УДК 621.391 DOI: 10.30748/soivt.2018.56.06

С.В. Озеров, О.В. Коваль, Ю.О. Котик, С.О. Гарвардт, Є.В. Марченко

Харківський національний університет Повітряних Сил ім. І.Кожедуба, Харків

АНАЛІЗ МОЖЛИВОСТІ ЗАСТОСУВАННЯ ХАОТИЧНИХ ПРОЦЕСІВ ДЛЯ ПІДВИЩЕННЯ СКРИТНОСТІ СЕНСОРНИХ МЕРЕЖ ТАКТИЧНОЇ ЛАНКИ УПРАВЛІННЯ ВІЙСЬКАМИ

В статті досліджено можливість застосування хаотичних коливань (сигналів) в якості інформаційного сигналу під час організації радіоканалу передачі даних в бездротових сенсорних мережах тактичної ланки. Розглянуто принципи побудови та функціонування бездротових сенсорних мереж. За допомогою аналізу статистичних характеристик хаотичних процесів здійснено оцінку їх скритності (у порівнянні з білим шумом) Надані пропозиції та рекомендації щодо підвищення скритності радіоканалу передачі даних в бездротових сенсорних мережах.

Ключові слова: *бездротова сенсорна мережа, незаконні збройні формування, хаотичний процес, скритність, передача даних, нелінійний аналіз спостережень, кореляційний аналіз.*

Вступ

Постановка проблеми. Досвід проведення Операції об'єднаних сил свідчить про те, що одним з вирішальних факторів успішного виконання бойових завдань є своєчасне забезпечення військ (сил) актуальною розвідувальною інформацією [1]. Одним із шляхів забезпечення збору розвідувальної інформації в режимі реального часу є застосування бездротових сенсорних мереж що розгортаються безпосередньо на лінії зіткнення.

Бездротові сенсорні мережі (Wireless Sensor Network) – це мережі, що складаються з сукупності датчиків з функціями збору, обробки та передачі даних щодо стану навколишнього середовища [2] Передача даних здійснюється за допомогою технології IEEE 802.11n (в якості несучих застосовуються широкосмугові гармонічні сигнали з різними видами модуляції). Проте, наявність у противника сучасних засобів радіоелектронної боротьби, ставить під сумнів завадозахищеність бездротових мереж: дані типи сигналів не відповідають вимогам скритності в повній мірі, тому що вони відрізняються від шуму спостереження при кореляційному, спектральному та нелінійному аналізі. Саме тому існує суттєва небезпека, що противник розкриє факт функціонування бездротової сенсорної мережі збору розвідувальної інформації, що в свою чергу може призвести до здійснення деструктивних дій з боку противника на радіоканали передачі даних. Під основою деструктивних дій на систему управління слід розуміти застосування засобів радіоелектронної розвідки та радіоелектронного подавлення [3].

Аналіз останніх досліджень і публікацій. [4–5] показує, що одним з перспективних підходів підвищення скритності каналів передачі даних в бездротових сенсорних мережах є застосування хаотичних процесів, що за своїми статистичними та динамічними характеристиками подібні до шуму спостереження.

Таким чином, **метою роботи** є обґрунтування можливості застосування хаотичних процесів для підвищення скритності радіоканалу передачі даних в бездротових сенсорних мережах під час виконання завдань по збору розвідувальної інформації.

Виклад основного матеріалу

Основний принцип функціонування бездротових сенсорних мереж полягає у використанні великої кількості різнорангових радіосенсорів, що розташовуються на визначеній ділянці місцевості для спостереження за визначеними об'єктами або для збору визначених параметрів оточуючого середовища. Зібрана інформація передається на спеціальні шлюзи шляхом ретрансляції через проміжні сенсорні вузли [2].

З початком активних бойових дій в Донецький та Луганських областей, ЗС України розпочали застосування бездротових сенсорних мереж для збору розвідувальної інформації з метою більш ефективного виконання бойових завдань. Це призвело до значного збільшення успішності бойових операцій і дозволило знищити значну кількість сил і засобів сепаратистів. Однак, на теперішній час почастішали випадки порушення коректного функціонування тактичних сенсорних бездротових мереж з боку незаконних збройних формувань (в склад яких входять штатні підрозділи РЕБ Збройних Сил Російської Федерації).

