

О возможности повышения помехозащищенности телекоммуникационных систем с OFDM с помощью дробного преобразования Фурье

С. А. Мартюгин, С. В. Поршневу

Аннотация—В статье представлена телекоммуникационная система связи (ТКС) 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 (ДОП) или многопараметрические (МОП) реализации. Такие преобразования зависят от конечного набора независимых параметров α (в случае дробных ОП) или $\alpha_0, \dots, \alpha_{N-1}$ (в случае МОП), при изменении которых меняется и их облик. При $\alpha = \pi/2$, или $\alpha_0, \dots, \alpha_{N-1} = \pi/2$ преобразования принимают форму классического ОП, а при $\alpha = 0$, или $\alpha_0, \dots, \alpha_{N-1} = 0$ вырождаются в тождественное преобразование.

Приведены результаты моделирования передачи сигнала предложенной ТКС-OFDM с дробным преобразованием Фурье (ДрПФ) в условиях действия специальной прицельной помехи, направленной на известные уязвимости в классической ТКС-OFDM. Сравнительный анализ предложенной системы и классической ТКС-OFDM позволил сделать вывод о том, что ТКС-OFDM с ДрПФ менее чувствительна к помехам такого типа. Показано, что предложенная ТКС-OFDM с ДрПФ обладает меньшим, по сравнению с классической ТКС-OFDM, пик-фактором.

Реализация ТКС-OFDM с ДрПФ не требует дополнительного оборудования или специального программного обеспечения. Сложность вычисления ДрПФ совпадает со сложностью вычисления классического дискретного преобразования Фурье (ДПФ).

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

I. ВВЕДЕНИЕ

Технология мультиплексирования с ортогональным частотным разделением каналов (orthogonal frequency-division multiplexing, OFDM) широко используется в

современных системах беспроводной связи, цифрового телевидения, радиовещания, передачи спутниковых данных, навигации и БПЛА [1], [2].

Для обеспечения необходимого уровня безопасности при передаче данных в телекоммуникационных системах с OFDM (ТКС-OFDM) обычно используют методы, которые реализованы на верхних уровнях сетевой модели OSI [3]. Однако их надёжность значительно снижается, когда легитимные и нелегитимные пользователи используют общую физическую среду [4], в которой злоумышленники могут «вслепую» оценивать параметры сигналов ТКС-OFDM и либо перехватывать передаваемый информационный сигнал, либо ставить радиозлектронную помеху. В этой связи, обеспечение безопасности и помехозащищенности передаваемой информации на физическом уровне является новым перспективным направлением в области беспроводной связи [5]–[7].

Для решения обсуждаемой задачи представляется перспективным использовать в ТКС-OFDM вместо классического преобразования Фурье различные дробные или многопараметрические ортогональные преобразования (ДОП, и МОП, соответственно). Эти преобразования зависят от параметра α (ДОП) или набора параметров $\alpha_0, \dots, \alpha_{N-1}$ (МОП), которые могут изменяться независимо друг от друга. Значения этих параметров определяют форму поднесущей ТКС-OFDM. Параметр α принимает значения от 0 до 2π , а вектор $\theta = \alpha_0, \dots, \alpha_{N-1}$ принадлежит параметрическому пространству $((N-1)$ -мерному тору) $(\alpha_0, \dots, \alpha_{N-1}) \in \mathbf{Tor}^{N-1}[0, 2\pi] = (0, 2\pi]^{N-1}$.

Если нарушитель знает параметры ОП (α , или $\alpha_0, \dots, \alpha_{N-1}$), которое используется в ТКС-OFDM в настоящий момент времени, то он может сформировать специальную помеху, которая препятствует правильному распознаванию информационного сообщения на стороне приёмника. Однако, если значения этих параметров неизвестны нарушителю, и, в этой связи, он выбирает их произвольно, то весьма маловероятно, что сигнал прицельной помехи сможет полностью подавить информационный сигнал и сделать

Статья получена 04.05.2024

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

Сергей Владимирович Поршневу, д.т.н., профессор, Уральский федеральный университет имени первого Президента России Б. Н. Ельцина, s.v.porshnev@urfu.ru

невозможным распознавание контента передаваемого сообщения. Таким образом, можно ожидать, что помехозащищенность ТКС-OFDM, в которой используется ДОП или МОП, будет выше, чем помехозащищенность ТКС-OFDM, в которой используется классическое преобразование Фурье.

В статье изложены результаты, проведенного авторами исследования, с целью принятия/отклонения высказанной выше гипотезы.

Статья имеет следующую структуру: в разделе II проведён краткий обзор теории ДОП и МОП, в разделе III описана модель OFDM-системы с ДОП или МОП, в разделе IV приведено описание вычислительного эксперимента, проведенного с целью подтверждения гипотезы о более высокой помехозащищенности ТКС-OFDM с ДОП или МОП, в разделе V приведены результаты исследования пик-фактора предложенной системы.

