

УДК 004.056

МЕТОДИ ПІДВИЩЕННЯ ПРИХОВАНOSTІ ПЕРЕДАВАННЯ ІНФОРМАЦІЇ НА ОСНОВІ РОЗШИРЕННЯ СПЕКТРА ТАЙМЕРНИХ СИГНАЛІВ

DOI 10 36994 / 2788- 5518- 2022-02-04-02

Корчинський В.В., д.т.н., проф. Державний університет інтелектуальних технологій і зв'язку, Одеса, Україна. vkadkorchin@ukr.net

Назаренко О.А., к.ф.-м.н, доц. Державний університет інтелектуальних технологій і зв'язку, Одеса, Україна. duitz.od@gmail.com

Степанов В.О. Військова Академія, Одеса, Україна. stepanovvadym333@gmail.com

Аль-Файюми Халед. Державний університет інтелектуальних технологій і зв'язку, Одеса, Україна. khaled@alfaiomi.com

Анотація: У статті розглянуто методи розширення спектра таймерних сигнальних конструкцій. Для систем радіозв'язку, що працюють в умовах радіоелектронного конфлікту, пропонується використовувати шумоподібні таймерні сигнали. Це дозволяє підвищити інформаційну, структурну та енергетичну прихованість сигнальних конструкцій. Проведено аналіз властивостей таймерних сигнальних конструкцій, що дає змогу виявити певні переваги непозиційних сигналів перед позиційними. Структурна прихованість таймерних сигналів залежить від параметрів пристрою кодування. Також таймерні сигнали можна використовувати як завадостійкий код, для якого не потрібні додаткові перевірочні елементи. За рахунок зміни параметрів побудови таймерних сигналів існує можливість змінювати коригувальну здатність коду, а також формувати різні ансамблі сигнальних конструкцій. Це потенційно збільшує структурну та інформаційну прихованість таймерних сигналів.

Енергетична прихованість досягається за допомогою різних методів розширення спектра бінарного сигналу: псевдовипадкового перескоку робочої частоти; прямого розширення спектра псевдовипадковими послідовностями; лінійної частотної модуляції. Однак розвиток радіотехнічних засобів перехоплення широкосмугових сигналів потребує також ускладнення структури сигнальних конструкцій. Використання таймерних сигналів дає можливість синтезувати більш складні шумоподібні сигнальні конструкції. Це дозволить підвищити структурну прихованість та ускладнить розкриття структури сигналу засобами радіотехнічної розвідки супротивника. Таким чином, обґрунтованим є розробка та вдосконалення методів розширення спектра таймерних сигналів. Однак методи розширення спектра сигналів розроблялися виключно для позиційних кодів, тому не можуть бути застосовані до таймерних непозиційних сигналів. Наукові роботи, які присвячені дослідженню шумоподібних таймерних сигналів, не повною мірою висвітлюють алгоритми перетворення вузькосмугового сигналу на широкосмуговий. Це стало приводом для подальшого дослідження в цьому напрямку, тому метою цієї роботи є синтез шумоподібних таймерних сигнальних конструкцій.

Ключові слова: прихованість, розширення спектра, шумоподібні сигнали, захист інформації, модуляція, спектр.

METHODS OF INCREASING SECRECY OF INFORMATION TRANSMISSION BASED ON EXPANDING THE SPECTRUM OF TIMER SIGNALS

Vladimir Korchynskyi, Dr. habil., Prof. State University of Intellectual Technologies and Communication, Odessa, Ukraine. vkadkorchin@ukr.net

Olexander Nazarenko, Ph.D., Ass..Prof. State University of Intellectual Technologies and Communication, Odessa, Ukraine. duitz.od@gmail.com

Vadim Stepanov. Military Academy, Odessa, Ukraine. stepanovvadym333@gmail.com

Khaled Alfaion. State University of Intellectual Technologies and Communications, Odessa, Ukraine. khaled@alfaiomi.com

Abstract: The article considers methods of expanding the spectrum of timer signal constructions. For radio communication systems operating in conditions of electronic conflict, it is proposed to use noise-like timer signals. This will increase the information, structural and energy secrecy of signal constructions. The analysis of the properties of timer signal constructions was carried out, which made it possible to identify certain advantages of such non-positional signals over positional ones. It has been established that the information capacity of timer signals is greater than bit-digital code. The structural secrecy of timer signals depends on the parameters of the encoder. Also, such signals can be used as an error-correcting code, which doesn't require additional check elements. By changing the parameters of contracting timer signals, it is possible to change the corrective ability of the code, as well as to form different ensembles of signal constructions. This potentially increases the structural and informational secrecy of timer signals.