Головною причиною даного явища є застосування з боку незаконних збройних формувань спеціальних засобів моніторингу частотного діапазону,

створення інформаційних перешкод – тобто застосування засобів радіоелектронної боротьби.

В цілому, підрозділи РЕБ противника мають на озброєнні сучасні засоби радіоелектронної боротьби російського виробництва, що дозволяють здійснювати ефективну розвідку та подавлення радіо систем, зокрема бездротових сенсорних мереж. Найбільшої уваги заслуговують комплекс РЕБ “Інфауна” (рис. 1) та комплекс РЕБ “Леєр-2” (рис. 2).

Рис. 1. Комплекс РЕБ Інфауна

Рис. 2. Комплекс РЕБ Леєр-2

Дані комплекси характеризуються наступними можливостями:

– автоматизоване проведення пошуку, виявлення, розкриття структури радіосигналів;

– постановка перешкод радіоелектронним засобам;

– відтворення виявлених радіосигналів;

– визначення всіх характеристик управляючого каналу.

Сигнали, сформовані за допомогою гармонійних коливань, є особливо вразливими для даних комплексів (за рахунок їх недостатньої розвідзахищеності), тому для підвищення стійкості радіоканалу передачі даних доцільно в якості несучого сигналу застосовувати складні шумоподібні сигнали. В контексті дослідження слід зазначити, що до основних переваг систем радіозв’язку з шумоподібними сигналами слід віднести [6]:

– ефективне функціонування приймальних пристроїв в умовах багатопроменевого поширення сигналу;

– висока завадостійкість до вузькосмугових перешкод;

– краще використання спектра частот на обмеженій території;

– можливість частотно-кодового поділу абонентів, що дає можливість уникнути колізій при адресації інформації в разі застосування декількох незалежних кластерів сенсорних мереж одночасно;

– забезпечення електромагнітної сумісності з вузькосмуговими системами радіозв'язку;

– підвищена скритність.

Для побудови сигнально-кодових конструкцій шумоподібних сигналів використовуються:

– багатопозиційні сигнально-кодові конструкції;

– згорткове кодування, фрактальне кодування;

– технологія об'єднання гребінчастих спектрів; псевдовипадкові методи формування ансамблів;

– хаотичні послідовності (процеси) та коди Лемера.

В контексті роботи перейдемо до розгляду та детального аналізу хаотичних процесів.

Успішною альтернативою гармонійним коливанням є динамічний хаос [4], – явище в теорії динамічних систем, при якому поведінка нелінійної системи виглядає випадковою, незважаючи на те, що вона визначається детерміністичними законами. При цьому важливу особливість алгоритмів, що описують систему з динамічним хаосом, є їх нелінійність, а особливістю часової реалізації процесу – його неперіодичність і можливість багаторазового його формування, що вигідно відрізняє хаотичний процес від випадкового.

Хаотичними процесами [4] називають складні коливання, що генеруються нелінійними динамічними системами. Вказані процеси володіють характеристиками що властиві стохастичним процесам: рівномірний амплітудно-частотний спектр і кореляційну функцію що являє собою дельта-функцію [7]. Для більш наглядного аналізу проведемо порівняння

деяких статистичних характеристик хаотичного процесу з характеристиками білого шуму.

На рис. 3 наведені часові реалізації хаотичного процесу, що сформований за допомогою поліному Чебишева та білого шуму.