II. ДРОБНЫЕ И МНОГОПАРАМЕТРИЧЕСКИЕ ПРЕОБРАЗОВАНИЯ ФУРЬЕ

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

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

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

$$T^{(a_0, \dots, a_{N-1})} = U \cdot \text{diag}(\lambda_0^{a_0}, \dots, \lambda_{N-1}^{a_{N-1}}) \cdot U^{-1} \quad (2)$$

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

$$T^a = U \cdot \text{diag}(\lambda_0^a, \dots, \lambda_{N-1}^a) \cdot U^{-1} = U \cdot \Lambda^a \cdot U^{-1} \quad (3)$$

При $a = 1$ имеем исходное преобразование $T^1 = U \Lambda U^{-1}$, а при $a = 0$ преобразование вырождается в тождественное: $T^0 = U \Lambda^0 U^{-1} = I$. Семейства $\{T^{(a_0, \dots, a_{N-1})}\}_{(a_0, \dots, a_{N-1}) \in \square}$ и $\{T^a\}_{a \in \square}$ формируют,

соответственно, многопараметрическую и однопараметрическую строго непрерывные унитарные группы, где умножение выполняется следующим образом: $T^{(a_0, \dots, a_{N-1})} \cdot T^{(b_0, \dots, b_{N-1})} = T^{(a_0+b_0, \dots, a_{N-1}+b_{N-1})}$ и $T^a \cdot T^b = T^{a+b}$.

Пусть $F = \left[e^{-j \frac{2\pi}{N} \omega t} \right]$ – дискретное $(N \times N)$ -преобразование Фурье (ДПФ). Собственными функциями оператора преобразования Фурье являются функции Эрмита [9]:

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

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

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

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:

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

где $U = [\Psi_0(i) | \Psi_1(i) | \dots]$ – матрица, составленная из собственных векторов оператора ДПФ.

Определение 3. Дискретным дробным преобразованием Фурье является следующее преобразование:

$$\begin{aligned} F^a &= U \left\{ \text{diag} \left(e^{-j \frac{\pi}{2} n a} \right) \right\} U^{-1} \\ &= \sum_{n=0}^{N-1} e^{-j \frac{\pi}{2} n a} \Psi_n(x) \Psi_n(y), \end{aligned} \quad (7)$$

где, $a \in \square$. Существует также и α -параметризация, где $\alpha = a\pi/2$, $\alpha \in \square$.

Матричные элементы, формирующие ядро данного преобразования и быстрые алгоритмы его реализации, были разработаны авторами в [10].

Определение 4. Дискретным многопараметрическим преобразованием Фурье является следующее преобразование:

$$\begin{aligned} F^{\mathbf{a}} &= F^{(a_0, a_1, \dots, a_{N-1})} \\ &= U \left\{ \text{diag} \left(e^{-j \frac{\pi}{2} n a_n} \right) \right\} U^{-1} \\ &= \sum_{n=0}^{N-1} e^{-j \frac{\pi}{2} n a_n} \Psi_n(x) \Psi_n(y), \end{aligned} \quad (8)$$

где $\mathbf{a} = (a_0, a_1, \dots, a_{N-1})$, $a_i \in \square$.

Так как $F^4 = I$, то операторы (7) и (8) являются периодическими с периодом 4. Они формируют непрерывные унитарные мультипликативные группы:

$\mathbf{F}^{(a_0, a_1, \dots, a_{N-1})} \cdot \mathbf{F}^{(b_0, b_1, \dots, b_{N-1})} = \mathbf{F}^{(a_0 \oplus_4 b_0, a_1 \oplus_4 b_1, \dots, a_{N-1} \oplus_4 b_{N-1})}$,
 $\mathbf{F}^a \cdot \mathbf{F}^b = \mathbf{F}^{a \oplus_4 b}$, где $a_i \oplus_4 b_i = (a_i + b_i) \bmod 4$,
 $\forall i = 0, 1, \dots, N-1$. Таким образом, параметры a_0, a_1, \dots, a_{N-1} и a меняются в пределах $(\square / 4\square)^{N-1} = [0, 4)^{N-1}$ и $\square / 4\square = [0, 4)$ соответственно. В случае α -параметризации имеем
 $\mathbf{F}^{(\alpha_0, \alpha_1, \dots, \alpha_{N-1})} \cdot \mathbf{F}^{(\beta_0, \beta_1, \dots, \beta_{N-1})} = \mathbf{F}^{(\alpha_0 \oplus_{2\pi} \beta_0, \alpha_1 \oplus_{2\pi} \beta_1, \dots, \alpha_{N-1} \oplus_{2\pi} \beta_{N-1})}$ и
 $\mathbf{F}^{\alpha} \cdot \mathbf{F}^{\beta} = \mathbf{F}^{\alpha \oplus_{2\pi} \beta}$, где $\alpha \oplus_{2\pi} \beta = (\alpha + \beta) \bmod 2\pi$,
 $\forall i = 0, 1, \dots, N-1$. Параметры $\alpha_0, \alpha_1, \dots, \alpha_{N-1}$ и α меняются в пределах $(\square / 4\square)^{N-1} = [0, 2\pi)^{N-1}$ и $\square / 4\square = [0, 2\pi)$ соответственно.

