УДК 681.3.06.543

**Толюпа С.В., Сташук О.В., Дружинін В.А.**

# ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ІНФОКОМУНІКАЦІЙНИХ СИСТЕМАХ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ НА ОСНОВІ МЕТОДУ ЕНЕРГЕТИЧНО-ЕФЕКТИВНОГО ПЕРЕТВОРЕННЯ ІКМ-СИГНАЛІВ

Розроблено принципово новий, в порівнянні з існуючими в сучасних інформаційно-телекомунікаційних системах (ІТС), метод багатоканальної передачі інформації шляхом перетворення ІКМ (імпульсно-кодова модуляція) сигналів в позиційні кодово-імпульсні сигнали (ПКІ) з подальшою маніпуляцією псевдовипадковими послідовностями. Запропонований метод дозволяє підвищити енергетичну ефективність та прихованість при передачі цифрових сигналів, що є особливо актуальним для ІТС спеціального призначення.

***Ключеві слова:*** інфокомунікаційні системи, бінарна імпульсно-кодова модуляція, цифровий сигнал, цифровий код.

**Вступ.** Одним з головних завдань, які вирішуються при створенні та функціонуванні інфокомунікаційних систем спеціального призначення (ІКС СП) є забезпечення належного рівня безпеки інформації. Вирішення цього завдання покладається на систему захисту інформації (СЗІ), як невід'ємну складову ІКС. СЗІ являє собою складну організаційно-технічну, економічну й інформаційну систему і складається з організаційних та інженерних заходів, фізичних засобів захисту, комплексу технічного захисту інформації (ТЗІ) та комплексу засобів захисту від несанкціонованого доступу.

Аналіз загроз безпеці інформації та методів захисту від них, проведений в [1] показав, що поряд з криптографічними методами захисту інформації одним з основних напрямків забезпечення безпеки інформації в інфокомунікаційних систем спеціального призначення є застосування методів підвищення прихованості передачі сигналів. Тому вдосконалення існуючих та розробка нових методів формування та обробки сигналів, спрямованих на підвищення прихованості та енергетичної ефективності є перспективним напрямком досліджень у галузі інформаційної безпеки.

В даний час в ІКС СП широко застосовується спосіб передачі сигналів, в якому в якості цифрового коду використовується бінарна імпульсно-кодова модуляція (ІКМ).

Метою статті є розробка методу енергетично-ефективного перетворення ІКМ сигналів для багатоканальних систем передачі, що функціонують у складі інформаційно-телекомунікаційних систем спеціального призначення.

**Основна частина.** Задача підвищення енергетичної ефективності в ІКС має комплексний характер і складається з цілого ряду аспектів, основними з яких є два:

1) енергетичні витрати на функціонування апаратури;

2) енергетичні витрати на передачу інформації, тобто витрати енергії, яка спрямовується безпосередньо в телекомунікаційний тракт.

В статті запропоновано рішення другого аспекту задачі, шляхом формування принципово нової, порівняно з ІКМ, структури цифрового сигналу. При перетворенні початкового сигналу (стандартного сигналу ІКМ) такі характеристики системи, як необхідна смуга частот, завадостійкість та інформаційна швидкість передачі, потрібно зберегти незмінними, такими ж, як і у відповідних структур ІКМ сигналів. Це дасть можливість застосовувати даний спосіб на діючих телекомунікаційних трасах стандарту Е1.

В існуючих системах передачі з ІКМ структури (формати) сигналів складаються з послідовності кодових комбінацій (КК), які об'єднуються в цикли і надцикли. Такі структури містять $k$-розрядні кодові комбінації, де кількість енергетично наповнених одиниць в середньому дорівнює $k/2$. Однак, при застосуванні замість бінарного, багатопозиційного, або $M$-арного кодування [2–4], відбувається підвищення енергетичної ефективності при передачі цифрових сигналів.

При $M$-арному способі передаються не $k$-розрядні кодові комбінації (КК), а одиночні імпульсні сигнали-символи (блоки), кожен з яких, містить в одному зі своїх параметрів інформацію про цифрове значення відповідної $k$-бітової КК, тобто дискретної (за

Котельниковим) вибірки. $M$ символів багатопозиційного $M$-арного алфавіту пов'язані з кількістю $k$ біт, які входять до складу КК, співвідношенням:

$$M = 2^k \text{ або } k = \log_2 M. \tag{1}$$

Сутність розробленого методу полягає в тому, що замість кожної $k$-розрядної кодової комбінації окремого канального інтервалу (КІ) формується лише один імпульс-символ, в якому цифрова інформація, на відміну від ІКМ, міститься не в розміщенні нульових і одиничних імпульсів на відповідних розрядних позиціях кодової комбінації, а в номері тієї квантованої часової позиції, на якій розміщується цей одиночний імпульс (рис. 1) [5, 6]. Назвемо такий інформаційно-насичений імпульс, що містить інформацію про всю кодову комбінацію, позиційним код-імпульсом (ПКІ).