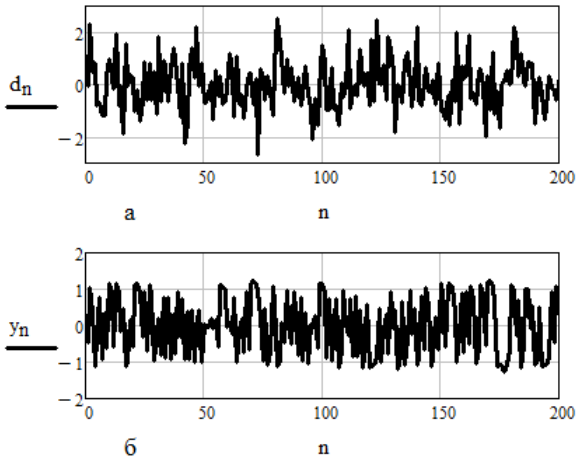

Рис. 3. Часова реалізація:
а – білого шуму;
б – хаотичного процесу

Рис. 3 показує, що навіть при візуальному аналізі, часова реалізація хаотичного процесу подібна до білого шуму, за рахунок відсутності періодичності та псевдовипадкових викидів деяких значень часової реалізації. Крім того, амплітудно-частотні складові білого шуму (а) і хаотичного процесу (б) рівномірно розподілені по всьому діапазону задіяних значень на заданому інтервалі (рис. 4).

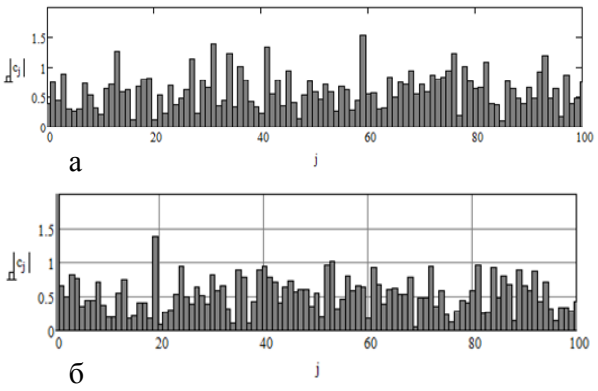

Рис. 4. Амплітудно-частотний спектр:
а – білого шуму;
б – хаотичного процесу

Крім того, висока чутливість хаотичних процесів до точності завдання керуючих параметрів обумовлює експоненціальне зростання часу розвідки [8–9], що значно перевищує можливу тривалість сигналу або час його передачі по каналу зв'язку.

Також слід зазначити, що хаотичні процеси, на відміну від випадкових процесів, мають такі властивості, як висока чутливість до початкових значень і експоненціальне розбігання близьких фазових траєкторій [10–11], що в подальшому може бути застосовано для кодового розподілу абонентів в радіомережі. На рис. 5 наведена залежність коефіцієнта кореляції та кореляційна функція двох хаотичних процесів, з різними початковими значеннями $x_0 \in (0..1)$ їх формування $\Delta x = x_0^{\langle 1 \rangle} - x_0^{\langle 2 \rangle}$.

В загальному випадку, формула за якою був розрахований коефіцієнт кореляції має вигляд [10]:

$$r_{ab} = \frac{\sum (a_i - \tilde{a}) \times (b_i - \tilde{b})}{\sqrt{\sum (a_i - \tilde{a})^2 \times (b_i - \tilde{b})^2}}. \qquad (1)$$

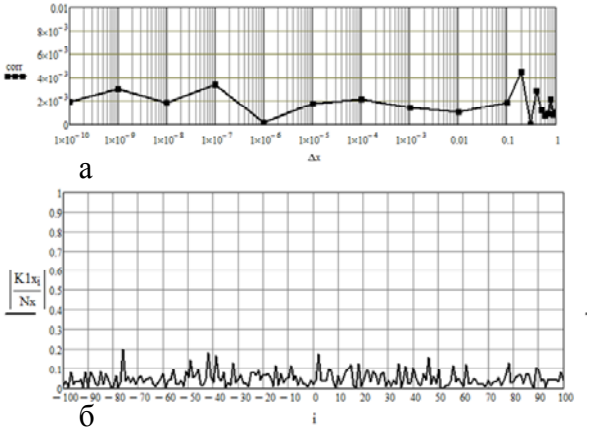

Рис. 5. Залежність кореляції двох хаотичних процесів від розбіжності початкових значень на Δx при їх формуванні:
а – коефіцієнт кореляції;
б – кореляційна функція

На рис.5 показано, що навіть при нікчемо малій різниці між початковими умовами формування (керуючими параметрами) двох хаотичних процесів, процеси не є корельованими. Слід також відзначити, що пікове значення автокореляційної функції білого шуму (рис. 6) так само як і хаотичного процесу (рис. 7) знаходиться біля певного центру, що залежить від значення математичного очікування випадкової величини.