III. МОДЕЛЬ СИСТЕМЫ OFDM С МОП

Пусть

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

будет сигнальным созвездием, состоящим из 2^d точек $z^{(b_0, b_1, \dots, b_{d-1})} = z^{(\mathbf{b})}$ комплексной плоскости \mathbf{C} , пронумерованных целыми числами, записанными в двоичной системе счисления $(b_0, b_1, \dots, b_{d-1}) \in \mathbf{B}_2^d$. 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, передаваемый OFDM-системой, является комплекснозначной функцией вида:

$$s(t) = e^{j\omega_0 t} \sum_{n=0}^{N-1} z^{(\mathbf{b})}_n \varphi_n(t), \quad (9)$$

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

$$\int_0^{\tau} \varphi_q(t) \varphi_l^*(t) dt = \begin{cases} 1, & q = l, \\ 0, & q \neq l. \end{cases}$$

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 :

$$\varphi_n(t_k) = e^{j2\pi n \Delta f t_k} = e^{j2\pi n (1/\tau) k\tau/N} = e^{j2\pi n k/N}, \quad (10)$$

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

$$\begin{aligned} s(t) &= e^{j\omega_0 t} \sum_{n=0}^{N-1} z_n \varphi_n(t_k) \\ &= e^{j\omega_0 t} \sum_{n=0}^{N-1} z_n e^{j2\pi n k/N} \\ &= e^{j\omega_0 t} (\mathbf{F}_N^{-1} \mathbf{z}^{(\mathbf{b})}), \end{aligned} \quad (11)$$

где $0 \leq k < N$, $\mathbf{F}_N^{-1} = \left[e^{j2\pi n k/N} \right]_{n,k=0}^{N-1}$ – 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 обратного дробного, или многопараметрического преобразования Фурье $\{\bar{\varphi}_n(t|\boldsymbol{\theta})\}_{n=0}^{N-1}$, где $\boldsymbol{\theta} = (\theta_0, \theta_1, \dots, \theta_{N-1})$ – набор параметров, от которых они зависят. При изменении параметров $\boldsymbol{\theta} = (\theta_0, \theta_1, \dots, \theta_{N-1})$ изменяются тип, свойства и характеристики OFDM-системы, что можно использовать для решения широкого круга адаптационных телекоммуникационных задач.

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

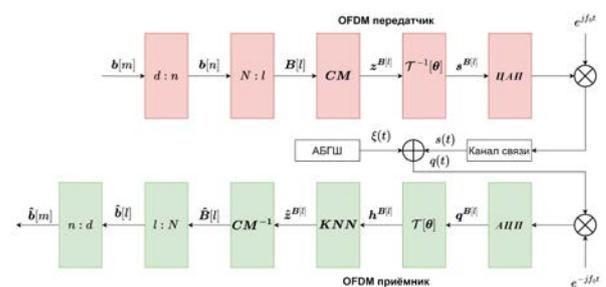


Рис. 1. Структурная схема OFDM-системы с МОП.

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:

$$\mathbf{z}^{(b[l])} = \begin{bmatrix} \mathbf{CM}\{\mathbf{b}_0[l]\} \\ \mathbf{CM}\{\mathbf{b}_1[l]\} \\ \vdots \\ \mathbf{CM}\{\mathbf{b}_{N-1}[l]\} \end{bmatrix} = \begin{bmatrix} z_0^{(b_0[l])} \\ z_1^{(b_1[l])} \\ \vdots \\ z_{N-1}^{(b_{N-1}[l])} \end{bmatrix}.$$

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

$$\mathbf{s}^{(b[l])} = \mathbf{T}^{-1}[\boldsymbol{\theta}] \cdot \mathbf{z}^{(b[l])}, \quad (12)$$

Полученный сигнал поступает на цифроаналоговый преобразователь, формируя передаваемый в линию связи аналоговый 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 по времени и квантуется по амплитуде в аналого-цифровом преобразователе. Далее, сигнал делится на N параллельных потоков и происходит оценка информационного сообщения ($\mathbf{q}^{(b[l])}$) с помощью прямого МОП с параметрами $\boldsymbol{\theta} = (\theta_0, \theta_1, \dots, \theta_{N-1})$, которые использовались при формировании сообщения:

$$\mathbf{h}^{(b[l])} = \mathbf{T}_N[\boldsymbol{\theta}] \cdot \mathbf{q}^{(b[l])} = \mathbf{T}_N[\boldsymbol{\theta}] \cdot (\mathbf{s}^{(b[l])} + \xi(l)). \quad (13)$$

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

$$\begin{aligned} \hat{\mathbf{z}}^{(b[l])} &= \mathbf{KNN}\{\mathbf{h}^{(b[l])}\} \\ &= \min_{\mathbf{z} \in \mathbf{CM}_b} \rho\{\mathbf{h}^{(b[l])}, \mathbf{z}\} \\ &= \min_{\mathbf{z} \in \mathbf{CM}_b} \rho\{\mathbf{h}^{(b[l])} + \xi(l|\boldsymbol{\theta}), \mathbf{z}\}, \end{aligned} \quad (14)$$

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

Затем полученный вектор $\hat{\mathbf{z}}^{(b[l])}$ 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 настоящей 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 $\mathbf{T}_N[\boldsymbol{\theta}^0]$ в OFDM-системе с поднесущими $\{\phi_n^0 = (t_0 | \theta_0^0, \theta_1^0, \dots, \theta_i^0)\}_{n=0}^{N-1}$, форма которых зависит от фиксированных начальных параметров $\boldsymbol{\theta}^0 = (\theta_0^0, \theta_1^0, \dots, \theta_{N-1}^0)$ в момент времени t_0 . Нарушителя обычно называют «Джемми». Его целью является постановка радиоэлектронной помехи, которая нарушает, или делает невозможным приём информации на приёмной стороне. Предполагается, что устройства Алисы и Боба всегда находятся в зоне видимости Джемми (Рис. 2).