Всі реальні системи передачі мають обмежену смугу частот передачі $\Delta f$ та обмежене значення пікової потужності $P$ (обмежений динамічний діапазон). Для отримання енергетичного виграшу, не виходячи при цьому за межі відведених для тракту стандартної смуги частот і обмеженого динамічного діапазону, необхідно, щоб ПКІ мав тривалість $\tau_{ПКІ}$ і потужність $P_{ПКІ}$ такі ж самі, як у одиночного імпульсу ІКМ кодової комбінації:

$$\tau_{ПКІ} = \tau_{ІКМ}, P_{ПКІ} = P_{ІКМ}. \tag{2}$$

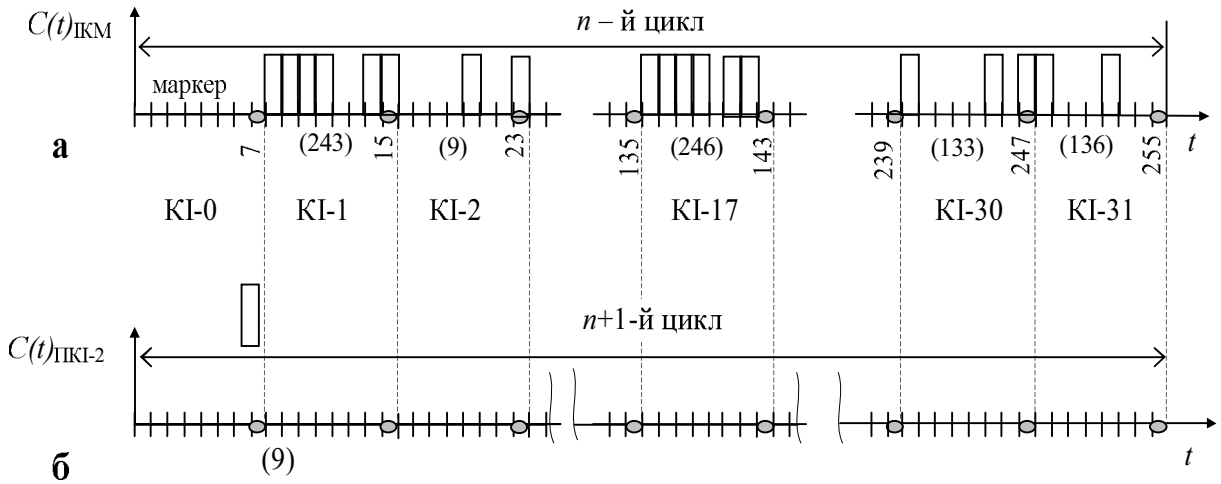


Рис. 1. Перетворення ІКМ-сигналів у позиційні код-імпульсні сигнали на прикладі другого каналу:
а - один цикл ІКМ сигналу, який містить 32 канальних інтервали;
б - ПКІ сигнал другого каналу (другого канального інтервалу)

Всі подальші перетворення утвореного ПКІ повинні виконуватись при забезпеченні умови, що значення його енергії буде залишатись постійним.

Отже, зберігання смуги частот тракту буде дотримано при виконанні умови $\tau_{ПКІ} = \tau_{ІКМ}$.

Щодо завадостійкості, то, як відомо, визначальним фактором тут є енергія одиночного імпульсу (біта) $E_б = P_б \times \tau_б$, або точніше, відношення $\alpha^2 = \frac{E_б}{N_0}$, де $N_0$ - спектральна щільність потужності завади. Потенційна завадостійкість цифрових систем оцінюється ймовірністю бітової помилки $P_{пом}$, яка визначається за критерієм ідеального спостерігача і для двійкової фазової маніпуляції знаходиться з наступного виразу:

