpha = a\pi/2$, $\alpha \in \mathbb{R}$.

Баргманн в [8] получил выражение для ядра этого преобразования:

$$\begin{aligned}be^{a}(x,y) &= \sum_{n=0}^{\infty} e^{-j\alpha n}\Psi_n(x)\Psi_n(y)\\ &= e^{-\left(x^2+y^2\right)}\sum_{n=0}^{\infty}\frac{e^{-j\alpha n}H_n(x)H_n(y)}{2^n n!\sqrt{\pi}},\end{aligned} \tag{8}$$

которое суммированием по формуле Мехлера было приведено в [9], [10] к следующему виду:

$$be^{a}(x,y) = \sqrt{\frac{1-j\cot\alpha}{2\pi}}\cdot e^{\frac{j}{2\sin\alpha}\left[\left(x^2+y^2\right)\cos\alpha-2xy\right]} \tag{9}$$

Преобразование (9) в дальнейшем будем называть дробным преобразованием Фурье-Баргманна (ДрПФБ).

Определение 4. Дискретным многопараметрическим преобразованием Фурье является следующее преобразование:

$$\begin{aligned}\mathsf{F}^{\mathbf{a}} &= \mathsf{F}^{(a_0,a_1,...,a_{N-1})}\\ &= \mathbf{U}\left\{\mathbf{diag}\left(e^{-j\frac{\pi}{2}na_n}\right)\right\}\mathbf{U}^{-1}\\ &= \sum_{n=0}^{N-1} e^{-j\frac{\pi}{2}na_n}\Psi_n(x)\Psi_n(y),\end{aligned} \tag{10}$$

где $\mathbf{a} = \left(a_0, a_1, ..., a_{N-1}\right)$, $a_i \in \mathbb{R}$.

Так как $\mathsf{F}^4 = \mathbf{I}$, то операторы (7) и (10) являются периодическими с периодом 4. Они формируют непрерывные унитарные мультипликативные группы:

$\mathsf{F}^{(a_0,a_1,...,a_{N-1})}\cdot\mathsf{F}^{(b_0,b_1,...,b_{N-1})} = \mathsf{F}^{\left(a_0\underset{4}{\oplus}b_0,a_1\underset{4}{\oplus}b_1...,a_{N-1}\underset{4}{\oplus}b_{N-1}\right)}$,

$\mathsf{F}^{a}\cdot\mathsf{F}^{b} = \mathsf{F}^{a\underset{4}{\oplus}b}$, где $a_i \underset{4}{\oplus} b_i = \left(a_i + b_i\right)\bmod 4$, $\forall i = 0,1,...,N-1$. Таким образом, параметры $a_0, a_1, ..., a_{N-1}$ и a меняются в пределах $\left(\mathbb{R}/4\mathbb{R}\right)^{N-1} = [0,4)^{N-1}$ и $\mathbb{R}/4\mathbb{R} = [0,4)$ соответственно. В случае α – параметризации имеем $\mathsf{F}^{(\alpha_0,\alpha_1,...,\alpha_{N-1})}\cdot\mathsf{F}^{(\beta_0,\beta_1,...,\beta_{N-1})} = \mathsf{F}^{\left(\alpha_0\underset{4}{\oplus}\beta_0,\alpha_1\underset{4}{\oplus}\beta_1...,\alpha_{N-1}\underset{4}{\oplus}\beta_{N-1}\right)}$ и $\mathsf{F}^{\alpha}+\mathsf{F}^{\beta} = \mathsf{F}^{\alpha\underset{2\pi}{\oplus}\beta}$, где $\alpha\underset{2\pi}{\oplus}\beta = (\alpha+\beta)\bmod 2\pi$, $\forall i = 0,1,...,N-1$. Параметры $\alpha_0, \alpha_1, ..., \alpha_{N-1}$ и α меняются в пределах $\left(\mathbb{R}/4\mathbb{R}\right)^{N-1} = [0,2\pi)^{N-1}$ и $\mathbb{R}/4\mathbb{R} = [0,2\pi)$ соответственно.