Energy secrecy is achieved by using various methods of expanding the spectrum of binary signal: random jumping of the operating frequency; direct spectrum extension by random sequences; linear frequency modulation. However, the development of radio engineering means for intercepting broadband signals also requires the complication structure of signal constructions. The use of timer signals makes it possible to form more complex noise-like signal constructions. This will increase structural secrecy and complicate the disclosure of the signal structure by means of enemy electronic intelligence. Thus, it is justified to develop and improve methods for expanding the spectrum of timer signals. However, signal spreading methods were developed exclusively for positional codes, and therefore cannot be applied to non-positional timer signals. Scientific articles devoted to the research of noise-like timer signals don't fully cover the algorithms for converting narrowband signal into wideband one. This was the reason for further research in this direction, so the aim of this article is the synthesis of noise-like timer signal constructions.

Key words: secrecy, spectrum spreading, noise-like signals, information security, modulation, spectrum.

Вступ

Підвищення завадозахищеності систем радіозв'язку [1,2] є пріоритетним напрямом по захисту передаваної інформації від несанкціонованого доступу (НСД). Завадозахищеність [2] є комплексним показником, за допомогою якого оцінюється ефективність конфіденційної системи радіозв'язку. Основними показниками завадозахищеності є: завадостійкість і прихованість. Розрізняють різні види прихованості: енергетична, структурна, інформаційна, просторова та інші.

Ускладнення структури сигналу дозволяє вирішити ряд завдань по забезпеченню прихованості сигнальних конструкцій у випадку перехоплення сеансу радіозв'язку засобами радіотехнічної розвідки противника. В сучасних завадозахищених системах радіозв'язку прихованість передавання забезпечується за рахунок застосування шумоподібних сигналів [1,2]. Для цієї задачі використовуються різні методи розширення спектра сигналу: псевдовипадковий перескок робочої частоти; пряме розширення спектра за допомогою псевдовипадкових послідовностей (ППРЧ); лінійна частотна модуляція (ЛЧМ) [7]. Відомо [1,2], що теоретичною основою для формування шумоподібних сигналів є процес розширення спектра бінарної послідовності. Подальший розвиток теорії шумоподібних сигналів орієнтований на застосування таймерних сигнальних конструкцій (ТСК) [3-6], які є непоозиційними. Процес формування шумоподібних ТСК потребує іншого алгоритму, тому що існуючі методи розширення спектра здебільшого орієнтовані на позиційні сигнали. Обґрунтованість застосування шумоподібних таймерних сигналів пояснюється необхідністю ускладнення структури сигнальних конструкцій для завдання підвищення інформаційної та структурної прихованості [3-6].

Таким чином, можна відзначити, що застосування шумоподібних таймерних сигналів є пріоритетним дослідженням для завдання підвищення завадостійкості передаваної конфіденційної інформації в каналах радіозв'язку [1]. Особливість застосування таймерних сигналів полягає в тому, що вони відносяться до класу непоозиційних сигнальних конструкцій та мають ряд переваг в порівнянні з позиційними, а також деякі недоліки. На основі таймерних сигналів можна реалізувати завадостійке кодування без додаткових перевірочних елементів. Зміна параметрів пристрою кодування ТСК дозволяє формувати різні ансамблі сигнальних конструкцій [8,9]. Такі властивості ТСК дозволяють вирішувати завдання по збільшенню інформаційної та структурної прихованості. Метою даної роботи є синтез шумоподібних таймерних сигнальних конструкцій на основі методів ППРЧ.

Виконання досліджень

В умовах радіоелектронного конфлікту [1,2] найчастіше в системах радіозв'язку застосовується метод розширення спектра інформаційного вузькосмугового сигналу на основі ППРЧ [2]. Пояснюється це можливістю забезпечення для передаваного сигналу певної енергетичної прихованості, яка досягається за рахунок зміни частоти носійного коливання для одного або кількох біт у заданому достатньо великому діапазоні частот. Закон зміни передаваної частоти носійного коливання відомий тільки передавачеві та приймачеві, та може змінюватися від одного сеансу передачі до іншого. Перехоплення такого сигналу без знання цього закону зміни частот може бути лише за допомогою широкодіапазонного сканера приймача противника, що не завжди може бути успішним при великій кількості працюючих радіостанцій з ППРЧ. Існує кілька варіантів розширення спектра за допомогою ППРЧ. В залежності від кількості біт, що передаються на одній частоті розрізняють швидку і повільну ППРЧ [2].