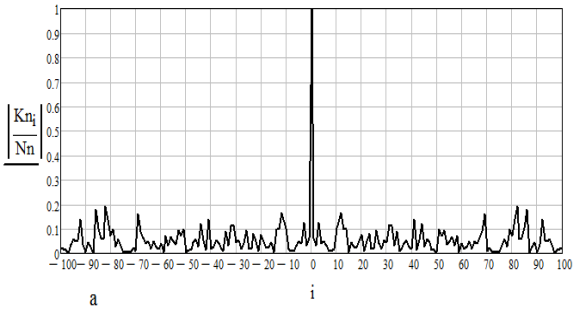

Рис. 6. Автокореляційна функція
білого шуму

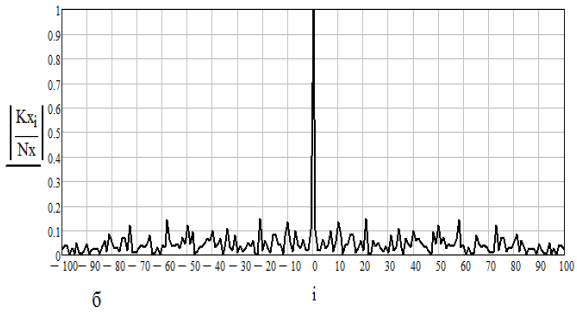

Рис. 7. Автокореляційна функція хаотичного процесу

Але слід розуміти що візуальна оцінка статистичних характеристик процесів що розглядаються має достатньо велику похибку, тому для точної оцінки доцільно застосувати елементи кореляційного аналізу, що наведені в роботі [12]:

1. Середньоквадратичне значення бічних вершин R_i, що визначається через дисперсію

$$\sigma_R^2 = \frac{1}{N}\sum_{i=-(N-1)}^{N-1} R_i^2 . \qquad (2)$$

2. Середнє значення модулів бічних вершин

$$m_{|R|} = \frac{1}{2N}\sum_{i=-(N-1)}^{N-1} |R_i| . \qquad (3)$$

3. Середньоквадратичне значення модулів бічних вершин, яке визначається через дисперсію

$$\sigma_{|R|}^2 = \sigma_R^2 - m_{|R|}^2 . \qquad (4)$$

4. Значення максимальної бокової вершини R_{max}.

Результати розрахунку що характеризують перевищення σ_R, $m_{|R|}, \sigma_{|R|}, R_{max}$ рівня $\sqrt{N}$ (для $N = 127$) наведені в табл. 1 в ненормованому вигляді.

Таблиця 1

Характеристики КФ хаотичних несучих та білого шуму

Корр. функції	$\sigma_R\sqrt{B}$	$m_{\|R\|}\sqrt{B}$	$\sigma_{\|R\|}\sqrt{B}$	$R_{max}\sqrt{B}$
АКФ хаотичного процесу	0,73	0,66	0,44	2,19
ВКФ хаотичного процесу	0,71	0,61	0,42	1,89
КФ (АКФ, ВКФ) білого шуму	0,7	0,56	0,43	2,1 – 3,5

У табл. 1 також для порівняння наведені характеристики КФ білого шуму [12].

На основі з аналізу даних, приведених в табл. 1, можна зробити висновок що характеристики АКФ та ВКФ наведеного хаотичного процесу подібні до статистичних характеристик білого шуму (шуму спостереження), що вигідно відрізняє хаотичні процеси від гармонічних сигналів.

