Алгоритм коррекции ошибок в модулярном коде классов вычетов, обеспечивающий повышение отказоустойчивости систем OFDM

И.А. Калмыков, В.С. Сляднев, М.И. Калмыков, Т.А. Пелешенко, И.А. Проворнов

Северо-Кавказский федеральный университет, Ставрополь

Одним из направлений, позволяющим повысить эффективность работы низкоорбитального спутникового интернета в условиях деструктивных воздействий, является использование систем OFDM, поддерживающих режим скачкообразной смены частоты (ССЧ). Очевидно, что эффективность противостояния помехам, которые формируются средствами радиоэлектронной борьбы (СРЭБ), во многом определяется алгоритмом выбора рабочих частот. В работе предлагается реализовать блок ССЧ на основе SPN-шифра «Кузнечик», который обеспечивает высокую стойкость к подбору рабочей частоты со стороны СРЭБ. Однако при возникновении сбоев и отказов в работе такого блока передатчик и приемник, работающие в режиме ССЧ, не смогут наладить передачу информации. Для решения данной проблемы в статье предлагается использовать полиномиальные модулярные коды классов вычетов (ПМККВ). Однако проведенный анализ известных алгоритмов коррекции ошибок в ПМКВ показал, что их нельзя применять для повышения надежности работы блока ССЧ на основе SPN-шифра «Кузнечик». Целью работы является разработка алгоритма коррекции ошибок в кодах ПМККВ с минимальной избыточностью, применение которого позволит повысить отказоустойчивость систем OFDM за счет устранения последствий сбоев и отказов в работе блока ССЧ.

Ключевые слова: системы OFDM, поддерживающие скачкообразную смену частоты, методы генерации псевдослучайных чисел, SPN-шифр Кузнечик, полиномиальные модулярные коды классов вычетов, алгоритм коррекции ошибки.

Введение

Главной целью широкого применения технологии OFDM является обеспечение качественного скачка в повышении эффективности работы систем радиосвязи (далее СРС). Особо наглядно это проявляется в таких показателях, как скорость передачи информации и спектральная эффективность. Именно поэтому технологию OFDM рекомендуют применять в перспективных системах спутникового интернета [1,2]. Для обеспечения высокоскоростного устойчивого и достоверного обмена информацией в условиях деструктивных воздействий на беспроводные каналы передачи данных широко используются системы OFDM, поддерживающие

скачкообразную смену частот (ССЧ) [3]. Процесс ССЧ представляет собой периодическое изменение рабочей частоты передачи по определенному закону, задаваемому блоком ССЧ. Использование режима ССЧ позволяет эффективно противостоять помехам, которые формируются средствами радиоэлектронной борьбы (далее СРЭБ). Очевидно, что эффективность противодействия СРЭБ во многом зависит от надежности работы блоков ССЧ, которые вычисляют номера рабочих частот для режима ССЧ. Появление сбоев или отказов в работе данных устройств может привести к тому, что передатчик и приемник, работающие в режиме ССЧ, не смогут наладить передачу информации. Поэтому обеспечение свойства устойчивости к сбоям и отказам систем OFDM с ССЧ можно отнести к актуальным задачам.

Для решения этой задачи целесообразно выбирать методы повышения отказоустойчивости, использующие избыточные коды. Среди них можно выделить полиномиальные модулярные коды классов вычетов (ПМККВ). Эти коды способны исправлять ошибки вычислений, которые выполняются в полях Галуа $GF(2^n)$. При этом им присуще свойство диверсности в области методов обнаружения и исправления ошибок. Цель – разработать алгоритм коррекции ошибок в ПМККВ с минимальной избыточностью, применение которого позволит повысить отказоустойчивость систем OFDM за счет устранения последствий сбоев и отказов в работе блока ССЧ.