При швидкій ППРЧ тривалість передавання одного інформаційного елемента t_0 розрядно-цифрового коду на одній частоті може бути:

$$t_{\text{пер}} \leq t_0. \quad (1)$$

При повільній ппрч на одній частоті $\Delta f_{\text{прч}}$ передається кілька біт, тобто:

$$t_{\text{пер}} > t_0. \quad (2)$$

Розглянемо можливість розширення спектра таймерного сигналу [3] з урахуванням особливостей його побудови. Таймерний сигнал є непозиційним, і базовим часовим елементом для його побудови є інтервал часу Δ . Далі задається інтервал побудови ТСК:

$$T_c = n t_0, \quad (3)$$

де n – кількість елементів Найквіста t_0 .

В часових границях сигнальної конструкції T_c тривалість імпульсів :

$$t_c = t_0 + \Delta \times l, \quad (4)$$

де $l \in 0, 1, 2, 3, \dots$ і кратне $\Delta = t_0/s$ ($s \in 2, 3, \dots k$).

Відстань між значущими моментами модуляції (ЗММ) ($t_c \geq t_0$) не менша за інтервал Найквіста ($t_0 = 1/\Delta F_c$) і кратна елементу Δ . Така умова дозволяє усунути міжсимвольні спотворення в ТСК. Число s показує, наскільки менше часовий інтервал Δ по відношенню до t_0 . Число переходів i в ТСК може бути різним і змінюватися в межах $i = 1, 2, \dots, n-1$.

На рис. 1 (а) надана часова діаграма реалізації ТСК на інтервалі $T_c = 4t_0$.

Як бачимо, тривалість імпульсу ТСК t_c може бути більше t_0 , тому застосувати умову (1) або (2) для розширення спектра таймерних сигналів за допомогою швидкої або повільної ППРЧ не є можливим. Тобто, основною проблемою для цього є непозиційність ЗММ в ТСК по відношенню до інтервалу Найквіста t_0 .

Розширення спектра ТСК за допомогою методу швидкої ППРЧ

Розглянемо випадок, коли тривалість передавання на частоті носійного коливання $t_{\text{пер}} < t_0$ та $t_{\text{пер}} \leq \Delta$. Це дає можливість реалізувати швидку ППРЧ, використовуючи інтервал Δ для передачі однієї або кількох частот. Для реалізації цього методу запропоновано спочатку виконати пряме розширення спектра ТСК за допомогою псевдовипадкової послідовності $c(T_c)$ (рис. 1 б) з тривалістю імпульсу τ .

Спектр ТСК $\chi_{\text{тск}}(t_c)$ розширюється за допомогою елементів :

$$\tau = \Delta / j \quad (5)$$

де $j = 1, 2, 3, \dots$ – кількість елементів τ на інтервалі Δ .

Перетворення ТСК за допомогою псевдовипадкової послідовності $c(T_c)$ (рис. 1 (б)) в широкополосний сигнал (рис. 1 (в)) відбувається за наступною формулою:

$$\chi_{\text{скк}}(T_c) = \chi_{\text{тск}}(t_c) \times c(T_c). \quad (6)$$

Далі відбувається розширення спектра вже широкосмугового ТСК $\chi_{\text{СКК}}(T_c)$ за допомогою швидкої ППРЧ (рис. 1 (г)):

$$u'(t) = \chi_{\text{СКК}}(T_c) U_0 \cos(\omega(g(t)t)), \quad (7)$$

де $\cos(\omega(g(t)t))$ – набір частот, який являє собою функцію від кодового сигналу $g(t)$.

Розширення спектра ТСК за допомогою методу повільної ППРЧ

Для методу повільної ППРЧ при розширенні спектра бітів розрядно-цифрового коду швидкість зміни частоти носійного коливання більше в кілька разів інтервалу Найквіста t_0 . В таймерних сигналах $\Delta < t_0$, тому час зміни частоти носійного коливання $T_{\text{МППРЧ}}$ для повільної ППРЧ буде визначатися з урахуванням елемента Δ , тобто:

$$T_{\text{МППРЧ}} = \Delta z, \quad (8)$$

де $z = 2, 3, \dots, M$ – кількість елементів Δ на інтервалі $T_{\text{МППРЧ}}$; $M = ns$.

