ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

УДК 681.3.06:519.248.681

д.т.н., проф. **Горбенко І.Д.** (ХНУ)
д.т.н., проф. **Замула О.А.** (ХНУ)
Вдовенко С.Г. (НУОУ)

ОЦІНКА ПОКАЗНИКІВ ЗАХИЩЕНОСТІ СУЧАСНИХ БЕЗДРОТОВИХ СИСТЕМ ЗВ'ЯЗКУ ШИРОКОСМУГОВОГО ДОСТУПУ НА ОСНОВІ ВРАХУВАННЯ ОСОБЛИВОСТЕЙ ТЕХНОЛОГІЇ OFDM

Рівень інформатизації держави визначається насамперед розвитком інфокомунікацій, як сукупності мережевих ресурсів, призначених для виробництва і надання телекомунікаційних, інформаційних та інших послуг. З появою нових інфокомунікаційних технологій (ІКТ), використанням різних середовищ передачі (оптичне волокно, радіочастотний ресурс), систем мобільного зв'язку з'явилася можливість істотно підвищити продуктивність, ефективність і якість обслуговування телекомунікаційних мереж, а також розширити спектр послуг, які ними надаються. Функціонування цілої низки сучасних ІКТ здійснюється в умовах зовнішніх і внутрішніх впливів, обумовлених, з одного боку, дією природних перешкод, перешкод від інших радіотехнічних систем, що функціонують на близьких частотах або в спільній ділянці діапазону частот, з іншого боку, - навмисних перешкод, створюваних станціями протидії з метою радіоелектронного придушення діючих систем. Можливими стратегіями станції протидії є: визначення змісту повідомлень при використанні легальними абонентами алгоритмів криптографічного захисту даних; фальсифікація повідомлень; порушення цілісності даних; постановка різних типів перешкод і інше. Тому, до ІКТ, особливо, критичного призначення, пред'являються все більш жорсткі вимоги щодо забезпечення ефективності їх функціонування (швидкості передачі інформації, достовірності передавання інформації, живучості, завадозахищеності, інформаційної безпеки). Підвищені вимоги до швидкого прийняття рішення і доведення до виконавців (користувачів) інформації в умовах внутрішніх і зовнішніх впливів, в значній мірі не враховується існуючими інформаційними технологіями. Існує протиріччя між жорсткими вимогами щодо забезпечення скритності, конфіденційності, цілісності, достовірності даних, що зберігаються і передаються по провідних і бездротових лініях зв'язку, з одного боку, і існуючими моделями, методами і технологіями управління телекомунікаційними мережами, інформаційною безпекою, послугами і якістю обслуговування, з іншого боку. Основними шляхами вирішення зазначеного протиріччя є підвищення завадозахищеності (зокрема, енергетичної, структурної та інформаційної скритності) та інформаційної безпеки ІКС на основі удосконалення методологічних основ побудови ІКТ шляхом розробки методів інформаційного обміну, методів синтезу нових класів сигналів з необхідними ансамблевими, кореляційними і структурними властивостями.

Ключові слова: захищеність інформації, інформаційна безпека, імітозахист, імітостійкість, криптографічний сигнал, мультиплексування сигналів з ортогональним частотним розділенням каналів, пропускна спроможність.

Вступ та постановка проблеми. Розвиток технологій безпроводових комунікацій постійно формувався на основі досліджень форм сигналів. Як приклад можна привести використання технології мультиплексування сигналів з ортогональним частотним розділенням каналів (далі OFDM) в сучасних бездротових системах зв'язку широкосмугового доступу (WiMAX, WiFi, LTE та ін.). Застосування такої технології дозволяє підвищити інформаційну ємність системи при обмеженій смузі пропускання, швидкість прийому-передачі даних, наблизивши її до пропускної спроможності каналу, збільшити скритність передачі і стійкість перед перешкодами прийому сигналів, і як наслідок, забезпечити постійно зростаючі потреби користувачів мереж в високошвидкісних з'єднаннях і мультимедійних сервісах.

По суті OFDM це схема модуляції, що використовує множину несучих. Канал ділиться на кілька субканалів. В OFDM високошвидкісний потік даних конвертується в кілька паралельних бітових потоків меншої швидкості, кожен з яких модулюється своєю окремою несучою. Вся ця множина несучих передається одночасно. Одна з переваг OFDM полягає в тому, що тривалість символу в допоміжній несучій значно більше в порівнянні з затримкою поширення, ніж в традиційних схемах модуляції. Все вищенаведене робить OFDM набагато стійкішою до між символьної інтерференції.