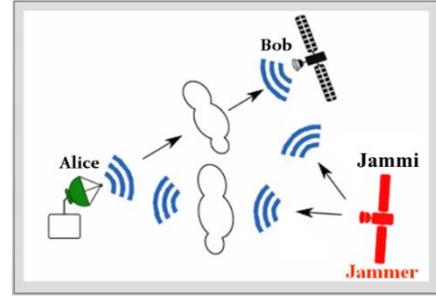
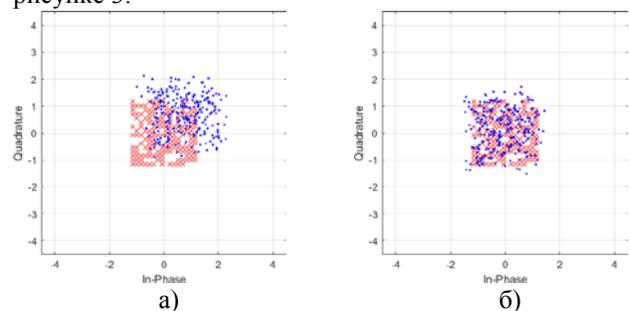


Рис. 2. Модель канала связи.

Если Джемми определит поднесущие, или $\boldsymbol{\theta}^0 = (\theta_0^0, \theta_1^0, \dots, \theta_{N-1}^0)$ в OFDM системе Алисы и Боба, то их система может быть подавлена, нейтрализована или уничтожена посредством специальной помехи, которая нацелена на известные уязвимости в классической ТКС-OFDM:

$$\begin{aligned} \mathbf{h}^{(b[l])} &= \mathbf{T}_N[\boldsymbol{\theta}^0] \{ \mathbf{s}^{(b[l])} + \xi(l) \} \\ &= \mathbf{T}_N[\boldsymbol{\theta}^0] \{ \mathbf{T}_N^{-1}[\boldsymbol{\theta}^0] \{ \mathbf{z}^{(b[l])} \} + \mathbf{T}_N^{-1}[\boldsymbol{\theta}^0] \{ \boldsymbol{\eta} \} \} \\ &= \mathbf{z}^{(b[l])} + \boldsymbol{\eta}, \end{aligned} \quad (15)$$

где $\xi = \mathbf{T}_N^{-1}[\boldsymbol{\theta}^0] \{ \boldsymbol{\eta} \}$ – помеха, комплексные элементы $\boldsymbol{\eta}$ которой имеют нормальное распределение со специальным средним значением $\dot{m}_{jam} = \Re(\dot{m}_{jam}) + j\Im(\dot{m}_{jam})$ и отклонением σ_{jam}^2 . Пример действия такой помехи на OFDM-сигнал представлен на рисунке 3.



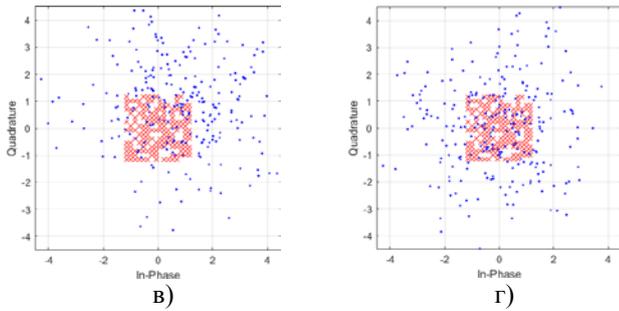


Рис 3. Принятый сигнал на сигнальном созвездии в отсутствии (символ «+») и присутствии (символ «.») атаки с умной помехой на символы ТКС-OFDM:

$$а) \eta_{k,1} \in \mathcal{CN}(m_{jam,1}, \sigma_{jam,1}^2), \quad a_{A,B} = a_J;$$

$$б) \eta_{k,1} \in \mathcal{CN}(m_{jam,1}, \sigma_{jam,1}^2), \quad a_{A,B} \neq a_J;$$

$$в) \eta_{k,2} \in \mathcal{CN}(m_{jam,1}, \sigma_{jam,2}^2), \quad a_{A,B} = a_J, \quad \sigma_{jam,2}^2 > \sigma_{jam,1}^2;$$

$$г) \eta_{k,2} \in \mathcal{CN}(m_{jam,1}, \sigma_{jam,2}^2), \quad a_{A,B} \neq a_J, \\ \sigma_{jam,2}^2 > \sigma_{jam,1}^2,$$

где $a_{A,B}$ – степенной параметр ОП в ТКС-OFDM

Алисы и Боба, a_J – степенной параметр ОП при формировании помехи

Здесь символы сигнального созвездия в отсутствии атаки с умной помехой обозначены символом «+», а с присутствием этой атаки символом «.» Из рисунка 3 видно, что помеха сдвигает распознанные приёмником символы на сигнальном созвездии, при этом среднее значение (m_{jam}) отвечает за направление сдвига (рис 3а), а отклонение (σ_{jam}^2) за разброс (рис 3в).