Материал и методы исследования

Тенденция интенсивного использования метода передачи OFDM прежде обусловлено всего его достоинствами [4,5]. Во-первых, к ним можно отнести увеличение скорости передачи информации за счет обеспечения параллельной передачи данных на поднесущих сигнала OFDM. Во-вторых, благодаря использованию при обработке сигналов быстрых преобразований Фурье (далее БПФ), а также цифровой фильтрации на основе целочисленной

фильтрации [6] была обеспечена высокая спектральная эффективность СРС. В-третьих, метод передачи OFDM позволяет эффективно противостоять многолучевости, возникающей при передаче сигналов. Именно поэтому разработчики систем радиосвязи используют режим ССЧ для обеспечения помехозащищенности СРС в условиях воздействия средств РЭБ. В этом случае методы передачи OFDM позволяют устранить основной недостаток систем связи с ССЧ – низкую скорость передачи данных.

Эффективность работы беспроводных систем OFDM, использующих ССЧ, в условиях тяжелой помеховой обстановки во многом определяется качеством выбора номеров рабочих частот. Так как процесс ССЧ представляет собой псевдослучайное изменение рабочей частоты, которое задается блоком ССЧ, то он должен генерировать рабочие частоты по определенному алгоритму. Блоки ССЧ могут использовать регистры сдвига с линейной обратной связью, позволяющие генерировать псевдослучайную последовательность элементов поля Галуа [3]. В работе [7] предлагается для генерации псевдослучайного набора целых 128-битовых чисел использовать метод Мерсенна Твистера. Для псевдослучайного изменения рабочих частот может быть использован линейный конгруэнтный генератор, работа которого описана в [8]. Особое место среди методов генерации псевдослучайных чисел занимает отечественный стандарт SPN-шифра.

1. Отечественный стандарт SPN- шифра

На рисунке 1 показана структура SPN-шифра «Кузнечик». Данный шифр работает следующим образом. На вход шифратора подается открытый текст, размер которого 128 бит. Далее выполняется девять раундов шифрования, которые включают в себя смешивание с раундовым ключом K_i (X_i), где $i = 1, \ldots, 9$; нелинейное преобразование (S_i); - линейное (L_i) преобразование. После выполнения этих раундов выполняется сложение по модулю два с десятым раундовым ключом K_{10}. В результате, после данной

операции с выхода шифратора в канал связи поступает закрытый текст, размер которого 128 бит [9].

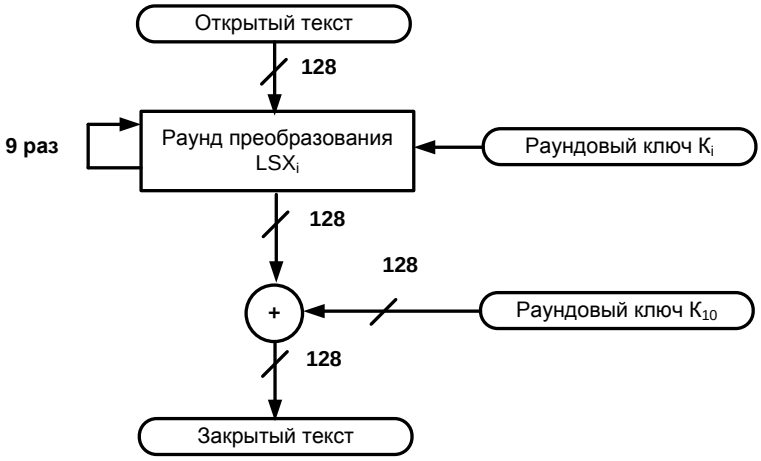

Рисунок 1. - Отечественный SPN-шифр «Кузнечик»

При реализации шифра входной блок текста, как и промежуточные результаты, представляются в виде элементов расширенного поля $GF(2^8)$. Порождающим многочленом данного поля выбран $p(x) = x^8 + x^7 + x^6 + x + 1$. В этом случае блок размером 128 бит разбивается на 16 байтов. Каждый байт при выполнении вычислений считается элементом поля Галуа $GF(2^8)$.

Для повышения отказоустойчивости работы шифратора отечественного стандарта «Кузнечик» можно воспользоваться решением, которое применено для подобного SPN-алгоритма AES. В работе [10] показана возможность перехода от вычислений в поле $GF(2^8)$ к вычислениям в составных полях. В статье рассмотрено выполнение преобразований Subbyte и InvSubbyte в условиях декомпозиции поля $GF(2^8)$ в $GF((2^4)^2)$, что позволило снизить аппаратурные затраты, а также повысить скорость шифрования AES. Таким образом, можно сделать вывод о том, что отечественный SPN-шифр «Кузнечик» можно реализовать в кольце полиномов, используя ПММКВ.