Викладення основних результатів. Аналітично OFDM сигнал може бути представлений у вигляді [1]:

$$S(t) = \sum_{k=0}^{N-1} S_k(t) = \sum_{k=0}^{N-1} A_k e^{\frac{j2\pi kf}{T}}, 0 \le t \le T, \quad (1)$$

де k - індекс піднесучої, $S_k(t)$- сигнал на k-піднесучий, A_k - амплітудна складова послідовності інформаційних символів, N - кількість піднесучих, T - тривалість інформаційного символу.

Структурну схему модулятора OFDM представлено в роботах [2-3]. У передавачі послідовний потік бінарних символів $S(n)$ кодується завадостійким кодом, перемежовується і далі, за допомогою інверсного мультиплексування (демультиплексування), перетворюється в N паралельних потоків, кожен з яких узгоджується (комплексно) з вихідним потоком $S(n)$, використовуючи деякі сузір'я модуляції (квадратурну амплітудну модуляцію QAM, квадратурну фазову модуляцію QPSK і ін.). Кількість виходів демультиплексора визначається кількістю піднесучих частот. Далі модульовані потоки $X_0,...,X_{N-1}$ символів піддаються швидкому зворотному перетворенню Фур'є (ЗШПФ), яке переводить їх у цифрові відклики $X_0,...,X_{N-1}$ (в загальному випадку комплексні числа) в часовій області. Дійсна $(\mathrm{Re}\{x_i\})$ і уявна $(\mathrm{Im}\{x_i\})$ складові відкликів $x_i\ (i = 0,...,N-1)$ піддаються цифро-аналоговому перетворенню (ЦАП). Отримані аналогові сигнали використовуються для модуляції відповідно синусоїди і косинусоїд (одержуваної зрушенням синусоїди на 90°) несучої частоти f_c, Після модуляції сигнали підсумовуються, утворюючи сигнал $S(t)$, який надходить до каналу зв'язку.

Ортогональність піднесучих дозволяє на прийомі виділити кожну з них із загального сигналу навіть в разі часткового перекриття їх спектрів. Оскільки піднесучи розташовуються впритул один до одного і навіть частково накладаються один на одного, спектральна ефективність модульованого OFDM сигналу є високою. Параметри піднесучих сигналів підбираються таким чином, щоб вони були по відношенню один до одного ортогональні, тобто для них виконується умова:

$$\int_0^T \sin 2\pi f_1(t) \sin 2\pi f_k(t) dt = 0, \quad (2)$$

де T – тривалість переданого символу, f_1 і f_k – частоти l-го і k-го несучих сигналів відповідно.

Ортогональність несучих сигналів гарантує частотну незалежність каналів один від одного і, отже, відсутність міжканальної інтерференції. Для швидкої реалізації даної процедури використовують алгоритм зворотного швидкого перетворення Фур'є (ЗШПФ), тобто значення сигналу на вході блоку ЗШПФ відносяться до частотної області. На виході блоку ЗШПФ отримують значення сигналу у часовій області. Об'єднуючи всі значення, отримують складний OFDM сигнал. З урахуванням того, що ЗШПФ працює ефективно з масивами розмірності 2^k, кількість піднесучих вибирається аналогічної кратності. Наприклад, в безпровідних системах зв'язку Wi MAX число піднесучих вибирається від 128

до 2048 і може займати смуги частот від 1,25 МГц до 20 МГц. Для кожної з піднесучих використовується свій вид модуляції в залежності від вимог і виду перешкод в каналі. На приймальному кінці виконуються зворотні операції, при цьому, замість цифро-аналогового перетворювача (ЦАП) використовують аналого-цифровий перетворювач (АЦП), замість ЗШПФ - пряме ШПФ.

Передавач представлено на рис. 1.