$$P_{пом} = Q\left(\sqrt{\frac{E_б}{N_0}}\right), \tag{3}$$

де $Q(\alpha)=\frac{1}{\sqrt{2\pi}}\int_{\alpha}^{\infty}e^{-\frac{t^2}{2}}dt$ - табульована функція інтегралу ймовірності [2]. Проведемо співставлення ймовірності помилки при використанні ПКІ з такою ж ймовірністю помилки для ІКМ. Оскільки потужність і тривалість одиночних імпульсів ПКІ та ІКМ однакові, то $\alpha_{ПКІ}=\alpha_{ІКМ}=\alpha$. Тому для одиночних імпульсів ймовірність помилки $P_{\text{пом}}$, яка залежить від аргументу інтеграла ймовірності $\alpha$, буде мати однакове значення для ПКІ і ІКМ. Тобто, потенційна завадостійкість ПКІ буде однаковою з ІКМ.

Але при передачі одного дискретного знака повідомлення в ІКМ використовується, в середньому, $k/2$ імпульсів, в той час, як в розробленому методі лише один. Очевидно, що завдяки цьому при передачі відбувається енергетичний виграш. Крім того, при прийомі кодових комбінацій відбувається накопичення помилок кожного з $k$ імпульсів (бітів), тобто сумарна помилка кодової комбінації $P_{\text{пом кк}}$ зростає, порівняно з бітовою помилкою $P_{\text{пом}}$, відповідно до виразу [8]:

$$P_{\text{пом кк}}=1-\left[1-Q\left(\sqrt{E_{\text{б}}/N_0}\right)\right]^k. \qquad (4)$$

Розраховані за цією формулою характеристики показано на рис. 2. Використання цих характеристик дозволяє провести розрахунок потенційних можливостей ІКМ та ПКІ сигналів і розрахувати енергетичний виграш запропонованого методу $\beta_{\text{E}}$.

Розрахунок характеристик та їх аналіз проведено для цифрового ІКМ сигналу, де за зразок взято формат кадру стандарту Е1, основу якого складають 8-розрядні кодові комбінації $(k=8)$. В таких ІКМ кодових комбінаціях кількість енергетично наповнених одиниць, в середньому, дорівнює $k/2$ (за умови однакової ймовірності з'явлення нуля або одиниці на кожній розрядній позиції).

Розглянемо найпростіший випадок звичайного сигналу ІКМ та виконаємо порівняння результатів з сигналами ПКІ.

Характеристики, подібні до характеристик на рис. 2, мають широке розповсюдження [2, 3, 7] і дозволяють визначати величину аргументу $\alpha^2=\frac{E_{\text{б}}}{N_0}$ потрібну для забезпечення заданого значення помилки $P_{\text{пом}}$. На основі використання цих характеристик проведено визначення потенційних значень для показників енергетичної ефективності та розраховано енергетичний виграш $\beta_{\text{E}}$, який може бути досягнуто. Очевидно, що більш енергетично ефективною буде та структура цифрового сигналу, для якої величина $\beta=1/\alpha^2$ буде мати більше значення. Отже величина $\beta$ характеризує енергетичну ефективність сигналу при його прийомі. Але в ній аж ніяк не враховується кількість енергетично наповнених імпульсів кодової комбінації, які посилаються в телекомунікаційний тракт, тобто не враховані повні енергетичні витрати цифрового сигналу при його передачі. Такі витрати враховуються кількістю імпульсів $k$, потрібних для передачі одного дискретного (за Котельниковим) виміру $k_{\text{потр.}}$. Для сучасних ІКМ систем в середньому $k_{\text{потр.}}=8/2=4$. Для розробленої ПКІ системи $k_{\text{потр.}}=1$. З урахуванням сказаного, зрозуміло, що більш енергетично економічною слід вважати ту систему, для якої показник $\gamma=1/k_{\text{потр}}$ має більше значення. Введемо показник, який характеризує енергетичну ефективність власне сигналу. За такий загальний енергетичний показник $\varphi$ приймемо добуток $\varphi=\beta\cdot\gamma$ $\frac{1}{\alpha^2}\cdot\frac{1}{k_{\text{потр}}}=\frac{1}{\alpha^2\cdot k_{\text{потр}}}$. Тоді загальний