III. Модель системы OFDM с МОП

Пусть

$$\mathbf{CM}_d = \left\{z^{(b_0,b_1,...,b_{d-1})} \in \mathbf{C}\,\middle|\,\left(b_0,b_1,...,b_{d-1}\right) \in \mathbf{B}_2^d\right\}$$

будет сигнальным созвездием, состоящим из 2^d точек $z^{\left(b_0,b_1,...,b_{d-1}\right)} = z^{(\mathbf{b})}$ комплексной плоскости $\mathbf{C}$, пронумерованных целыми числами, записанными в двоичной системе счисления $\left(b_0,b_1,...,b_{d-1}\right) \in \mathbf{B}_2^d$. Здесь $\mathbf{B}_2^d = \{0,1\}^d$ – d -мерный двоичный куб.

Информационные сообщения в OFDM-системе представляют собой последовательности комплексных чисел, каждое из которых представляет собой точку сигнального созвездия (или сигнальный символ) $z^{(\mathbf{b})} \in \mathbf{CM}_d^N \subset \mathbf{C}_d^N$.

Сигнал, предаваемый OFDM-системой, является комплекснозначной функцией вида:

$$s(t) = e^{j\omega_0 t}\sum_{n=0}^{N-1} z_n\varphi_n(t), \tag{11}$$

где ω_0 – несущая частота, $\varphi_n(t)$ – некоторый ортонормированный базис комплекснозначных сигналов.

Для классической OFDM-системы базисными функциями являются гармонические сигналы вида $\varphi_n(t) = e^{j2\pi n\Delta f t}$, где Δf – шаг сдвига по частоте, равный расстоянию между поднесущими, причём $\Delta f = 1/\tau$, где τ – длительность OFDM символа. Тогда выполняется условие ортогональности $\int_0^{\tau}\varphi_q(t)\varphi_l^{*}(t)\,dt = \begin{cases}1, & q = l,\\ 0, & q \neq l.\end{cases}$ Это необходимо для устранения взаимного влияния поднесущих, позволяя повысить плотность передачи информации, подавить межканальную интерференцию и значительно упростить схему передатчика и приёмника, так как позволяет не использовать разделительный фильтр, который необходим для систем с частотным разделением каналов (FDM).

Цифровая система передачи данных является системой с дискретным временем, в которой период дискретизации выбирается так, чтобы на длительности символа τ укладывалось целое число отсчётов. Обозначив это число как N , получим набор моментов времени $t_k = kT = k\tau/N$, где $T = \tau/N$ – интервал дискретизации, k – номер отсчёта. Тогда в момент времени t_k :

$$\varphi_n(t_k) = e^{j2\pi n\Delta f t_k} = e^{j2\pi n(1/\tau)k\tau/N} = e^{j2\pi nk/N}, \tag{12}$$

где $0 \le t < \tau$. Следовательно, комплексным OFDM-символом будет:

$$\begin{aligned} s(t) &= e^{j\omega_0 t}\sum_{n=0}^{N-1} z_n \varphi_n(t_k) \\ &= e^{j\omega_0 t}\sum_{n=0}^{N-1} z_n e^{j2\pi nk/N} \\ &= e^{j\omega_0 t}\left(\mathsf{F}_N^{-1}\mathbf{z}\right), \end{aligned} \tag{13}$$

где $0 \le k < N$, $\mathsf{F}_N^{-1} = \left[e^{j2\pi nk/N}\right]_{n,k=0}^{N-1}$ – матрица обратного ДПФ, $\mathbf{z}$ – вектор сигнальных символов.

Кроме ДПФ в качестве поднесущих могут использоваться вейвлет-преобразования [11], последовательности Голея [12] и псевдослучайные последовательности [13].

В исследуемой далее OFDM-системе в качестве поднесущих $\{\varphi_n(t)\}_{n=0}^{N-1}$ используются базисные функции многопараметрических преобразований Фурье-Баргманна $\{\varphi_n(t\,|\,\boldsymbol{\theta})\}_{n=0}^{N-1}$, где $\boldsymbol{\theta} = (\theta_0, \theta_1, ..., \theta_{M-1})$ – набор параметров, от которых зависят все базисные функции. Это могут быть как степенные параметры используемого МОП ($a_0, a_1, ..., a_{N-1}$), так и параметры алгоритма его расчёта (например, могут использоваться разные выражения собственных векторов [16]). При изменении параметров $\boldsymbol{\theta} = (\theta_0, \theta_1, ..., \theta_{M-1})$ изменяются тип, свойства и характеристики OFDM-системы, что можно использовать для решения широкого круга адаптационных телекоммуникационных задач.