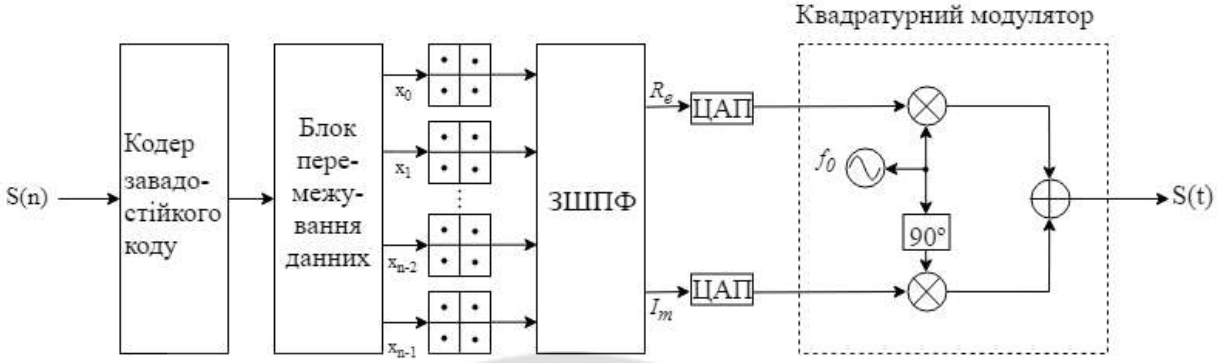

Рисунок 1 – Схема OFDM-модулятора

Структура OFDM сигналу може бути досить складною оскільки складається з множини компонентів:

- структура частотно-часового розподілу, що задана: початковою частотою, кроком сітки частот, кількістю піднесучих;
- за часовими слотами, що задані: тривалістю символу, тривалістю захисного інтервалу;
- вид маніпуляції: фазова (BPSK, QPSK, 8-PSK) або амплітудно-фазова квадратурна модуляція (QAM);
- дискретні послідовності, які визначають закон (правило) маніпуляції фази високочастотної несучої, і задаються розмірністю сигнального простору;
- вид символьної синхронізації;
- наявність і вид завадостійкого кодування (код Ріда-Соломона, код Боуза-Чоудхурі-Хоквінгема, турбокоди і ін.);
- наявність і вид перемеження даних і ін.

Наведені вище особливості структури OFDM сигналу можуть бути використані при побудові ІКТ, для яких вимоги забезпечення заданих показників захищеності від введення (нав'язування) неправдивих повідомлень, фальсифікації повідомлень; порушення цілісності даних, конфіденційності, завадостійкості прийому, скритності функціонування є визначальними.

Однією зі складових (поряд з інформаційної скритністю) інформаційної безпеки є система імітозахисту (забезпечення цілісності) інформації. Математичний апарат системи імітозахисту включає криптографічний алгоритм імітозахищеного кодування інформації (це може бути алгоритм шифрування, код автентифікації, або інше перетворення) і алгоритм прийняття рішення про істинність отриманої інформації, а також ключову систему. По суті імітозахищеність є складною послугою, яка забезпечується наданням таких послуг як цілісність, справжність, (автентичність), а також застосуванням різних криптографічних протоколів з певними властивостями [4-5]. Як показали дослідження [6-7], забезпечити необхідну в ІКС імітозахищеність можливо на рівні джерела складних сигналів за рахунок збільшення розмірності простору сигналів, ступеня корельованності між ними, складності законів їх побудови. Згідно з наведеними визначеннями, для кількісної оцінки імітозахищеності може бути застосована теорія автентифікації Дж. Сімонса [8]. Саме Сімонс показав, що кількісний показник автентичності - ймовірність обману, може бути обчислено за виразом:

$$P_{\text{обм}} \geq 2^{-\Delta I(C,K)}, \qquad (3)$$

де $\Delta I(C,K)$ - кількість інформації, що вводиться в криптограму C про ключі K автентифікації.

Проведемо аналіз виразу (3).

1. Системи, в яких досягається рівність (3), відносять до систем, що володіють абсолютною стійкістю до омани.

2. Для зменшення ймовірності омани необхідно збільшувати $\Delta I(C,K)$.

З урахуванням особливостей структури OFDM сигналу, імітостійкість (I_C) залежить від розмірності сигнального простору (l), числа спроб (C) нав'язування (імітації), простору (Z) компонент структури OFDM сигналу, (зокрема: початкова частота, крок сітки частот, кількість піднесучих і ін.), стратегій (X) нав'язування:

$$I_C = F(1, Z, C, X). \tag{4}$$

На рівні джерела складних сигналів (на фізичному рівні) ймовірність обману або нав'язування помилкового сигналу, є:

$$P_{\text{обм}} \geq 2^{-l_i}, \tag{5}$$

де l_i - довжина імітовставки (коду автентифікації, розмірність сигнального простору).