виграш в системі $\varphi_{\text{ПКІ}}$, порівняно з системою $\varphi_{\text{ІКМ}}$ (з урахуванням енергетичних показників як при прийомі так і при передачі), буде дорівнювати:

$$\beta_E = \frac{\varphi_{\text{ПКІ}}}{\varphi_{\text{ІКМ}}}. \tag{5}$$

За наведеними в статті характеристиками потенційний енергетичний виграш для сигналів ПКІ порівняно з сигналами ІКМ буде:

$$\beta_E = \varphi_{\text{ПКІ}} \Big/ \varphi_{\text{ікм}} \quad \frac{1}{1\cdot\alpha^2{}_{\text{ПКІ}}} \Big/ \frac{1}{4\cdot\alpha^2{}_{\text{ІКМ}}} \quad 4{,}82\,. \quad = \tag{6}$$

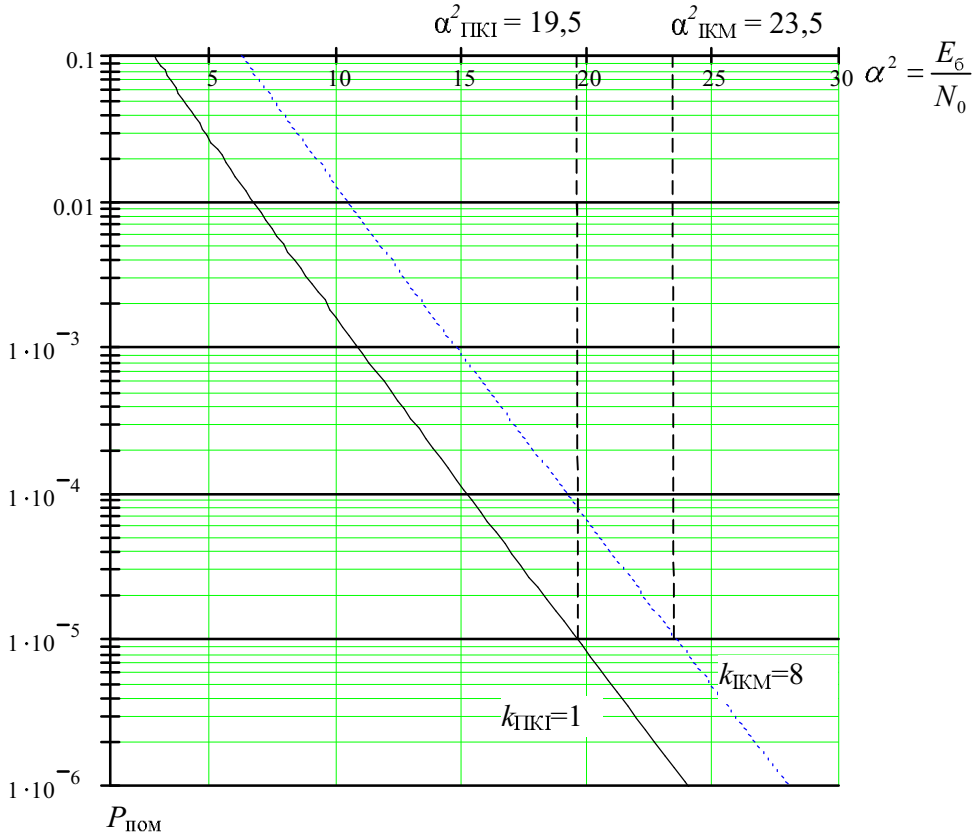


Рис. 2. Розрахунок залежності $P_{\text{пом}}$ від $E_{\text{б}}/N_0$

Вираз (6) характеризує максимально можливе значення енергетичного виграшу в ПКІ-системі. Досягнення енергетичного виграшу не повинно призводити до зменшення швидкості роботи системи. Для того щоб швидкість передачі не була знижена, а залишилась незмінною, необхідно знайти потрібну кількість квантованих часових позицій для кожного ПКІ. При дотриманні умов виразу (2) для передачі замість однієї восьмирозрядної кодової комбінації лише одного ПКІ необхідно мати не 8, а $L = 2^8 = 256$ квантованих часових позицій, на одній з яких повинен розташовуватись ПКІ. Така кількість часових позицій в системі, яка використовує восьмирозрядні кодові комбінації (наприклад, ІКМ-30/32), відводиться для передачі цілого циклу, який складається з $N = 32$ кодових комбінацій. Тому на форматі одного циклу, що містить $L$ квантованих часових позицій, необхідно сформувати ПКІ не одного, а всіх $N$ каналів. Для того, щоб реалізувати цю можливість, необхідно виділити резерв часу тривалістю рівно один цикл $T_{\text{ц}}$.