2 Принципы построения полиномиальных модулярных кодов классов вычетов

Полиномиальный модулярный код классов вычетов относится к непозиционным кодам, с помощью которых можно проводить арифметические вычисления в расширенных полях Галуа. В качестве оснований ПМККВ используются неприводимые многочлены $p_1(x),\ldots,p_k(x)$. Данные основания используются для получения остатков при делении полинома $G(x)=g_m x^m+\ldots+g_1 x^1+g_0 x$. В этом случае полученный набор остатков и будет кодовой комбинацией ПМККВ

$$G(x)=(G_1(x),\ldots,G_k(x)), \quad (1)$$

где $G_i(x)\equiv G(x)\bmod p_i(x);\ i=1,\ldots,k$.

При этом степень полинома $m=\deg G(x)$ должна быть меньше степени рабочего диапазона ПМККВ:

$$m<\deg P_k(x), \quad (2)$$

который определяется, как:

$$P_k(x)=\prod_{i=1}^{k} p_i(x). \quad (3)$$

Пусть имеем два полинома $G(x)$ и $M(x)$, для которых справедливо (2). Тогда для их представления в модулярном коде $G(x)=(G_1(x),\ldots,G_k(x))$ и $M(x)=(M_1(x),\ldots,M_k(x))$справедливы выражения

$$G(x)+M(x)=\left(G_1(x)+M_1(x)\bmod p_1(x),\ldots,G_k(x)+M_k(x)\bmod p_k(x)\right), \quad (4)$$

$$G(x)\cdot M(x)=\left(G_1(x)\cdot M_1(x)\bmod p_1(x),\ldots,G_k(x)\cdot M_k(x)\bmod p_k(x)\right), \quad (5)$$

где $M_i(x)\equiv M(x)\bmod p_i(x);\ i=1,\ldots,k$.

Основные достоинства ПМККВ, которые наглядно видны в равенствах (4) и (5), это параллельные и независимые вычисления по основаниям кода. В результате этого, данные модулярные коды нашли применения в системах, в

которых требуется высокая скорость вычислений [11-13]. Кроме этого, ПМККВ обладают значительным потенциалом для коррекции ошибок, которые могут возникнуть при вычислениях.

3 Разработка алгоритма коррекции ошибок в ПМККВ с использованием одного основания

Для исправления однократной ошибки в ПМККВ (искажение одного остатка), необходимо ввести два контрольных основания $p_{k+1}(x)$, $p_{k+2}(x)$:

$$\deg p_{k-1}(x) \le \deg p_k(x) \le \deg p_{k+1}(x) \le \deg p_{k+2}(x). \quad (6)$$

Это приводит к увеличению разрядности кодовой комбинации:

$$G(x) = (G_1(x), \ldots, G_k(x), G_{k+1}(x), G_{k+2}(x)). \quad (7)$$

При этом также расширяется диапазон ПМККВ:

$$P_{k+2}(x) = \prod_{i=1}^{k+2} p_i(x) = P_k \prod_{i=k+1}^{k+2} p_i(x). \quad (8)$$

В избыточном ПМККВ комбинация (7) не содержит ошибку, если:

$$\deg G(x) < \deg P_k(x). \quad (9)$$

Но ПМККВ – это непозиционные коды, в которых сразу нельзя проверить условие (9). Поэтому для коррекции ошибок в ИПМК разрабатываются алгоритмы вычисления позиционных характеристик (ПХ) [11-13]. Однако известные алгоритмы вычисления ПХ непригодны для повышения отказоустойчивости систем OFDM, использующих блоки ССЧ на основе SPN-шифра «Кузнечик», так как при реализации подхода [10] в качестве контрольного основания может быть использован только один неприводимый полином. Поэтому необходимо провести разработку алгоритма коррекции ошибок в ПМККВ, способного исправлять однократные ошибки с использованием одного контрольного основания.