Покажемо можливість підвищення імітозахищеності бездротових комунікаційних систем, на основі використання різних класів дискретних маніпулюючих послідовностей (далі - ДП). В [9-13] представлені результати досліджень, які присвячені питанням синтезу, формування і дослідження властивостей нового класу ДП, - нелінійних дискретних криптографічних послідовностей (далі - КП). Синтез таких ДП і сигналів, які отримують, наприклад, шляхом маніпуляції фази високочастотної несучої за законом ДП, ґрунтується на застосуванні випадкових (псевдовипадкових) процесів, в тому числі, - ключових даних криптографічних алгоритмів, і при цьому, сигнали повинні володіти: абсолютною структуної скритністю щодо законів їх формування; покращеними ансамблевими властивостями (існувати практично для будь-якого значення періоду, мати значний об'єм системи сигналів); необхідними кореляційними властивостями, що дозволить забезпечити необхідні для того чи іншого додатка ІКС значення завдозахищеності, інформаційної безпеки та скритності функціонування системи. Особлива властивість систем криптографічних сигналів (КС): можливість їх відновлення в просторі і в часі із застосуванням ключів і ряду інших параметрів, які використовуються в процесі синтезу сигналів.

Проведемо оцінку імітостійкості радіоканалу ІКС при вирішенні задачі розрізнення сигналів при застосуванні динамічного режиму зміни відповідності: біт повідомлення - складний сигнал, і різних систем сигналів. У табл. 1 наведено результати оцінки ансамблевих властивостей різних систем складних сигналів (М-послідовності, послідовності з трирівневим значенням функції взаємної кореляції (ПФВКТ), криптографічні сигнали (КС)), гранично досяжні значення максимальних бічних пелюсток функції взаємної кореляції (так звана «границя щільної упаковки») для відповідних періодів ДП, а також значення ймовірностей нав'язування, що отримані відповідно до виразу (5), при використанні в ІКС в якості фізичного переносника даних зазначених класів сигналів.

Таблиця 1

Ансамблеві можливості систем складних сигналів

Клас сигналів	Період послідовності	Значення «границі щільної упаковки»	Число пар послідовностей	Значення ймовірності нав'язування
М- послідовності	31	9	3	$3 \cdot 10^{-1}$
ПФВКТ	31	9	495	$2 \cdot 10^{-3}$
КС	31	9	1465137	$7 \cdot 10^{-7}$
М- послідовності	63	17	20	$5\ 10^{-2}$
ПФВКТ	63	17	975	$1\ 10^{-3}$
КС	63	17	12 214 869	$8\ 10^{-7}$
М- послідовності	127	27	36	$2 \cdot 10^{-2}$
ПФВКТ	127	17	11610	$8 \cdot 10^{-5}$
КС	127	27	9006648	$1 \cdot 10^{-7}$
М- послідовності	255	36	28	$3 \cdot 10^{-2}$
КС	255	36	17599	$5 \cdot 10^{-5}$
М- послідовності	511	63	276	$3 \cdot 10^{-3}$
ПФВКТ	511	33	147500	$6 \cdot 10^{-6}$
КС	511	63	2666671	$3{,}7 \cdot 10^{-7}$
М - послідовності	1023	100	435	$2 \cdot 10^{-3}$
ПФВКТ	1023	65	338000	$3 \cdot 10^{-6}$
КС	1023	100	5293538	$2 \cdot 10^{-7}$

Аналіз даних табл. 1 показує, що запропонований метод синтезу складних нелінійних дискретних криптографічних сигналів, дозволяє формувати великі ансамблі дискретних послідовностей практично будь-якого періоду. Так для періоду послідовності N = 63 число пар КП, що задовольняють граничному значенню максимальних бічних пелюсток ПФВК - 17, становить 12 214 869. Для представника класу лінійних послідовностей - послідовностей з трирівневою функцією взаємної кореляції (множини Голда, які є оптимальними з точки зору функцій взаємної кореляції [14]), число пар сигналів, які відповідають даній границі становить - 975. Перевищення об'єму КС над ансамблем, складеного з М-послідовностей становить більш ніж 10^7 раз. Для періоду послідовності 1023 елементи, число пар КП, що задовольняють граничному значенню для бічних пелюсток функцій взаємної кореляції (ФВК) - 100, становить 5293538, тоді як для представника класу лінійних послідовностей - М-послідовностей, число пар, які відповідають даній границі, становить – 435 , тобто перевищення об'єму системи сигналів становить більш ніж 10^5 разів. При незначному зниженні вимог до граничного значення максимального бічного піку ПВКФ, відповідно до якого здійснюється відбір сигналів (по суті, зниження завадостійкості прийому), можуть бути істотно покращені показники імітостійкості функціонування ІКС. Так, для періоду послідовності N = 127, збільшення значення границі на 1,2 дБ, дозволить збільшити об'єм ансамблю з М = 11610 (при границі 17), до 9 006 648 сигналів, при граничному значенні 27, тобто в 776 разів. Як випливає з даних табл. 1, значення ймовірностей нав'язування в разі застосування КС значно менше. Так при періоді послідовності L = 1023 – на чотири порядку менше, ніж при застосуванні М-послідовностей і на порядок менше, ніж у разі застосування послідовностей з 3-х рівневою ПФВК. Покращення показника імітостійкості ІКС досягається завдяки тому, що КС мають поліпшені в порівнянні з лінійними класами сигналів, зокрема, М-послідовностями, ансамблеві властивості. У табл. 2 наведено результати розрахунку статистичних