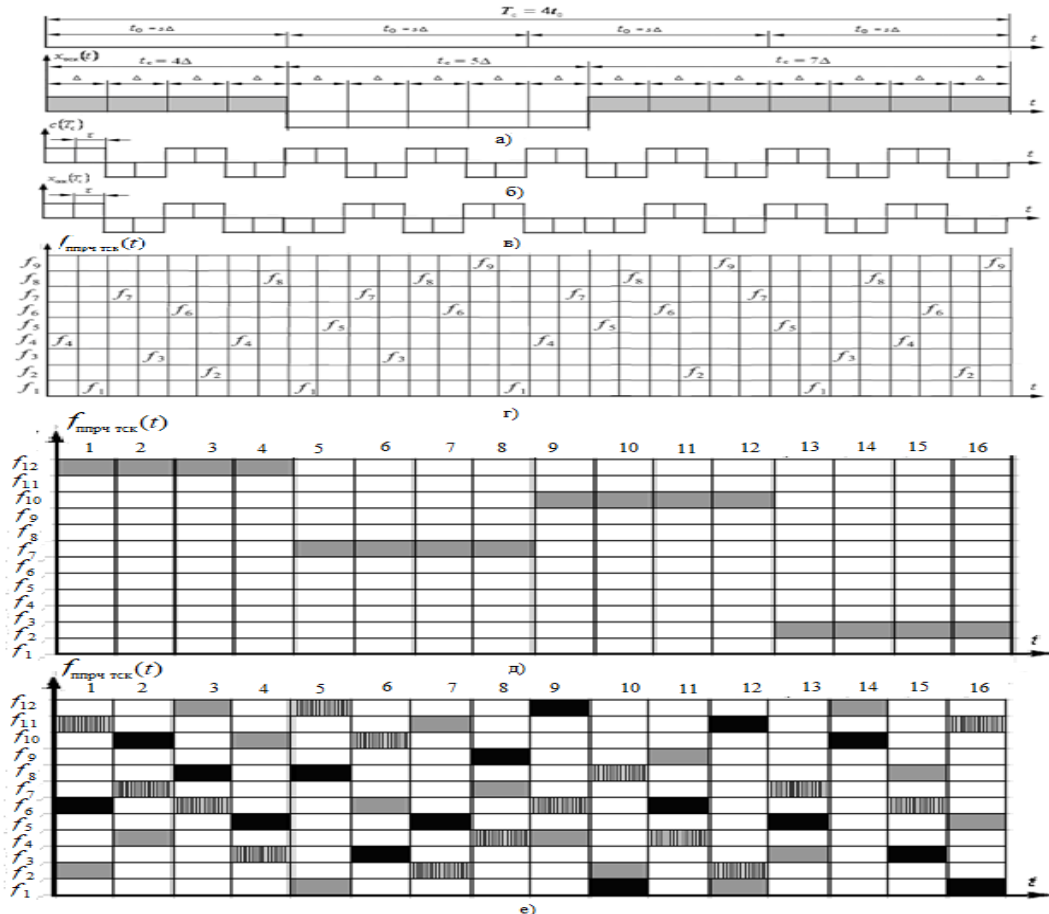


Рис 1. Розширення спектра ТСК $\chi_{\text{ТСК}}(t_c)$ за допомогою ПВП (в), методами швидкої (г) та повільної (д)

ППРЧ, багатоканальної ППРЧ (е) на інтервалі $T_c = 4t_0$

При виборі часового інтервалу зміни частоти носійного коливання слід брати до уваги, що при збільшенні значення $T_{\text{МППРЧ}}$ ймовірність ураження завадою сигналу в радіоканалі підвищується. На рис. 2 (д) надано процес розширення спектра методом повільної ППРЧ з

інтервалом $T_{\text{МППРЧ}} = 4\Delta$, де $z = 4$. Якщо $z = M$, тоді зміна частоти носійного коливання відбуватиметься на інтервалі:

$$T_{\text{МППРЧ}} = T_c, \quad (9)$$

тобто для кожної сигнальної конструкції. За умови (9) кожна таймерна сигнальна конструкція передається на певній частоті носійного коливання.