Висновки

Застосування бездротових сенсорних мереж для збору розвідувальної інформації Збройними Силами України під час проведення Операції об'єднаних сил набуває все більшого розповсюдження.

Наявність у незаконних збройних формувань сучасних зразків техніки радіоелектронного подавлення російського виробництва ставить під загрозу безперервність та надійність функціонування розгорнутих на передовій тактичних бездротових систем за рахунок того, що в якості несучих застосовуються широкосмугові гармонічні сигнали з різними видами модуляції, що володіють недостатньою завадостійкістю та розвідзахищеністю (скритністю) та можуть бути виявлені методами спектрального, кореляційного та нелінійного аналізу.

Для підвищення скритності та стійкості радіоканалу передачі даних бездротових сенсорних мереж пропонується застосовувати в якості несучої хаотичні сигнали (процеси), що за своїми статистичними характеристиками (часова реалізація, амплітудно-частотний спектр та кореляційні складові) подібні до шуму спостереження, володіють високою чутливістю до початкових значень формування, можуть бути сформовані в цифровому виді та передані в радіоканал в реальному масштабі часу.

Список літератури

1. Алімпієв А.М. Застосування досвіду АТО для підготовки фахівців зв'язку, РТЗ, А та ІС / А.М. Алімпієв, О.І. Кушнір, К.С. Васюта. – Х.: ХУПС, 2016. – 326 с.

2. Dargie W. Fundamentals of wireless sensor networks: Theory and practice / W. Dargie, C. Poellabauer. – John Wiley and Sons Ltd, 2010. – 300 p.

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

4. Васюта К.С. Анализ эвристических моделей информационных систем на хаотической несущей / К.С. Васюта // Межведомственный научно-технический сборник. Радиоэлектроника. – 2009. – № 156. – С. 17-22.

5. Костенко П. Ю. Повышение скрытности сигналов на основе усложнения аттрактора хаотического процесса с использованием линейного преобразования с ядром Мандельброта / П.Ю. Костенко, К.С. Васюта, С.Н. Симоненко // Радиоэлектроника. – 2010. – № 12(53). – С. 14-23.

6. Wang S. A New Ranging Technique for IEEE 802.16e Uplink / S.Wang, W.Yingchun, G.Jianxin // International Journal of Wireless and Microwave Technologies. – 2011. – Vol. 1, No. 4. – P. 19-26.

7. Huang L. The Design and its application in Secure Communication and image encryption of a new lorenz-like system with varying parameter / L. Huang, D. Shi, J. Gao // Mathematical Problems In Engineering. – 2016. – Vol. 2016. – P. 1-11.

8. Vasylyshyn V.I. Adaptive variant of the surrogate data technology for enhancing the effectiveness of signal spectral analysis using eigenstructure methods / V.I. Vasylyshyn // Radioelectronics and Communications Systems. International peer-reviewed scientific journal. – 2015. – Vol. 58. – P. 116-126.

9. Барсуков А.Н. Методы повышения скрытности хаотических сигналов и их обработки: дис. канд. техн. наук: 05.12.17 / Барсуков Андрей Николаевич. – Х., 2010. – 148 с.

10. Jovic B. Synchronization techniques for chaotic communication systems / B. Jovic. – Berlin, Springer, 2011. – 354 p.

11. Pan J. A New improved scheme of chaotic masking secure communication based on Lorenz system / J. Pan, Q. Ding, B. Du // International Journal of Bifurcation and Chaos. – 2012. – Vol. 5. – P. 10.

12. Кушнир А.И. Корреляционные свойства радиоимпульса, сформированного с применением псевдослучайной последовательности Лемера / А.И. Кушнир, К.С. Васюта, А.В. Крыжный, Ф.Ф. Зоц // Збірник наукових праць Харківського національного університету Повітряних Сил. – 2014. – № 3(40). – С. 69-72.

References

1. Alimiev, A.M., Kushnir, O.I. and Vasyuta, K.S. (2016), "*Zastosuvannja dosvidu ATO dlja pidhotovky faxivciv zvjazku, RTZ, A ta IS*" [*Application of the ATO experience for the training of communication specialists, RTS, A and IS*], KAFU, Kharkiv, 326 p.