Структурная схема предложенной OFDM системы с ДрПБФ приведена на Рис.1. На вход системы поступает набор двоичных символов (информационное сообщение) $\mathbf{b}[m]$, $m = 0,1,...$ который разбивается на группы из d бинарных символов $\mathbf{b}[m] = \mathbf{b}[nd + r] \to \mathbf{b}[n] = (b_0[n], b_1[n], ..., b_{d-1}[n])$, где $\mathbf{b} \in \mathbf{B}_2^d = \{0,1\}^d$, $r = 0,1,...,d-1$, $m = 0,1,...$. Из этих групп формируют последовательности из N символов $\mathbf{b}[n] = \mathbf{b}[lN + k] \to \mathbf{B}[l] = (\mathbf{b}_0[l], \mathbf{b}_1[l], ..., \mathbf{b}_{N-1}[l])$, которые называются временными слотами (l –индекс).

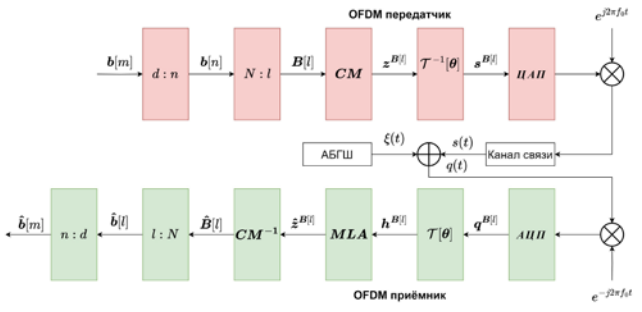

Рис. 1. Структурная схема OFDM-системы с МОП.

Каждое число $\mathbf{b}[l]$ интерпретируется как адрес в памяти, где хранится комплексное число $z^{(b[l])}$ из сигнального созвездия. Арифметическое устройство по очереди обращается к памяти по N адресам и извлекает из памяти N комплексных чисел:

$$\mathbf{z}^{(\mathbf{B}[l])} = \begin{bmatrix} \mathbf{CM}\{\mathbf{b}_0[l]\} \\ \mathbf{CM}\{\mathbf{b}_1[l]\} \\ \vdots \\ \mathbf{CM}\{\mathbf{b}_{N-1}[l]\} \end{bmatrix} = \begin{bmatrix} z_0^{(\mathbf{b}_0[l])} \\ z_1^{(\mathbf{b}_1[l])} \\ \vdots \\ z_{N-1}^{(\mathbf{b}_{N-1}[l])} \end{bmatrix}.$$

Полученный N - мерный вектор $\mathbf{z}^{(\mathbf{B}[l])}$ оценивается с помощью обратного МОП с параметрами $\boldsymbol{\theta} = (\theta_0, \theta_1, ..., \theta_{M-1})$, которые используются в системе в настоящий момент времени. В результате формируется новый N - мерный вектор, который называется дискретным групповым сигналом:

$$\mathbf{s}^{(\mathbf{B}[l])} = \mathsf{T}^{-1}[\boldsymbol{\theta}] \cdot \mathbf{z}^{(\mathbf{B}[l])}, \tag{14}$$

Полученный сигнал поступает на цифроаналоговый преобразователь, формируя передаваемый в линию связи сигнал OFDM – $s(t)$.