Вочевидь, що для визначення значущих моментів відновлення (ЗМВ) фронтів ТСК [3] на приймальній стороні необхідно в передавачі після прямого розширення спектра використовувати попередню маніпуляцію елементів Δ або τ (за умови, що $\tau \neq \Delta$), наприклад, ФМ-2, ФМ-4 або КАМ-4. Так при ФМ-4 або КАМ-4 (квадратурна-амплітудна модуляція) можна забезпечити збільшення швидкості передавання інформації за рахунок того, що на одну сигнальну конструкцію аналогового сигналу передаються два елементи Δ в порівнянні з ФМ-2. Застосування більш складних видів модуляції для підвищення швидкості передавання інформації, наприклад, КАМ-8 або КАМ-16, призведе до зниження завадостійкості системи радіозв'язку.

Для методу швидкої ППРЧ (рис. 2 (в)) часовий інтервал несучої частоти $T_{\text{БППРЧ}}$ збігається або менше елемента Δ :

$$T_{\text{БППРЧ}} \leq \Delta. \quad (10)$$

Слід зазначити, що метод швидкої ППРЧ більш стійкий до завад. У разі впливу вузькосмугової завади, яка спотворює сигнал в певному підканалі, не відбувається повного спотворення сигнальної конструкції, так як рівень імпульсу в межах $t_c = t_0 + k\Delta$ повторюється по Δ кілька разів на різних частотних підканалах. Як правило, таке спотворення призводить до дроблення одного або декількох імпульсів ТСК, що виявляється приймачем при демодуляції.

При повільній ППРЧ вплив вузькосмугової завади може привести до суттєвого спотворення структури таймерного сигналу, що ускладнює процес його відновлення на приймальній стороні. Однак цей метод простіший в реалізації, ніж метод швидкої ППРЧ.

Розширення спектра ТСК за допомогою методу багатоканальної швидкої ППРЧ

На рис. 1 (е) надано метод багатоканальної швидкої ППРЧ на основі ТСК. За рахунок передавання одного елемента Δ на різних частотах носійного коливання f_i цей метод дозволяє підвищити стійкість системи радіозв'язку до завад. Використання непарного числа підканалів f_i , наприклад, $w = 3$ (рис. 1 г), дозволить реалізувати оцінку якості прийнятого елемента Δ за мажоритарним принципом, що суттєво підвищить завадостійкість системи радіозв'язку. При цьому остаточне рішення про стан прийнятої ТСК буде здійснюватися шляхом визначення приналежності її до підмножини дозволених та недозволених сигнальних конструкцій.

На рис. 2 надано структурну схему завадозахищеної системи зв'язку з шумоподібними таймерними сигналами. Джерело повідомлення (ДП) видає на пристрій завадостійкого кодування (ПЗК) розрядно-цифрового коду інформаційну двійкову послідовність k . ПЗК виконує завадостійке кодування та добавляє до інформаційної послідовності перевірочні символи r , тобто загальна довжина комбінації [3]:

$$n = k + r. \quad (11)$$

З виходу ПЗК елементи РЦК поступають на кодер таймерних сигналів (КДТСК). Сформовані ТСК з виходу КДТСК подаються на помножувач, де відбувається розширення спектра таймерних сигналів за допомогою псевдовипадкових послідовностей, наприклад Уолша. Далі в пристрої $M_{\text{ФМ}}$ відбувається фазова маніпуляція елементів розширеної послідовності. Помножувач $\boxtimes$ за допомогою частот носійного коливання, що формуються синтезатором робочих частот, переносяться в спектр високих частот.

Таким чином, процес розширення спектра відбувається за рахунок двох методів: прямого розширення спектра та швидкої ППРЧ. Генератор ключів служить для формування параметрів

таймерних сигналів та закону генерування псевдовипадкових послідовностей синтезатора робочих частот. Робота генератора ключів відбувається за допомогою вхідних параметрів.