Для ухода от помехи Алиса и Боб меняют параметры ТКС-OFDM на $\theta^1 = (\theta_0^1, \theta_1^1, \dots, \theta_{N-1}^1)$. Тогда Алиса будет передавать новые информационные сообщения $\mathbf{s}^{(B[l])} = \mathbf{T}^{-1}[\theta^1]\{\mathbf{z}^{(B[l])}\}$, а приёмник Боба будет принимать следующий сигнал:

$$\mathbf{h}^{(B[l])} = \mathbf{T}_N[\theta^1]\{\mathbf{s}^{(B[l])} + \xi(l)\} \\ = \mathbf{T}_N[\theta^1]\{\mathbf{T}_N^{-1}[\theta^1]\{\mathbf{z}^{(B[l])}\} + \mathbf{T}_N^{-1}[\theta^0]\{\boldsymbol{\eta}\}\} \\ = \mathbf{z}^{(B[l])} + \mathbf{T}_N[\theta^1]\mathbf{T}_N^{-1}[\theta^0]\boldsymbol{\eta} \\ \neq \mathbf{z}^{(B[l])} + \boldsymbol{\eta},$$

и

$$\hat{\mathbf{z}}^{(B[l])} = \mathbf{KNN}\{\mathbf{h}^{(B[l])}\} \\ = \mathbf{KNN}\{\mathbf{z}^{(B[l])} + \mathbf{T}_N[\theta^1]\mathbf{T}_N^{-1}[\theta^0]\{\boldsymbol{\eta}\}\}.$$

Сигнальное созвездие в обсуждаемом случае приведено на рис 3б. и 3в. Здесь прицельная помеха формировалась с использованием обратного ДрПФ при $a = -1$ (или ОДПФ), а в ТКС-OFDM использовалось ОДрПФ с $a = -0.125$. На этих рисунках видно, что если значения a в ОДрПФ ТКС-OFDM и ОДрПФ помехи, не совпадают, то величина сдвига принятых

символов сигнального созвездия уменьшается.

Для выбора значения m_{jam} (или направления сдвига), при котором достигается наиболее негативное воздействие помехи был проведён анализ сигнального созвездия типа QAM. Напомним, что точки сигнального созвездия индексируются кодами Грея, основанными на метрике Ли. Сигнальное созвездие QAM-16, на котором

изображена точка $z^{(b^*)}$ (0101) с её ближайшими соседями ($z_{k\pi/4}^{(b^*)}$, $k = 0, 1, \dots, 7$), представлена на рис 4.

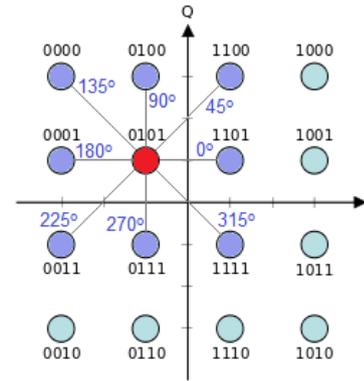


Рис 4. Точка $z^{(b^*)}$ (0101) на сигнальном созвездии QAM-16 и её ближайшие соседи

Максимальная ошибка распознавания данной точки, достигается в том случае, когда расстояние Ли будет максимальным. Расстояния Ли от $z^{(b^*)}$ до её ближайших соседей приведены в Таблице 1.

Таблица 1. Расстояние Ли от точки 0101 (рис 4.) до её ближайших соседей по выбранным направлениям

Направление	0°	45°	90°	135°	180°	225°	270°
ρ_{Lee}	1	2	1	2	1	2	1

Аналогичным способом можно вычислить максимальную ошибку для каждой точки по каждому направлению. Нетрудно видеть, что для такого типа сигнального созвездия максимальная ошибка появляется при диагональном сдвиге точек сигнального созвездия, поэтому в описываемых далее экспериментах использовалось

$$m_{jam} = \Re(m_{jam}) + j\Im(m_{jam}) = \frac{\sqrt{2}}{2}(\pm 1 \pm j).$$

Цель эксперимента – продемонстрировать более высокую защищенность ТКС-OFDM с ДрПФ от направленной радиоэлектронной помехи и определить величину изменения параметров $\theta = (\theta_0, \theta_1, \dots, \theta_{N-1})$, при которых влияние такой помехи на качество принимаемого сообщения минимально.

Для количественного сравнения результатов вычислялись следующие показатели:

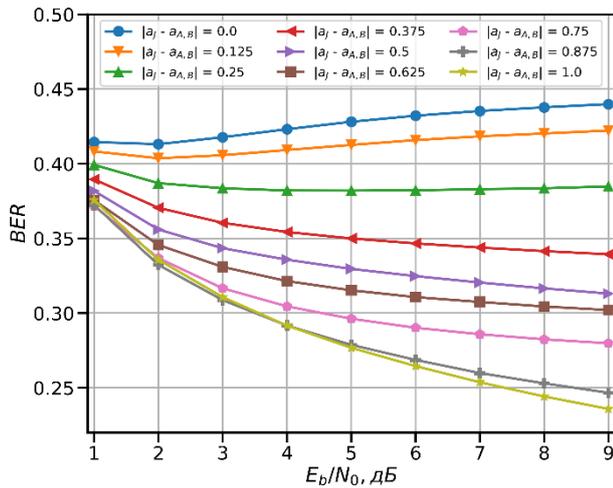
- 1) доля числа бит, которыми отличается истинная битовая последовательность от той, которую восстановил Боб из сообщения после действия умной помехи (вероятность битовой ошибки, **BER**):

$$\mathbf{BER}[l|\theta] = \frac{1}{Nd} \sum_{m=0}^{Nd-1} (b[m|\theta] \oplus \hat{b}[m|\theta]); \quad (16)$$