Приёмник имеет зеркальную по отношению к передатчику структуру. Он принимает сигнал $q(t) = s(t) + \xi(t)$, где $\xi(t)$ – аддитивный белый гауссовский шум (АБГШ), который дискретизируется и квантуется в аналого-цифровом преобразователе. Далее, сигнал делится на N параллельных потоков и происходит оценка информационного сообщения ($\mathbf{q}^{(\mathbf{B}[l])}$) с помощью прямого МОП с параметрами $\boldsymbol{\theta} = (\theta_0, \theta_1, ..., \theta_{M-1})$, которые использовались при формировании сообщения:

$$\mathbf{h}^{(\mathbf{B}[l])} = \mathsf{T}_N[\boldsymbol{\theta}] \cdot \mathbf{q}^{(\mathbf{B}[l])} = \mathsf{T}_N[\boldsymbol{\theta}] \cdot \left(\mathbf{s}^{(\mathbf{B}[l])} + \boldsymbol{\xi}(l)\right). \tag{15}$$

Результат оценки передаётся в систему распознавания, в основе которой лежит алгоритм поиска *k*-ближайших соседей (*k-nearest neighbors*, KNN), где $k = 1$:

$$\begin{aligned} \hat{\mathbf{z}}^{(\mathbf{B}[l])} &= \mathbf{KNN}\left\{\mathbf{h}^{(\mathbf{B}[l])}\right\} \\ &= \min_{\mathbf{z} \in \mathbf{CM}_b} \rho\left\{\mathbf{h}^{(\mathbf{B}[l])}, \mathbf{z}\right\} \\ &= \min_{\mathbf{z} \in \mathbf{CM}_b} \rho\left\{\mathbf{z}^{(\mathbf{B}[l])} + \boldsymbol{\xi}(l\,|\,\boldsymbol{\theta}), \mathbf{z}\right\}, \end{aligned} \tag{16}$$

где ρ – Евклидовое расстояние на $\mathbf{C}$.

Полученный вектор $\hat{\mathbf{z}}^{(\mathbf{B}[l])}$ оценивается сигнальным созвездием, после чего полученные бинарные последовательности $\hat{\mathbf{B}}[l]$ собираются в информационное сообщение $\hat{\mathbf{b}}[m]$.

IV. Постановка эксперимента

Модель канала связи, которая была исследована в нашей работе была впервые предложена Шенноном [14] и Винером [15]. Она состоит из легитимного передатчика, которого обычно называют «Алисой» и легитимного приёмника, которого обычно называют «Бобом». Предполагается, что они используют канал двусторонней связи с МОП $\mathsf{F}_N[\boldsymbol{\theta}^0]$ в OFDM-системе с поднесущими $\left\{\varphi_n^0 = (t_0\,|\,\theta_0^0, \theta_1^0, ..., \theta_i^0)\right\}_{n=0}^{N-1}$, форма которых зависит от фиксированных начальных параметров

$\boldsymbol{\theta}^0 = \left(\theta_0^0, \theta_1^0, ..., \theta_{M-1}^0\right)$ в момент времени t_0. Нарушителя, цель которого перехватить сообщения Алисы, обычно называют «Ева». Предполагается, что устройства Алисы и Боба всегда находятся в зоне видимости Евы (Рис. 2). Условимся, что Боб и Ева имеют одинаковые инструменты для декодирования сообщения. Таким образом, если Ева знает параметры $\boldsymbol{\theta}^0 = \left(\theta_0^0, \theta_1^0, ..., \theta_{M-1}^0\right)$, то она может успешно перехватить и декодировать переданное сообщение Алисы Бобу. Для недопущения прослушивания Алиса и Боб выбирают новые поднесущие в их OFDM-системе путём изменения преобразования $\mathsf{F}_N\left[\boldsymbol{\theta}^0\right]$ на преобразование $\mathsf{F}_N\left[\boldsymbol{\theta}^1\right]$ с новым набором параметров $\boldsymbol{\theta}^1 = \left[\theta_0^1, \theta_1^1, ..., \theta_{M-1}^1\right]$, известным только Алисе и Бобу.

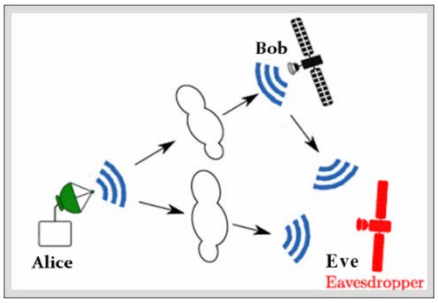

Рис. 2. Модель канала связи.