Известно, что введение двух избыточных оснований $p_{k+1}(x)$, $p_{k+2}(x)$ приводит к расширению кодовой комбинации на два остатка $G_{k+1}(x), G_{k+2}(x)$.

Значит, в разрабатываемом алгоритме должна быть возможность получения двух избыточных остатков, используя одно контрольное основание. При этом эти остатки должны указывать местоположение ошибочного остатка, а также глубину возникшей ошибки. Тогда, в разработанном алгоритме коррекции с одним избыточным основанием, контрольные остатки определяются следующим образом:

$$\begin{cases} G_3(x) = G_3^* = G_1(x) + G_2(x), \\ G_4(x) = G_4^* = G_1(x) + xG_2(x) \bmod p_3(x). \end{cases} \quad (10)$$

В работе [14] представлен алгоритм коррекции ошибок в модулярном коде, который использовал ПХ – невязку. В данном алгоритме, используя информационные остатки, вычислялись контрольные вычеты кодовой комбинации $\alpha_{k+1}^*, \alpha_{k+2}^*$. Затем они подавались на вычитатели по модулю p_{k+1}, p_{k+2}, где выполнялась операция невязки контрольных остатков:

$$\begin{cases} \delta_1 = \left|\alpha_{k+1} - \alpha_{k+1}^*\right|_{p_{k+1}}^+, \\ \delta_2 = \left|\alpha_{k+2} - \alpha_{k+2}^*\right|_{p_{k+2}}^+, \end{cases} \quad (11)$$

где $\alpha_{k+1}, \alpha_{k+2}$ – остатки избыточной кодовой комбинации.

Полученная невязка поступала на вход блока памяти, с выхода которого снимался вектор ошибки в модулярном коде. Данный вектор и кодовая комбинация поступали на сумматоры по модулю $p_1, \ldots, p_{k+2}$, где происходила коррекция ошибочной комбинации. Тогда в разработанном алгоритме коррекции невязки избыточных остатков будут определяться:

$$\begin{cases} \delta_1(x) = G_3(x) + G_3^*(x), \\ \delta_2(x) = G_4(x) + G_4^*(x), \end{cases} \quad (12)$$

где $G_3(x), G_4(x)$ – остатки кодовой комбинации (7); $G_3^*(x), G_4^*(x)$ – избыточные остатки, которые вычислены с помощью (10).

При этом, разработанный алгоритм позволяет сократить аппаратные затраты по сравнению с [14]. Пусть после выполнения одного из

преобразований SPN-шифра «Кузнечика» была получена комбинация $(\tilde{G}_1(x), G_2(x), G_3(x), G_4(x))$, в которой ошибка произошла в первом остатке по модулю $p_1(x) = x^4 + x + 1$. Искаженный остаток получается путем суммирования по модулю два истинного остатка и глубины ошибки $\Delta G_1(x)$:

$$\tilde{G}_1(x) = G_1(x) + \Delta G_1(x), \quad (13)$$

где $\tilde{G}_1(x)$ – искаженный остаток; $\deg \Delta G_1(x) < \deg p_1(x)$.

Воспользуемся (11) и определим первый контрольный остаток:

$$G_3^*(x) = \tilde{G}_1(x) + G_2(x) = (G_1(x) + G_2(x)) + \Delta G_1(x). \quad (14)$$

Если данное значение подставить в первое равенство (11), то:

$$\delta_1(x) = G_3(x) + G_3(x) = \Delta G_1(x). \quad (15)$$

А это глубина однократной ошибки в искаженной комбинации.

В этом случае, для искаженной комбинации ИПМК, имеем:

$$G_4(x) = \left|(G_1(x) + \Delta G_1(x)) + x \cdot G_2(x)\right|_{p_3(x)}. \quad (16)$$

Подставим (16) в выражение (11). Тогда получаем:

$$\delta_2(x) = G_4(x) + G_4(x) = \Delta G_1(x). \quad (17)$$

Так как $\delta_1(x) = \delta_2(x) = \Delta G_1(x)$, то исправление ошибки в первом остатке можно выполнить без использования вектора ошибки:

$$G_1(x) = \tilde{G}_1(x) + \Delta\delta_1(x). \quad (18)$$

Таким образом, разработанный алгоритм коррекции позволяет сократить объем блока памяти, где хранятся вектора ошибок, на 25%.