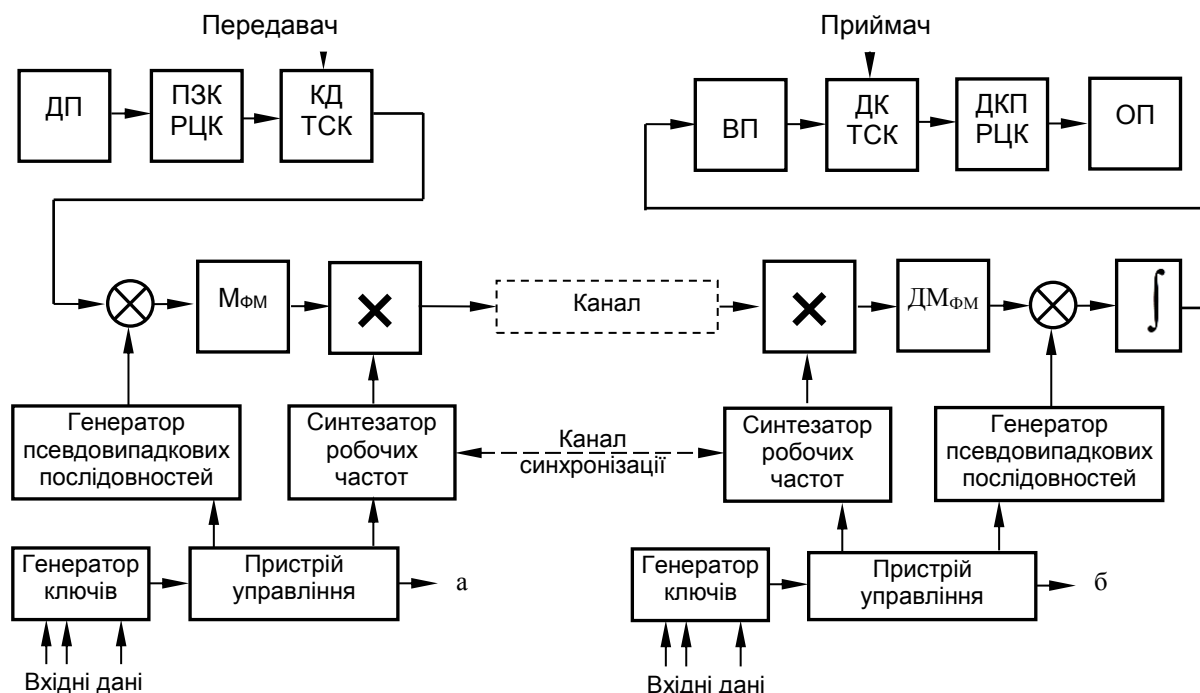


Рис. 2. Структурна схема завадозахищеної системи зв'язку з ТСК та ППРЧ: ДП – джерело повідомлення; ПЗК – пристрій завадостійкого кодування РЦК; КД – пристрій кодування ТСК; МФМ – фазовий маніпулятор; ДМФМ – демодулятор фазових сигналів; $\times$ – помножувач; $\int$ – інтегратор; ВП – вирішальний пристрій

Висновки

1. Запропонований метод формування шумоподібних сигналів на основі непозиційних таймерних сигнальних конструкцій вимагає застосування двох етапів розширення спектра, що дозволяє вирішити ряд завдань з підвищення прихованості та завадостійкості.

2. На першому етапі пропонується пряме розширення спектра ТСК з маніпуляцією елементів псевдовипадкової послідовності, що підвищує структурну прихованість сигнальних конструкцій, а також вирішує проблему визначення ЗМВ в приймачі.

3. На другому етапі використовується один із розглянутих методів ППРЧ, при цьому перенос спектра в область високих частот відбувається для одного або кількох елементів розширення псевдовипадкової послідовності. Також можливий варіант застосування швидкої ППРЧ за умови, коли тривалість передавання частоти носійного колювання менше за елемент розширення псевдовипадкової послідовності.

4. Застосування двох етапів розширення спектра ТСК потребує ускладнення системи радіозв'язку, в якій потрібно застосовувати додаткові пристрої: в передатчику – це пристрій прямого розширення спектра, а в приймачі – пристрій кореляційного прийому.

Література

1. Куприянов А.И., Захаров А.В. Теоретические основы радиоэлектронной борьбы. М.: Вузовская книга, 2007. 356 с.
2. Борисов В.И., Зинчук В.М., Лимарев А.Е. Помехозащищенность систем радиосвязи с расширением спектра сигналов методом псевдослучайной перестройки рабочей частоты, под ред. Борисова В.М.. М.: Радио и связь, 2000. 384 с.
3. Захарченко В.М. Синтез багатопозиційних часових кодів. Київ: Техніка, 2012. 284 с.
4. Zakharchenko N. Information security of Time-Controlled Signals in Confidential Communication Systems / N. Zakharchenko, V. Korchinsky, B. Radzimovsky // Modern problems of radio engineering, telecommunications and computer science: XI International Conference TCSET 2012, (Lviv-Slavske, 21-24 february 2012) – Lviv; Publishing House of Lviv Polytechnic, 2012. С. 317.
5. Zakharchenko M. Integrated methods of information security in telecommunication systems / Zakharchenko M.,

Korchynskii V., Kildishev V. 2017 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo'2017), IEEE Xplore Digital Library. 11 – 15 September 2017. – V. 1. – pp. 78–81. URL: <http://ieeexplore.ieee.org/document/8095366/>.