Цель эксперимента – продемонстрировать работоспособность предложенного метода защиты информации в системе с OFDM и определить параметры $\boldsymbol{\theta} = \left(\theta_0, \theta_1, ..., \theta_{M-1}\right)$, при которых уровень защиты максимален. Для количественного сравнения результатов декодирования принятых сообщений Бобом и Евой вычислялись следующие показатели:

1) доля числа бит, которыми отличается истинная битовая последовательность от той, которую восстановила Ева из подслушанного сообщения (вероятность битовой ошибки, **BER**):

$$\mathbf{BER}\left[l \mid \boldsymbol{\theta}\right] = \frac{1}{Nd} \sum_{m=0}^{Nd-1} \left(b\left[m \mid \boldsymbol{\theta}\right] \oplus \hat{b}\left[m \mid \boldsymbol{\theta}\right]\right); \quad (17)$$

2) доля числа символов, которыми отличаются истинная символьная последовательность от той, которую восстановила Ева из подслушанного сообщения (вероятность символьной ошибки, **SER**):

$$\mathbf{SER}\left[l \mid \boldsymbol{\theta}\right] = \frac{1}{N} \sum_{k=0}^{N-1} \left(\mathbf{b}^k\left[l \mid \boldsymbol{\theta}\right] \neq \hat{\mathbf{b}}^k\left[l \mid \boldsymbol{\theta}\right]\right). \quad (18)$$

Моделирование проводилось со следующими параметрами OFDM-системы: тип модуляции 256-QAM, количество поднесущих N=256. В качестве передаваемого сообщения использовалось серое изображение Лены размером $\left(256 \times 256\right)$. Каждый передаваемый временной слот являлся столбцом данного изображения, число временных слотов принималось равным 256 (количеству столбцов изображения Лены). Длина битового потока единичного временного слота составляла $8 \cdot 256 = 2048$, или 256 8-битных символов (т.е. на один символ приходилось 8 бит). В качестве МОП использовалось ДрПФБ (9):

$$\begin{aligned} \mathsf{F}_N^a\left[\boldsymbol{\theta}\right] &= \mathbf{U}_N \cdot \mathbf{diag}\left\{e^{-j\frac{\pi}{2}a\cdot\boldsymbol{\theta}}\right\} \cdot \mathbf{U}_N^T \\ &= \mathbf{U}_N \cdot \mathbf{diag}\left\{e^{-j\frac{\pi}{2}a\cdot\theta_0}, e^{-j\frac{\pi}{2}a\cdot\theta_1}, ..., e^{-j\frac{\pi}{2}a\cdot\theta_{N-1}}\right\} \cdot \mathbf{U}_N^T, \end{aligned} \quad (19)$$

где $a\boldsymbol{\theta} = a\left(\theta_0, \theta_1, ..., \theta_{N-1}\right) = a\left(0, 1, ..., N-2, N\right)$. Таким образом, форма этого преобразования зависела от параметра a.

V. Результаты

Зависимости **BER** и **SER** от параметра ДрПФБ a представлены на рис. 3а, 3б, соответственно.

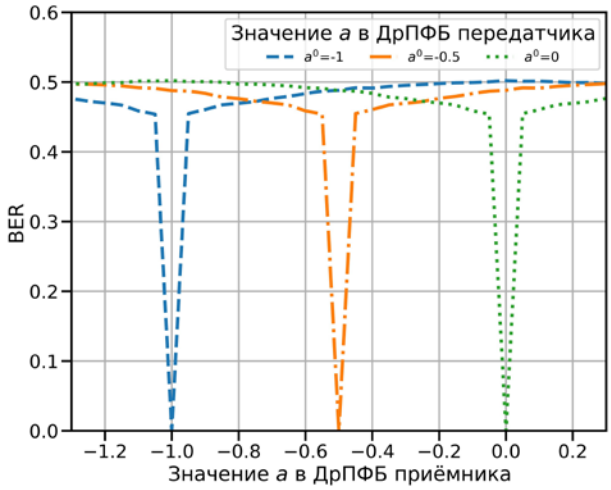

Рис 3а. Значения **BER** в приёмнике (Ева) при изменении параметра a в ДрПФБ в передатчике (Алиса).