Таким чином, сформовані за таким принципом ПКІ виявляються розташованими не послідовно канал за каналом, як кодові комбінації ІКМ, а в іншому порядку. Утворені ПКІ

розміщуються на $N$ паралельних виходах. Кожен на своєму виході та на відповідній квантованій часовій позиції.

Далі необхідно кожному ПКІ надати індивідуальну відрізнювальну ознаку, яка показувала б його канальний порядковий номер $i$. Імпульсними сигналами, що мають такі індивідуальні ознаки є різного роду ортогональні імпульсні псевдовипадкові послідовності (ПВП) [4, 8]. Кожний $i$-й ПКІ перетворюється у відповідну $i$-ту ПВП. При цьому буде відбуватися взаємне накладання ПВП різних каналів, а також можливе накладання ПВП одного каналу (рис. 3). Але це не призводить до порушення прийому сигналів, оскільки при використанні методів оптимального прийому, заснованих на обробці квазіортогональних ПВП за допомогою узгоджених фільтрів, буде здійснено незалежне відтворення кожного з сигналів, які накладалися. Сигнал відповідного узгодженого фільтру буде прийматися із загальної суміші усіх інших сигналів, які будуть сприйматися як адитивна інтерференція (шум). Принцип обробки сигналів такої системи на приймальному боці буде аналогічним асинхронно адресній системі зв'язку з кодовим розділенням каналів, яка описана в літературі [4].

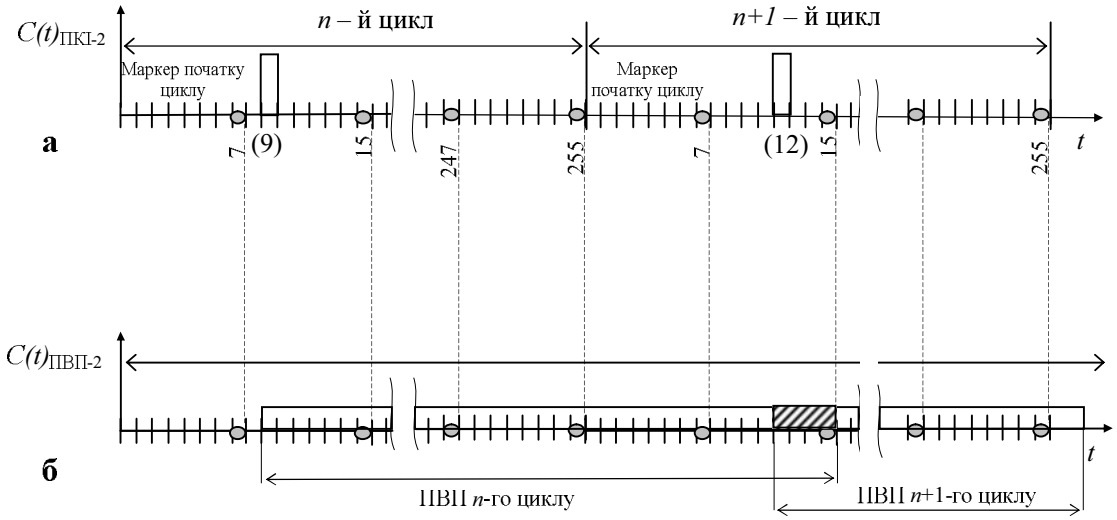


Рис. 3. Перетворення позиційних код-імпульсних сигналів у ПВП на прикладі другого каналу:
а - два цикли ПКІ сигналів;
б - ПВП сигнали другого каналу, які частково накладаються один з одним.

Адитивна суміш таких ПВП після модуляції утворює груповий сигнал, який передається каналом зв'язку. Структура групового сигналу такої складної форми утворює суміш, яка подібна білому шуму і заважає виявити та декодувати її у випадку перехоплення .

Загальна енергія всіх субімпульсів такої ПВП $E_{\text{ПВП}}$ дорівнює енергії перетвореного ПКІ $E_{\text{ПКІ}}$, а тривалість кожного $j$-го субімпульсу послідовності дорівнює тривалості ПКІ:

$$E_{\text{ПВП}} = E_{\text{ПКІ}};\ \tau_{\text{ЛПВП}} = \tau_{\text{ПКІ}}. \tag{7}$$

Умову рівності енергій можна легко забезпечити, якщо потужність кожного субімпульсу ортогональної ПВП $P_{\text{ПВП}}$ прийняти у $D$ разів меншою, ніж потужність ПКІ, де $D$ - значення бази послідовності:

$$P_{\text{ПВП}} = \frac{P_{\text{ПКІ}}}{D}. \tag{8}$$

При дотриманні умов (2) і (8) розроблений метод перетворення ІКМ-сигналів може бути використаний на телекомунікаційних трактах зі стандартними значеннями смуги частот та швидкості стандарту Е1.