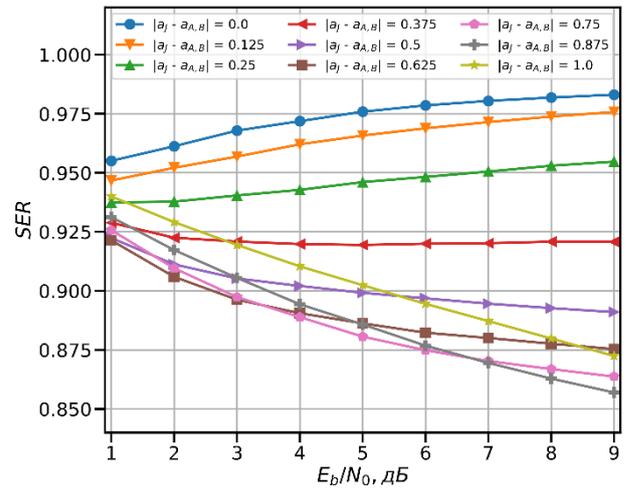
2) доля числа символов, которыми отличаются истинная символьная последовательность от той, которую восстановил Боб из сообщения после действия умной помехи (вероятность символьной ошибки, **SER**):

$$\mathbf{SER}[l|\theta] = \frac{1}{N} \sum_{k=0}^{N-1} (\mathbf{b}^k[l|\theta] \neq \hat{\mathbf{b}}^k[l|\theta]). \quad (17)$$

Моделирование проводилось со следующими параметрами ТКС-OFDM: тип модуляции 256-QAM, количество поднесущих $N=256$. В качестве передаваемого сообщения использовалось серое изображение Лены размером (256×256) . 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 ОП было использовано ДрПФ, быстрые алгоритмы которого были разработаны в [10]. Таким образом, форма этого преобразования зависела от параметра a . Для оценки эффективности ухода от помехи вычислялись средние значения **BER** и **SER** по 256 временным слотам. Вычисления повторялись 100 раз для каждого из значений E_b/N_0 , после чего результаты усреднялись. Параметр a , в ТКС-OFDM принимал значения $a_k = -1 + 0,125 \cdot k$, $k = 0, 8$, в то время как Джемми для создания помехи использовал прежнее значение параметра $a_J = -1$, или классическое ОДПФ.



а)

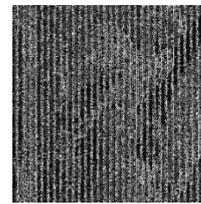
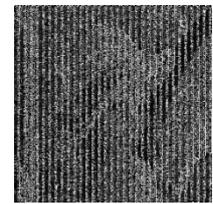
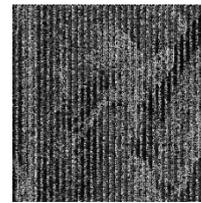
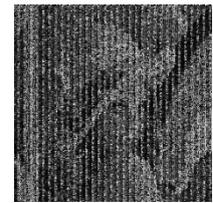
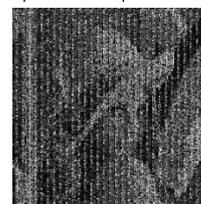


б)

 Рис 5. Значения а) $\mathbf{BER}(F_{A,B}^{a(k)}, F_J^{-1} | E_b/N_0)$, б)

$$\mathbf{SER}(F_{A,B}^{a(k)}, F_J^{-1} | E_b/N_0).$$

Средние значения **BER** и **SER** приведены на рис 5. Из рисунка 5 видно, что изменение параметра a позволяет снизить влияние прицельной помехи на контент передаваемого сообщения. Соответствующие сообщения (изображение Лены), полученные Бобом в условиях действия помехи приведены на рис. 6.


 $|a_j - a_{A,B}| = 0$

 $|a_j - a_{A,B}| = 0.125$

 $|a_j - a_{A,B}| = 0.25$

 $|a_j - a_{A,B}| = 0.375$

 $|a_j - a_{A,B}| = 0.5$

 $|a_j - a_{A,B}| = 0.625$

 $|a_j - a_{A,B}| = 0.75$

 $|a_j - a_{A,B}| = 0.875$



Рис. 6. Изображения, восстановленные Бобом после воздействия прицельной помехи, при разных значениях параметра $a_{A,B}$ в ТКС-OFDM Алисы и Боба.

Из рис. 6 видно, что при $|a_j - a_{A,B}| > 0.375$ распознавание контента переданного сообщения не вызывает каких-либо проблем.

Таким образом, устойчивость ТКС-OFDM с ДрПФ к негативному воздействию направленной помехи, действительно, оказывается выше, чем у классической ТКС-OFDM с ДПФ.

V. ИССЛЕДОВАНИЕ ПИК-ФАКТОРА ТКС-OFDM

OFDM-сигнал является суммой большого количества поднесущих колебаний (нескольких сотен, или даже тысяч) со случайными амплитудами и начальными фазами, поэтому, следуя, центральной предельной теореме его можно рассматривать как узкополосный гауссовский случайный процесс, в котором с конечной вероятностью мгновенная мощность может превысить среднюю примерно в 5 раз [8]. Отношение пиковой мгновенной мощности сигнала к его средней мощности называется пик-фактором. Высокие значения пик-фактора являются одним из основных недостатков систем с OFDM [8]. Они приводят к низкому значению коэффициента полезного действия передатчиков, и к неэффективному использованию батарей. Кроме того, возникают нелинейные искажения передаваемого сигнала, что ухудшает, а в некоторых случаях, делает невозможным демодуляцию сигнала на приёмной стороне.