Из рис. 3а, 3б видно, что, что при одинаковых значениях параметра a (или одинаковых ОП) в OFDM-системе Алисы и Евы имеем $\mathbf{BER} = 0$ и $\mathbf{SER} = 0$, следовательно, Ева успешно перехватывает сообщения Алисы. При изменении Алисой рабочего значения параметра $a_i \to a_j$ ($a_j \in \{-1, -0.5, 0\}$) с учётом того, что Ева использует старое значение a_i значения **BER** и **SER** начинают увеличиваться. Это означает, что сообщение, дешифрованное Евой, содержит ошибки, которые увеличиваются по мере увеличения разности значений параметра a в системах Алисы и Евы.

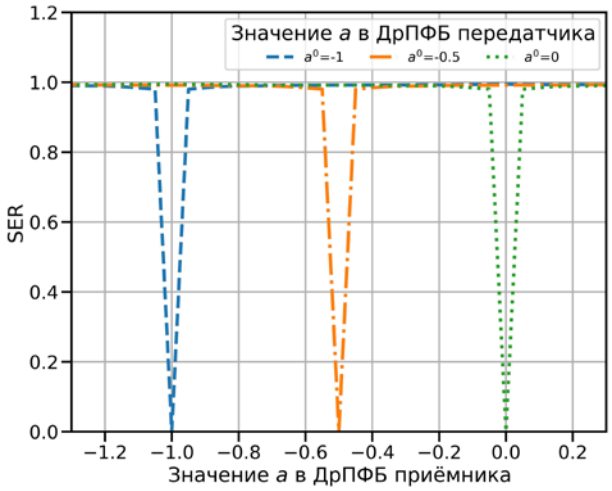

Рис 3б. Значения **SER** в приёмнике (Ева) при изменении параметра a в ДрПФБ в передатчике (Алиса).

Изображения Лены, восстановленные из декодированных Евой сообщений, представлены на рис. 4.

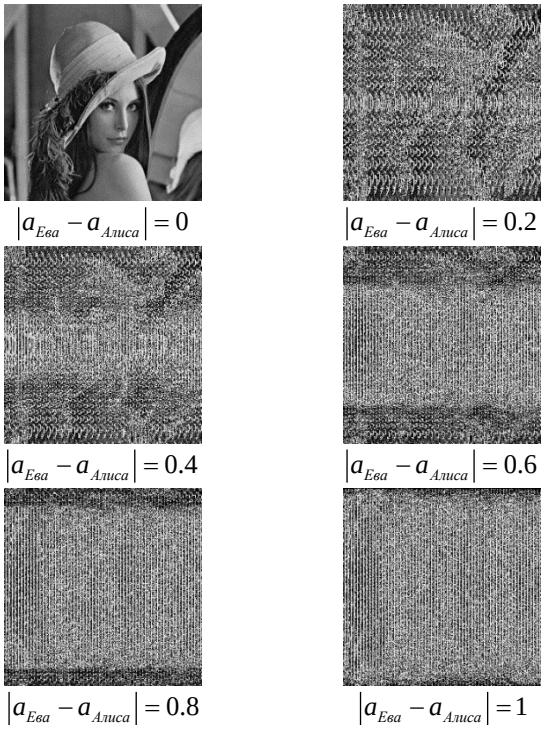

Рис4. Изображения, восстановленные Евой при различных значениях параметра a в OFDM-системах Евы и Алисы.

Из рис. 4 видно, что при $|a_{Ева} - a_{Алиса}| > 0.4$ качество перехваченного изображения оказывается столь низким, что визуальный анализ изображения не позволяет сделать какой-либо вывод о его контенте.

Таким образом, изменение параметров $\boldsymbol{\theta} = (\theta_0, \theta_1, ..., \theta_{M-1})$ в ДрПФБ OFDM позволяет защитить передаваемую этой системой информацию от нелегитимного доступа.

VI. Заключение

В статье представлена модификация классической системы с OFDM, в которой вместо ДПФ предложено использовать дробные или многопараметрические преобразования Фурье. Результаты моделирования с использованием ДрПФБ, подтверждают возможность защиты передаваемой информации от несанкционированного доступа.