Недоліком запропонованого методу є збільшення складності обладнання приймального та передавального трактів. Проте розвиток елементної бази робить цей недолік несуттєвим.

Для оцінки ефективності [9] розробленого методу було створено імітаційну модель в середовищі програмування *MatLab*. Результати моделювання показали, що при використанні ПВП, які повністю ортогональні між собою, енергетична ефективність системи передачі інформації підвищується в 2,2 рази, порівняно зі стандартною ІКМ-системою. При використанні реальних ПВП (які не є повністю ортогональними) енергетичний виграш складає близько 15-20%.

**Висновки.** Таким чином, використання розробленого методу підвищує енергетичну ефективність при передачі сигналів в інформаційно-телекомунікаційних системах спеціального призначення, що в свою чергу дозволяє покращити прихованість та завадозахищеність, а значить, й інформаційну безпеку взагалі. Перевагою отриманої внаслідок запропонованих перетворень структури сигналу є, також, набуття властивостей шумоподібності, що, в свою чергу, підвищує прихованість передачі інформації. Така малопотужна шумоподібна суміш групового сигналу може передаватися, не створюючи завад сусіднім радіоелектронним засобам, які працюють в тому ж діапазоні частот. При цьому, також, ускладнюється розкриття факту передачі засобами радіотехнічної розвідки.

Отже, розроблений у статті метод забезпечує наступні переваги для інформаційно-телекомунікаційної системи:

- зниження щільності випромінювання електромагнітної енергії, завдяки чому відбувається покращення електромагнітної сумісності телекомунікаційних засобів;
- підвищення енергетичної прихованості;
- підвищення структурної та інформаційної прихованості завдяки використанню складних шумоподібних сигналів.

## ЛІТЕРАТУРА


1. Сташук О.В. Цілісність інформації в інформаційно-телекомунікаційних системах спеціального призначення: загрози та методи захисту / О.В. Сташук, М.М. Браіловський, О.В. Труш // Збірник наукових праць ВІТІ НТУУ „КПІ". - 2010. - Вип. 1. - С. 32-36.
2. Скляр Б. Цифровая связь. Теоретические основы и практическое применение / Б. Скляр - Изд 2-е. - М.: Вильямс, 2003. - 1104 с.
3. Прокис Дж. Цифровая связь: пер. с англ. / Дж. Прокис; под ред. Д.Д. Кловского. - М.: Радио и связь, 2000. - 797 с.
4. Варакин Л.Е. Теория систем сигналов / Л.Е. Варакин. - М.: Советское радио, 1978. - 304 с.
5. Пат. № 42417А Україна, МПК 7 Н 03 К 5/00. Спосіб аналого-цифрового перетворення електричних сигналів і позиційний код-імпульсний аналого-цифровий перетворювач електричних сигналів; Сташук О. В., Сташук Л. Д., Сташук В. Д. - Промислова власність, 2001, бюл. № 9, від 15.10.2001р.
6. Пат. № 5071 Україна, МПК 7 G 06 F 1/00. Кодоперетворювач ІКМ-сигналів у позиційні код-імпульсні сигнали; Сташук О.В., Сташук Л.Д., Сташук В.Д. - Промислова власність, 2005, від 15.02.2005р.
7. Теплов Н.Л. Теория передачи сигналов по электрическим каналам связи / Н.Л. Теплов. - М.: Воениздат, 1976 - 424 с.
8. Волков Л.Н. Системы цифровой радиосвязи: базовые методы и характеристики: учеб. пособ. / Волков Л.Н., Немировский М.С., Шинаков Ю.С. - М.: Эко-Трендз, 2005. - 392 с.
9. Толюпа С.В., Лівенцев С.П., Браун В.О., Жиров Б.Г. Оцінка ефективності систем захисту інформації в інформаційно-телекомунікаційних системах // Вісник Київського національного університету ім. Тараса Шевченка. Військово-спеціальні науки. - 2007. - № 15. - С. 86-89.



Надійшла: 10.01.2012

Рецензент: д.т.н., проф. Корнійчук М.Т.