4 Результаты исследования и их обсуждение.

Рассмотрим пример повышения отказоустойчивости систем OFDM, поддерживающих режим ССЧ. Так как порождающим многочленом, используемым в SPN-сети «Кузнечик», является $p(x) = x^8 + x^7 + x^6 + x + 1$, то

рабочими модулями выступают $p_1(x)=x^4+x+1$ и $p_2(x)=x^4+x^3+1$, а $p_3(x)=x^4+x^3+x^2+x+1$ – контрольный модуль.

Рассмотрим операцию смешивания с первым раундовым ключом. Выберем в качестве байта открытого текста a(0) = 218_{10} = 11011010_2. Выполним операцию смешивания (сложения по модулю два) байта с байтом первого раундового ключа $k^1(0) = 77_{10} = 0100\ 1101_2$. Результатом является:

$$x^1(0)=a(0)+k^1(0)=10010111=x^7+x^4+x^2+x+1.$$

Представим байт открытого текста в избыточном ПМККВ:

$$a(0)=x^7+x^6+x^4+x^2+x=(x^3+x^2+x\,||\,x^3+x+1\,||\,x^2+1\,||\,x^2+x+1).$$

Представим байт первого раундового ключа в избыточном ПМККВ:

$$k^1(0)=x^6+x^3+x^2+1=(1\,||\,x\,||\,x+1\,||\,x^2+1).$$

Выполним операцию суммирования по модулю два. Получаем:

$$s^1(0)=a(0)+k^1(0)=(x^3+x^2+x+1\,||\,x^3+1\,||\,x^2+x\,||\,x).$$

Проведем проверку полученного результата. Для этого воспользуемся (10) и вычислим контрольные остатки:

$$s_3^*(0)=x_1^1(0)+x_2^1(0)=x^2+x.\quad s_4^*(0)=\left|x_1^1(0)+x\cdot x_2^1(0)\right|_{p_3(x)}=x.$$

Подставляем полученные результаты в (12) и вычисляем:

$$\begin{cases}\delta_1(x)=s_3^1(x)+s_3^*(x)=(x^2+x)+(x^2+x)=0.\\ \delta_2(x)=s_4^1(x)+s_4^*(x)=x+x=0.\end{cases}$$

Так как невязка равна нулю, то комбинация не содержит ошибки.

Пусть при выполнении смешивания ошибка глубиной $\Delta s_1=x^3$ произошла в первом остатке. Тогда, используя (13), получаем:

$$\tilde{s}_1(x)=s_1(x)+\Delta s_1(x)=(x^3+x^2+x+1)+x^3=x^2+x+1.$$

В этом случае искаженная комбинация имеет вид:

$$\tilde{s}^1(0)=(x^2+x+1\,||\,x^3+1\,||\,x^2+x\,||\,x).$$

Вычислим контрольные остатки, используя (10):

$$s_3^*(0)=\tilde{x}_1^1(0)+x_2^1(0)=x^3+x^2+x.\quad s_4^*(0)=\left|\tilde{x}_1^1(0)+x\cdot x_2^1(0)\right|_{p_3(x)}=x^3+x.$$

Подставляем полученные результаты в (12):

$$\begin{cases}\delta_1(x)=s_3^1(x)+s_3^*(x)=(x^2+x)+(x^3+x^2+x)=x^3.\\ \delta_2(x)=s_4^1(x)+s_4^*(x)=x+(x^3+x)=x^3.\end{cases}$$

Так как $\delta_1(x)=\delta_2(x)=x^3$, то корректируется первый остаток:

$$s_1(x)=\tilde{s}_1(x)+\Delta\delta_1(x)=(x^2+x+1)+x^3=x^3+x^2+x+1.$$

Пусть ошибка с глубиной $\Delta s_2=x$ произошла во втором остатке. Тогда

$$\tilde{s}^1(0)=(x^3+x^2+x+1\|x^3+x+1\|x^2+x\|x).$$

Вычислим контрольные остатки, используя (10):

$$s_3^*(0)=\tilde{x}_1^1(0)+x_2^1(0)=x^2.\quad s_4^*(0)=\left|\tilde{x}_1^1(0)+x\cdot x_2^1(0)\right|_{p_3(x)}=x^2+x.$$