Стоит отметить, что если нелигитимному пользователю известно, что в OFDM-системе используется ДрПФБ с одним параметром, то он может найти его значение простым перебором и получить доступ к передаваемой информации. Поэтому, для уменьшения риска несанкционированного доступа рекомендуется скрывать тип используемого дискретного преобразования, и использовать его многопараметрические реализации, в которых при увеличении количества параметров возрастает и сложность их перебора (которая становится экспоненциальной).

Отметим, что предложенный способ защиты информации в OFDM-системе не требует использования дополнительного оборудования и может применяться одновременно с иными техническими средствами защиты информации, сертифицированными регуляторами в области ИБ.

Библиография

[1] Банк данных угроз безопасности информации https://bdu.fstec.ru/threat/ubi.083
[2] Банк данных угроз безопасности информации https://bdu.fstec.ru/ubi/terms/terms/view/id/38
[3] Бакулин М. Г., Крейнделин В. Б., Шлома А. М., Шумов А. П. Технология OFDM. Учебное пособие для вузов. –М.: Горячая линия - Телеком, 2015. 360 с.
[4] Ахмед Н., Рао К. Р. Ортогональные преобразования при обработке цифровых сигналов: Пер. с англ./Под ред. И. Б. Фоменко. –М.: Связь, 1980. 248 с.
[5] F. Renna, N. Laurenti, H. V. Poor, “Physical-layer secrecy for OFDM transmissions over fading channels”, *IEEE Trans. Inf. Forens. Security*, 2012, 7(4), pp. 1354-1367.
[6] A. Chorti, H. V. Poor, “Faster than Nyquist interference assisted secret communication for OFDM systems”, *Proceedings of the IEEE Asilomar Conf. Signals, Systems and Comput.*, 2011, pp. 183-187.
[7] H. M. Wang, Q. Yin, X. G. Xia, “Distributed beamforming for physical-layer security of two-way relay networks”, *IEEE Trans. Signal Process.*, 2012, 60(7), pp. 3532-3545.
[8] V. Bargmann “On a Hilbert space of analytic functions and an associated integral transform. Part 1”, *Commun. Pure Appl. Math.*, 1961, 14, pp.187–214.
[9] A. Bultheel, and H. Martinez, “Computation of the Fractional Fourier Transform, preprint”.
[10] H. M. Ozaktas, O. Arıkan, M. A. Kutay, and G. Bozdagi, “Digital computation of the fractional Fourier transform,” *IEEE Trans. Signal Processing*, vol. 44, pp. 2141–2150, Sept. 1996.
[11] M. K. Gupta, S. Tiwari. “Performance evaluation of conventional and wavelet based OFDM System”, *International Journal on Electronics and Communication*, 2013, vol. 67, no.4, pp 348– 354.
[12] M. J. E. Golay. Complementary series, *IEEE Trans. Inform. Theory*, 1961, 7, pp. 82–87.
[13] T. A. Wilkinson, A. E. Jones. “Combined coding for error control and increased robustness to system nonlinearities in OFDM”, *Proceedings of the IEEE 46th Vehicular Technology Conf.*, 1996, pp. 904-908.
[14] C. E. Shannon 1949 *Communication Theory of Secrecy Systems Bell Labs Technical Journal* 28(4) 657-715.
[15] A. D. Wyner, “The wiretap channel”, *Bell Sys. Tech. J.*, 1975, 54(8), pp. 1355–1387.
[16] E. Labunets, V. Labunets, “Fast fractional Fourier transforms”, *Proc. of Eusipco-98*, Rhodes, Greece, 8–11 Sept. 1998, pp. 1757–1760.