6. Skopa O. Korchinsky. V. Management of Relative Effective Transmission Rate in Packet Switching Networks . Proceedings of the International Conference TCSET'2002, February 18-23, 2002 Lviv-Slavsko, Ukraine, 2 p.

7. Volodymyr Korchynskiy, Matin Hadzhyiev, Pavlo Pozdniakov, Vitalii Kildishev, Valeriy Hordiichuk Development of the procedure for forming non-stationary signal structures based on multicomponent LFM signals . *Eastern-European Journal of Enterprise Technologies / Information and controlling system*.2018. №6/9(96). Vol 6.pp.. 29-37.

8. Korchynskiy V. V., Kildishev V. I., Holey D.V., Berdnikov O. M. Increasing the secrecy of transmission information based on combined random coding // National University «Zaporizhzhia Polytechnic» Radio Electronics, Computer Science, Control The scientific journal, 2019. № 3(50). pp. 108-116.

9. V Hordiichuk, A Shyshatskyi2, V Korchinskyi, Timing pulse code modulation as a tool for quantization noise reduction in special-purpose IT systems 1, *Journal of Physics: Conference Series* .2021. ICOLSSTEM 2020 IOP Publishing.

References

1. Kupriyanov A.I. , Sakharov A. V. Teoreticheskie osnovy radio`elektronnoj bor'by.[Theoretical foundations of electronic warfare]. M.: University book, 2007. 356 p.

2. Borisov V.I. Zinchuk V.M., Limarev A.E. Pomehozaschischennost' sistem radiosvyazi s rasshireniem spektra signalov metodom psevdosluchajnoj perestrojki rabochej chastoty , pod red. Borisova V.M.[_Noise Immunity of Radio Communication Systems with Signal Spectrum Spreading by the Method of Pseudo-Random Frequency Tuning]. M.: Radio i svyaz', 2000. 384 p.

3. Zakharchenko V.M. Sintez bagatopozitsijnih chasovih kodiv. [Synthesis of rich positional clock codes] Kyiv: Technique, 2012. 284 p.

4. Zakharchenko N. Information security of Time-Controlled Signals in Confidential Communication Systems / N. Zakharchenko, V. Korchinsky, B. Radzimovsky // Modern problems of radio engineering, telecommunications and computer science: XI International Conference TCSET 2012, (Lviv-Slavsko, 21-24 february 2012) – Lviv; Publishing House of Lviv Polytechnic, 2012. C. 317.

5. Zakharchenko M. Integrated methods of information security in telecommunication systems / Zakharchenko M., Korchynskii V., Kildishev V. 2017 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo'2017), IEEE Xplore Digital Library. 11 – 15 September 2017. – V. 1. – pp. 78–81. URL: <http://ieeexplore.ieee.org/document/8095366/>.

6. Skopa O. Korchinsky. V. Management of Relative Effective Transmission Rate in Packet Switching Networks . Proceedings of the International Conference TCSET'2002, February 18-23, 2002 Lviv-Slavsko, Ukraine, 2 p.

7. Volodymyr Korchynskiy, Matin Hadzhyiev, Pavlo Pozdniakov, Vitalii Kildishev, Valeriy Hordiichuk Development of the procedure for forming non-stationary signal structures based on multicomponent LFM signals . *Eastern-European Journal of Enterprise Technologies / Information and controlling system*.2018. №6/9(96). Vol 6.pp.. 29-37.

8. Korchynskiy V. V., Kildishev V. I., Holey D.V., Berdnikov O. M. Increasing the secrecy of transmission information based on combined random coding // National University «Zaporizhzhia Polytechnic» Radio Electronics, Computer Science, Control The scientific journal, 2019. № 3(50). pp. 108-116.

9. V Hordiichuk, A Shyshatskyi2, V Korchinskyi, Timing pulse code modulation as a tool for quantization noise reduction in special-purpose IT systems 1, *Journal of Physics: Conference Series* .2021. ICOLSSTEM 2020 IOP Publishing.