2. Dargie, W. and Poellabauer, C. (2010), *Fundamentals of wireless sensor networks: theory and practice*, John Wiley and Sons Ltd, 300 p.

3. Makarenko, S.Y., Ivanov, M.S. and Popov, S.A. (2013), "*Pomehozaschischennost sistem svyazi s psevdosluchaynoy perestroykoy rabochey chastot*" [*Noise immunity of communication systems with pseudorandom reorganization to working frequency*], The publishing house, Saint Paterburg, 166 p.

4. Vasyuta, K.S. (2009), "Analiz evristicheskih modeley informatsionnyih sistem na haoticheskoy nesuschey" [The analysis of empirical models of information systems on chaotic bearing], *The Interdepartmental scientific and technical collection, Radio electronics*, Kharkiv, No. 156, pp. 17-22.

5. Kostenko, P., Vasyuta, K. and Simonenko, S. (2010), "Povyishenie skryitnosti signalov na osnove uslozhneniya attraktora haoticheskogo protsessa s ispolzovaniem lineynogo preobrazovaniya s yadrom Mandelbrota" [Increased stealth of signals on the basis of complication of an attractor of chaotic process with use nonlinear transformation with Mandelbrot's core], *Radio electronic engineer*, No. 12(53), pp. 14-23.

6. Wang, S., Yingchun, W. and Jianxin, G. (2011), A New Ranging Technique for IEEE 802.16e Uplink, *International Journal of Wireless and Microwave Technologies*, Vol. 1, No. 4, pp. 19-26.

7. Huang, L., Shi, D. and Gao, J. (2016), The Design and its application in Secure Communication and image encryption of a new lorenz-like system with varying parameter, *Mathematical Problems In Engineering*, Vol. 2016, pp. 1-11.

8. Vasylyshyn, V. (2015), Adaptive variant of the surrogate data technology for enhancing the effectiveness of signal spectral analysis using eigenstructure methods, *Radioelectronics and Communications Systems*, Vol. 58, pp. 116-126.

9. Barsukov, A.N. (2010), "*Metodyi povyisheniya skryitnosti haoticheskih signalov i ih obrabotki*" [*Methods of increasing stealth of chaotic signals and their processing*], Kharkiv, 148 p.

10. Jovic, B. (2011), *Synchronization techniques for chaotic communication systems*, Springer, Berlin, 354 p.

11. Pan, J., Ding, Q. and Du, B. (2012), A New improved scheme of chaotic masking secure communication based on Lorenz system, *International Journal of Bifurcation and Chaos*, Vol. 5, pp. 10.

12. Kushnir, O.I. and Vasyuta, K.S. (2014), "Korrelyatsionnyie svoystva radioimpulsa, sformirovannogo s primeneniem psevdosluchaynoy posledovatelnosti Lemera" [Correlation properties of a radio pulse generated using a Lemer pseudo-random sequence], *Scientific Works of Kharkiv National Air Force University*, No. 3(40), pp. 69-72.

Надійшла до редколегії 4.10.2018
Схвалена до друку 5.11.2018

Відомості про авторів:

Озеров Сергій Вікторович
кандидат технічних наук
старший викладач Харківського національного університету Повітряних Сил ім. І. Кожедуба,
Харків, Україна
https://orcid.org/0000-0003-3953-5187

Коваль Олексій Васильович
магістр
викладач Харківського національного університету Повітряних Сил ім. І. Кожедуба,
Харків, Україна
https://orcid.org/0000-0002-9997-6884

Information about the authors:

Serhii Ozerov
Candidate of Technical Sciences
Senior Instructor of Ivan Kozhedub Kharkiv National Air Force University,
Kharkiv, Ukraine
https://orcid.org/0000-0003-3953-5187

Oleksii Koval
Master
Instructor of Department of Ivan Kozhedub Kharkiv National Air Force University,
Kharkiv, Ukraine
https://orcid.org/0000-0002-9997-6884