On the possibility of information protection in telecommunication OFDM-systems using multi-parameter orthogonal transformations

S. A. Martiugin, S. V. Porshnev

Abstract— **Information security is one of the most important areas in wireless communication systems. Traditional information security methods are based on the upper layers of the open systems interconnection model (OSI) protocol stack, but their reliability is significantly reduced for scenarios where legitimate and illegitimate users share a common physical environment.**

In this article we develop an OFDM (orthogonal frequency-division multiplexing) communication system where instead of traditional orthogonal transformations (OT), for example, Walsh, Haar, Fourier transforms, their fractional (FOT) or multiparameter implementations (MPOT) are used. Such transformations depend on a finite set of independent parameters α (in case of fractional OT) or $\alpha_0,...,\alpha_{N-1}$ (in case of MPOT), which change their form. When $\alpha = \pi/2$, or $\alpha_0 =,...,= \alpha_{N-1} = \pi/2$ the transformation takes the form of the classical OT, and when $\alpha = 0$, or $\alpha_0 =,...,= \alpha_{N-1} = 0$ degenerates into the identical transformation. Successful information exchange requires knowledge of the parameters of the currently used FOT or MPOT, which may change periodically.

The simulation results of OFDM system using single-parameter Fourier-Bargmann transform (FrFBT) show that the proposed OFDM system provides better security against unauthorized access to information compared to the traditional OFDM system.

REFERENCES

[1] Data Bank of Information Security Threats https://bdu.fstec.ru/threat/ubi.083

[2] Data Bank of Information Security Threats https://bdu.fstec.ru/ubi/terms/terms/view/id/38

[3] M. Bakulin, V. Kreindelin, A. Shloma, A. Shumov. “OFDM technology”, Telecom, 2015, 360 pp.

[4] N. Ahmed, K Rao, “Orthogonal Transforms for Digital Signal Processing” Springer; Softcover reprint of the original 1st ed. 1975.

[5] F. Renna, N. Laurenti, H. V. Poor, “Physical-layer secrecy for OFDM transmissions over fading channels”, *IEEE Trans. Inf. Forens. Security*, 2012, 7(4), pp. 1354-1367.

[6] A. Chorti, H. V. Poor, “Faster than Nyquist interference assisted secret communication for OFDM systems”, *Proceedings of the IEEE Asilomar Conf. Signals, Systems and Comput.*, 2011, pp. 183-187.

[7] H. M. Wang, Q. Yin, X. G. Xia, “Distributed beamforming for physical-layer security of two-way relay networks”, *IEEE Trans. Signal Process.*, 2012, 60(7), pp. 3532-3545.

[8] V. Bargmann “On a Hilbert space of analytic functions and an associated integral transform. Part 1”, *Commun. Pure Appl. Math.*, 1961, 14, pp.187–214.

[9] A. Bultheel, and H. Martinez, “Computation of the Fractional Fourier Transform, preprint”.

[10] H. M. Ozaktas, O. Arıkan, M. A. Kutay, and G. Bozdagi, “Digital computation of the fractional Fourier transform,” *IEEE Trans. Signal Processing*, vol. 44, pp. 2141–2150, Sept. 1996.

[11] M. K. Gupta, S. Tiwari. “Performance evaluation of conventional and wavelet based OFDM System”, *International Journal on Electronics and Communication*, 2013, vol. 67, no.4, pp 348– 354.

[12] M. J. E. Golay. Complementary series, *IEEE Trans. Inform. Theory*, 1961, 7, pp. 82–87.

[13] T. A. Wilkinson, A. E. Jones. “Combined coding for error control and increased robustness to system nonlinearities in OFDM”, *Proceedings of the IEEE 46th Vehicular Technology Conf.*, 1996, pp. 904-908.

[14] C. E. Shannon 1949 *Communication Theory of Secrecy Systems Bell Labs Technical Journal* 28(4) 657-715.

[15] A. D. Wyner, “The wiretap channel”, *Bell Sys. Tech. J*., 1975, 54(8), pp. 1355–1387.

[16] E. Labunets, V. Labunets, “Fast fractional Fourier transforms”, *Proc. of Eusipco-98*, Rhodes, Greece, 8–11 Sept. 1998, pp. 1757–1760.

Stepan A. Martiugin, Ural Federal University named after First President of Russia B.N. Yeltsin, stmart2608@gmail.com.

Prof. Sergey V. Porshnev, Ural Federal University named after First President of Russia B.N. Yeltsin, Leading Researcher, N.N. Krasovsky Institute of Mathematics and Mechanics of the Ural Branch of the Russian Academy of Sciences, Russia, s.v.porshnev@urfu.ru.