Подставляем полученные результаты в (12):

$$\begin{cases}\delta_1(x)=s_3^1(x)+s_3^*(x)=(x^2+x)+x^2=x.\\ \delta_2(x)=s_4^1(x)+s_4^*(x)=x+(x^2+x)=x^2.\end{cases}$$

Данной невязки соответствует вектор ошибки $\bar{e}(x)=(0\|x\|0\|0\|0)$, который хранится в блоке памяти. Исправим искаженную комбинацию:

$$s_1(x)=\tilde{s}^1(0)+\bar{e}(x)=(x^3+x^2+x+1\|x^3+1\|x^2+x\|x).$$

Заключение

В статье предложено использовать полиномиальные модулярные коды классов вычетов при выполнении SPN-преобразования «Кузнечик», обеспечивающего режим ССЧ для систем OFDM. Переход к вычислениям в полях GF(2^4) позволяет обнаруживать и корректировать ошибки, которые возникают при реализации SPN-преобразований. В работе осуществлена разработка и исследование алгоритма коррекции ошибок в ПМККВ, позволяющих исправлять однократные ошибки на основе использования одного контрольного основания. При этом разработанный алгоритм

обеспечивает снижение на 25% объема блока памяти, где хранятся вектора ошибок, по сравнению с прототипом [14]. Представленные примеры показывают процесс обнаружения и коррекции ошибок в ПМККВ с использованием разработанного алгоритма.

Исследование выполнено за счет гранта Российского научного фонда № 23-21-00036, rscf.ru/project/23-21-00036/.

Литература

1. Oughton Edward, J. A review paper on, A Techno-Economic Framework for Satellite Networks Applied to Low Earth Orbit Constellations. Assessing Starlink, OneWeb and Kuiper, IEEE Access, vol. 9, October 2021, pp. 141611-141622.

2. Shreehari H.S., Makam Supreeth Starlink Satellite Internet Service. International Journal of Research Publication and Reviews, 2022, Vol 3, no 6, pp. 4501-4504.

3. Макаренко С.И., Иванов М.С. Помехозащищенность систем связи с псевдослучайной перестройкой рабочей частоты. Монография. СПб.: Свое издательство, 2013. 166 с.

4. Бакулин М.Г., Крейнделин В.Б., Шумов А.П. Технология OFDM. Учебное пособие для вузов. М.: Горячая линия-Телеком, 2017. 352 с.

5. Parveen N., Abdullah K., Islam R. Diversity Technique Using Discrete Wavelet Transform in OFDM System. International Journal of Engineering and Advanced Technology (IJEAT), 2019, Vol 8, Issue 2S2. pp. 284-286.

6. Kalmykov M.I, Yurdanov D.V. Development of a Fast Algorithm of Number-Theoretic Signal Transformation for OFDM Communication Systems Using UFMC Technology // Proceedings of the 8th scientific conference on information technologies for intelligent decision making support (ITIDS 2020). Advances in Intelligent Systems Research Том: 174 Стр. 150-154.

7. Saito M., Matsumoto M. SIMD-oriented Fast Mersenne Twister: a 128-bit Pseudorandom Number Generator. Monte Carlo and QuasiMonte Carlo Methods 2006, pp. 607 - 622.

8. Schneier, B. Applied Cryptography: Protocols, Algorithms and Source Code in C. Wiley New York. 2017, 784 p.

9. Biryukov A., Perrin L., Udovenko A. Reverse-engineering the S-Box of Streebog, Kuznyechik and STRIBOBr1 // Advances in cryptology – EUROCRYPT 2016. Springer, 2016, pp. 372 - 402.

10. Gnanambika M., Adilakshmi S., Noorbasha F. AES-128 Bit Algorithm Using Fully Pipelined Architecture for Secret Communication // International Journal of Engineering Research and Applications. 2013. Vol. 3, Issue 2, pp.166-169.