Котик Юрій Олегович
бакалавр
курсант Харківського національного університету Повітряних Сил ім. І. Кожедуба, Харків, Україна
https://orcid.org/0000-0002-5563-3249

Гарвардт Сергій Олегович
бакалавр
курсант Харківського національного університету Повітряних Сил ім. І. Кожедуба, Харків, Україна
https://orcid.org/0000-0001-5312-830

Марченко Євген В'ячеславович
бакалавр
курсант Харківського національного університету Повітряних Сил ім. І. Кожедуба, Харків, Україна
https://orcid.org/0000-0003-1619-8915

Yurii Kotyk
Bachelor
Cadet of Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine
https://orcid.org/0000-0002-5563-3249

Serhii Harvardt
Bachelor
Cadet of Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine
https://orcid.org/0000-0001-5312-8305

Yevhen Marchenko
Bachelor
Cadet of Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine
https://orcid.org/0000-0003-1619-8915

АНАЛИЗ ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ ХАОТИЧЕСКИХ ПРОЦЕССОВ ДЛЯ ПОВЫШЕНИЯ ПОМЕХОЗАЩИЩЕННОСТИ СЕНСОРНЫХ СЕТЕЙ ТАКТИЧЕСКОГО ЗВЕНА УПРАВЛЕНИЯ ВОЙСКАМИ

С.В. Озеров, А.В. Коваль, Ю.О. Котик, С.О. Гарвардт, Е.В. Марченко

В статье исследована возможность применения хаотических колебаний (сигналов) в качестве информационного сигнала при организации радиоканала передачи данных в беспроводных сенсорных сетях тактического звена. Рассмотрены принципы построения и функционирования беспроводных сенсорных сетей. С помощью анализа статистических характеристик хаотических процессов осуществлена оценка их скрытности (по сравнению с белым шумом) Приведены предложения и рекомендации по повышению скрытности радиоканала передачи данных в беспроводных сенсорных сетях.

Ключевые слова: *беспроводная сенсорная сеть, незаконные вооруженные формирования, хаотичный процесс, скрытность, передача данных, нелинейный анализ наблюдений, корреляционный анализ.*

THE ANALYSIS TO POSSIBILITY OF APPLICATION CHAOTIC PROCESSES FOR INCREASE INTERFERENCE IMMUNITY THE TACTICAL WIRELESS NETWORKS

S. Ozerov, O. Koval, Y. Kotik, S. Garvardt, Ye. Marchenko

The experience of carrying out the Operation of the Joint Forces shows that one of the decisive factors for the successful implementation of combat missions is the timely provision of troops (forces) to current intelligence information. One way to ensure intelligence gathering in real time is to use wireless sensor networks deployed directly on the collision line. Wireless Sensor Network (Wireless Sensor Network) is a distributed network of small nodes (sensors) with functions for gathering, processing and transmitting data about the state of the environment. Data transfer is carried out using IEEE 802.11n technology (broadband harmonic signals with different modulation types are used as carriers). However, the presence of advanced electronic warfare means by the opponent calls into question the wireless security interference: these types of signals do not fully meet the requirements of secrecy. Because they differ from the noise of observation with correlation, spectral and nonlinear analysis. That is why there is a significant danger that the enemy will disclose the fact that a wireless sensory intelligence information network is operating, which in turn can lead to hostile acts on the radio channel of the data transmission. The basis of destructive actions on the management system should be understood to be the use of radio-electronic intelligence and radio-electronic suppressing devices. Analysis of literature shows that one of the promising approaches to increasing the secrecy of data transmission channels in wireless sensor networks is the use of chaotic processes that, according to their statistical and dynamic characteristics, are similar to the noise of observation. Thus, the purpose of the work is to justify the possibility of using chaotic processes to organize the radio channel of data transmission in wireless sensory networks while performing tasks for the collection of intelligence information.

Keywords: *wireless sensor network, illegal armed formations, chaotic process, secrecy, data transfer, non-linear analysis of observations, correlation analysis.*