В этой связи была проведена серия экспериментов, в которых были исследованы зависимости пик-фактора от изменения значения параметра a в ОДрПФ ТКС-OFDM. Для этого формировалось $Q = 256$ случайных последовательностей символов сигнального созвездия, длиной $N = 256$. Далее для каждой последовательности вычислялся её $F_N^{-1}[\theta^i]$ -спектр с параметрами $a_i \in (0, -1/16, \dots, -1)$, который записывался в соответствующие строки матрицы \mathbf{S} , размером $Q \times N$:

$$\mathbf{S}_{Q \times N} = \begin{bmatrix} \mathbf{s}_0 \\ \mathbf{s}_1 \\ \vdots \\ \mathbf{s}_Q \end{bmatrix} = \begin{bmatrix} s_{0,0}, s_{0,1}, \dots, s_{0,N-1} \\ s_{1,0}, s_{1,1}, \dots, s_{1,N-1} \\ \vdots \\ s_{Q,0}, s_{Q,1}, \dots, s_{Q,N-1} \end{bmatrix} = \begin{bmatrix} F_N^{-1}[\theta^0] \mathbf{s}_0 \\ F_N^{-1}[\theta^1] \mathbf{s}_1 \\ \vdots \\ F_N^{-1}[\theta^Q] \mathbf{s}_Q \end{bmatrix}.$$

Описанная процедура эквивалента передаче в ТКС-OFDM $Q = 256$ информационных сообщений по $N = 256$ символов в каждом. Вычисления выполнялись для следующих типов модуляции поднесущих: 16-QAM,

64-QAM, 256-QAM, 1024-QAM.

Значения пик-фактора вычислялись следующим образом:

$$\mathbf{PARP1} = \frac{1}{Q} \sum_{q=0}^{Q-1} 20 \log \frac{\max_{n=0, \dots, N-1} (|s_{q,n}|^2)}{\frac{1}{N} \sum_{n=0}^{N-1} |s_{q,n}|^2}, \text{ [дБ]} \quad (18)$$

$$\mathbf{PARP2} = 20 \log \frac{\max_{q=0, \dots, Q-1} \left(\max_{n=0, \dots, N-1} (|s_{q,n}|^2) \right)}{\frac{1}{Q} \sum_{q=0}^{Q-1} \frac{1}{N} \sum_{n=0}^{N-1} |s_{q,n}|^2}, \text{ [дБ]} \quad (19)$$

Зависимости $\mathbf{PARP1}$, $\mathbf{PARP2}$ от изменения параметра a в ДрПФ ТКС-OFDM приведены на рис. 7.

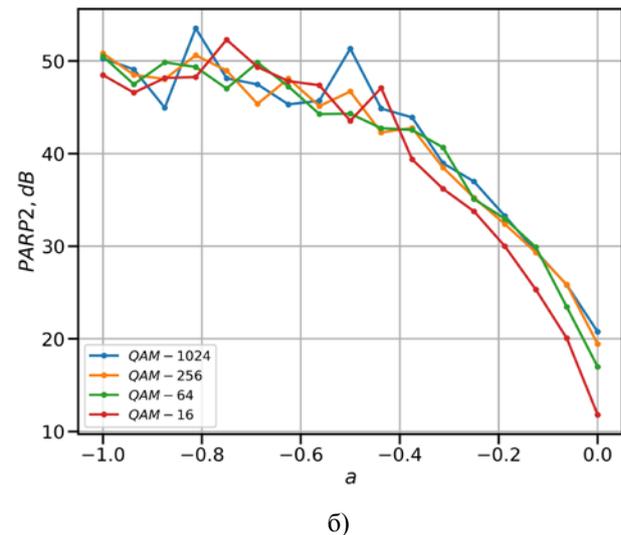
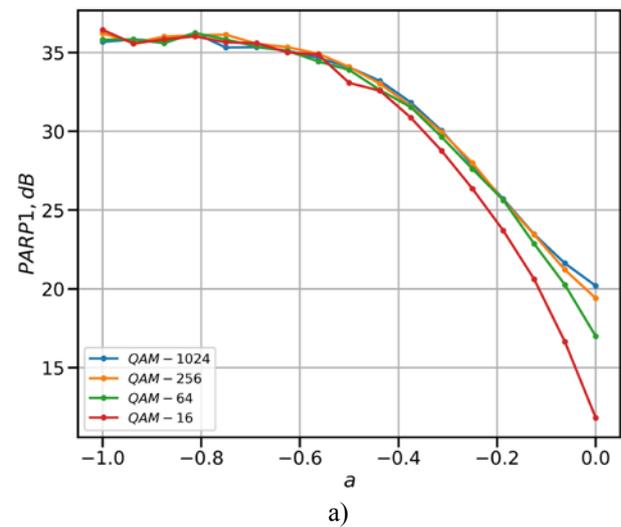


Рис 7. Зависимость а) $\mathbf{PARP1}$, б) $\mathbf{PARP2}$ от изменения параметра a в ДрПФ ТКС-OFDM для разных типов модуляции

Из рисунка 7 видно, что при плавном уменьшении параметра a в ДрПФ ТКС-OFDM наблюдается и снижение её пик-фактора. При $a = 0$ ДрПФ вырождается в тождественное преобразование, поэтому меняется и тип ТКС на ТКС с временным уплотнением (ТКС-TDM, TDM - time division multiplexing). Известно,

что системы с TDM обладают меньшим, чем системы с OFDM пик-фактором. Однако при небольших значениях a (например, $a = -0.25$) ортогональность поднесущих сохраняется. В этом случае ТКС обладает всеми преимуществами OFDM, но имеет более низкий, чем классическая ТКС-OFDM, пик-фактор. Притом уменьшение пик-фактора может быть больше 10 дБ.