11. Чистоусов Н.К., Калмыков И.А., Чипига А.Ф. Разработка протоколов аутентификации низкоорбитальных космических аппаратов на основе параллельных кодов систем остаточных классов // Инженерный вестник Дона, 2021, №4. URL: ivdon.ru/ru/magazine/archive/n4y2021/6912.

12. Mohan A. Residue Number Systems. Theory and Applications. Springer International Publishing Switzerland. 2016, 351 p.

13. Чистоусов Н.К., Калмыкова Н.И., Духовный Д.В. Ортогональная обработка сигналов с использованием математических моделей целочисленных вейвлет-преобразований, реализованных в модулярных кодах классов вычетов // Инженерный вестник Дона, 2023, №3. URL: ivdon.ru/ru/magazine/archive/n3y2023/8273.

14. Червяков Н.И., Коляда А.А. Модулярная арифметика и ее приложения в инфокоммуникационных технологиях. М.: ФИЗМАТЛИТ, 2017. 400 с.

References

1. Edward, J. Oughton Assessing Starlink, OneWeb and Kuiper, IEEE Access, vol. 9, October 2021. pp. 141611-141622.

2. Shreehari H.S., Makam Supreeth International Journal of Research Publication and Reviews, 2022, Vol 3, № 6. pp. 4501-4504.

3. Makarenko S.I., Ivanov M.S. Pomehozashhishhennost' sistem svjazi s psevdosluchajnoj perestrojkoj rabochej chastoty. Monografija [Noise immunity of communication systems with pseudorandom adjustment of the operating frequency. Monograph]. Sankt-Peterburg.: Svoe izdatel'stvo, 2013. 166 p.

4. Bakulin M.G., Krejndelin V.B., Shumov A.P. Tehnologija OFDM. Uchebnoe posobie dlja vuzov [OFDM technology. Textbook for universities]. Moskva: Gorjachaja linija-Telekom, 2017. 352 p.

5. Parveen N., Abdullah K., Islam R. International Journal of Engineering and Advanced Technology (IJEAT). 2019.Vol 8, Issue 2S2. pp. 284 - 286.

6. Kalmykov M.I, Yurdanov D.V. Proceedings of the 8th scientific conference on information technologies for intelligent decision-making support (ITIDS 2020). Advances in Intelligent Systems Research Vol 174. pp. 150 - 154.

7. Saito M., Matsumoto M. SIMD-oriented Fast Mersenne Twister: a 128-bit Pseudorandom Number Generator. Monte Carlo and QuasiMonte Carlo Methods 2006, pp. 607–622.

8. Schneier B. Applied Cryptography: Protocols, Algorithms and Source Code in C. Wiley New York. 2017. 784 p.

9. Biryukov A., Perrin L., Udovenko A. Reverse-engineering the S-Box of Streebog, Kuznyechik and STRIBOBr1. Advances in cryptology – EUROCRYPT 2016. Springer, 2016, pp. 372 - 402.

10. Gnanambika M., Adilakshmi S. International Journal of Engineering Research and Applications. 2013. Vol. 3, Issue 2, pp.166-169.

11. Chistousov N.K., Kalmykov I.A., Chipiga A.F. Inzhenernyj vestnik Dona, 2021, №4. URL: ivdon.ru/ru/magazine/archive/n4y2021/6912.

12. Mohan A. Residue Number Systems. Theory and Applications. Springer International Publishing Switzerland. 2016. 351 p.

13. Chistousov N.K., Kalmykova N.I., Duhovnyj D.V. Inzhenernyj vestnik Dona, 2023, №3. URL: ivdon.ru/ru/magazine/archive/n3y2023/8273

14. Chervjakov, N.I. Koljada A.A. Moduljarnaja arifmetika i ee prilozhenija v infokommunikacionnyh tehnologijah [Modular arithmetic and its applications in infocommunication technologies]. Moskva: FIZMATLIT, 2017. 400 p.

Дата поступления: 15.01.2024

Дата публикации: 21.02.2024