Таким образом, изменение параметра a (например, в зависимости от некоторых условий) в ТКС-OFDM с ДрПФ позволяет адаптивно управлять пик-фактором этой системы, и получить значительно меньшие, по сравнению с классической ТКС-OFDM с ДПФ, его значения.

VI. ЗАКЛЮЧЕНИЕ

В статье представлена модификация классической системы с OFDM, в которой вместо классических ОП предложено использовать их дробные или многопараметрические обобщения.

Результаты моделирования воздействия прицельной помехи на передаваемый сигнал ТКС-OFDM с ДрПФ позволяют сделать вывод о том, что предложенная система является менее чувствительной к помехе такого вида, чем классическая ТКС-OFDM с ДПФ.

Исследование пик-фактора ТКС-OFDM с ДрПФ показало, что при низких значениях параметра a в ДрПФ можно получить значительное (до 10 дБ) снижение пик-фактора этой ТКС по сравнению с классической ТКС-OFDM.

Отметим, что реализация ТКС-OFDM не требует дополнительного оборудования, или специального программного обеспечения, и может применяться одновременно с иными техническими средствами защиты информации, сертифицированными регуляторами в области ИБ.

БИБЛИОГРАФИЯ

- [1] А.И. Миночкин, В.И. Рудаков, В.И. Слюсар. “Основы военно-технических исследований. Теория и приложения. Том 2.” Монография. 2011.
- [2] 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.
- [3] X. Liang, K. Zhang, X. Shen, X. Lin. “Security and privacy in mobile social networks: challenges and solutions”, *IEEE Wireless Commun.*, 2014, 21(1), pp. 33–41.
- [4] E. Jorswieck, S. Tomasin, A. Sezgin Broadcasting into the uncertainty: Authentication and confidentiality by physical-layer processing, *Proc. IEEE*, 2015, 103(10), pp. 1702–1724.
- [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] Ю.С. Шинаков. “Пикфактор сигналов OFDM и нелинейные искажения в радиооборудовании систем беспроводного доступа”, *Цифровая обработка сигналов №4/2012*, с 58–65.
- [9] 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.

- [10] S. Martugin, S. Porshnev. “Fast fractional Fourier transform”, *International Journal of Open Information Technologies ISSN: 2307-8162 vol. 12, no. 1, 2024.*
- [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.

On the possibility of increasing the noise immunity of OFDM telecommunication systems using fractional Fourier transforms

S. A. Martiugin, S. V. Porshnev

Abstract— In this article we develop a telecommunication system with orthogonal frequency-division multiplexing technology (TCS-OFDM) 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 $\alpha_0, \dots, \alpha_{N-1}$ (in case of MPOT), which change their form. When $\alpha = \pi/2$, or $\alpha_0 = \dots = \alpha_{N-1} = \pi/2$ the transformation takes the form of the classical OT, and when $\alpha = 0$, or $\alpha_0 = \dots = \alpha_{N-1} = 0$ degenerates into the identical transformation.

The results of modeling the signal transmission of the proposed TCS-OFDM with fractional Fourier transform (FrFT) under the action of a special targeting interference aimed at known vulnerabilities in the classical TCS-OFDM are presented. Comparative analysis of the proposed system and classical TCS-OFDM allowed us to conclude that TCS-OFDM with FrFT is less sensitive to this type of interference. It is also shown that proposed TCS-OFDM with FrFT has a smaller peak to average power ratio (PAPR) compared to the classical TCS-OFDM.

Realization of TCS-OFDM with FrFT does not require additional hardware or special software. The complexity of the FrFT calculation is comparable to the complexity of the classical discrete Fourier transform (DFT) calculation.

REFERENCES

- [1] A. I. Minochkin, V. I. Rudakov, V. I. Slusar “Fundamentals of military-technical research. Theory and applications”, 2011.
- [2] M. Bakulin, V. Kreindelin, A. Shloma, A. Shumov. “OFDM technology”, Telecom, 2015, 360 pp.
- [3] X. Liang, K. Zhang, X. Shen, X. Lin. “Security and privacy in mobile social networks: challenges and solutions”, *IEEE Wireless Commun.*, 2014, 21(1), pp. 33–41.
- [4] E. Jorswieck, S. Tomasin, A. Sezgin Broadcasting into the uncertainty: Authentication and confidentiality by physical-layer processing, *Proc. IEEE*, 2015, 103(10), pp. 1702–1724.
- [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] U. S. Shinalov “OFDM PARP and nonlinear distortion in radio equipment of wireless access systems”, *Digital Signal Processing* №4/2012, pp 58–65.
- [9] 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.
- [10] S. Martiugin, S. Porshnev. “Fast fractional Fourier transform”, *International Journal of Open Information Technologies ISSN: 2307-8162 vol. 12, no. 1, 2024.*
- [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.

Stepan A. Martiugin, Ural Federal University named after First President of Russia B.N. Yeltsin, smart2608@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.