характеристик різних кореляційних функцій для широко використовуваних в системах зв'язку дискретних сигналів і, в тому числі, характеристики криптографічних ДП. Розрахунки проводилися для різних значень періоду ДП. Як статистичні характеристики кореляційних функцій були обрані: значення найбільших бічних викидів $\frac{R_{\max}}{\sqrt{N}}$; величина математичного очікування модуля викидів $\frac{m_{|R|}}{\sqrt{N}}$; значення середньоквадратичного відхилення модуля викидів $\frac{D_{|R|}^{\frac{1}{2}}}{\sqrt{N}}$ і значення викидів $\frac{D_{(R)}^{\frac{1}{2}}}{\sqrt{N}}$.

Таблиця 2

Статистичні характеристики кореляційних функцій дискретних сигналів

Тип сигналів	Характеристики	$\frac{R_{макс}}{\sqrt{N}}$	$\frac{m_{\|R\|}}{\sqrt{N}}$	$\frac{D_{\|R\|}^{1/2}}{\sqrt{N}}$	$\frac{D_{(R)}^{1/2}}{\sqrt{N}}$
Характеристичні дискретні сигнали	АФАК	1,0 - 1,8	0,5	0,4	0,5
	ПФАК	0,1 – 1,9	0,2	0,1	0,2
	МІФАК	1,4 - 2,6	0,6	0,5	0,8
	АФВК	1,9 - 3,2	1,0	0,8	1,0
	ПФВК	2,5 – 3,6	1,0	0,8	1,2
	СФВК	2.1 – 5,0	0,9	0,7	1,1
М - послідовності	АФАК	0,7...1,25	0,32	0,26	0,41
	ПФАК	$1/\sqrt{N}$	$1/\sqrt{N}$	0	0
	МІФАК	1,3...2,3	0,66	0,49	0,82
	АФВК	1,4...5,0	0,54	0,48	0,73
	ПФВК	1,9...6,0	0,8	0,62	1,0
	СФВК	2,0...5,1	0,83	0,62	1
Криптографічні сигнали	АФАК	1,2 – 1,9	0,5	1	1,1
	ПФАК	0,2 - 1,9	0,6	0,4	0,7
	АФВК	1,4 – 3,4	0,5	0,4	0,6
	ПФВК	1,9 – 5,2	0,7	0,5	0,8

Аналіз даних, які наведено в табл. 2, свідчить про те, що значення максимальних бічних викидів КС, а також статистичні характеристики даного класу сигналів не поступаються відповідним характеристикам сигналів, побудованих на використанні М-послідовностей і характеристичних дискретних сигналів [15]. Зазначене, в свою чергу, свідчить про те, що використання КС забезпечує завадостійкість прийому сигналів не гірше, ніж при застосуванні зазначених вище сигналів, заснованих на лінійних законах формування. З даних таблиць 1-2 також випливає, що варіюючи граничними значеннями рівня бічних пелюсток функції кореляції, в залежності від вимог, що пред'являються до ІКС, можуть бути вирішені завдання досягнення необхідних значень показників завадостійкості прийому сигналів, імітостійкості і скритності ІКС.

Виконаємо оцінку захищеності ІКС від нав'язування помилкових повідомлень, якщо в системі застосовується (за законом управляючої послідовності) динамічний режим зміни відповідності: біт повідомлення – складний сигнал. В цьому випадку значення імовірності нав’язування хибного повідомлення $\left(P_{\text{нав/пов}}\right)$ (при рівно ймовірному виборі символів управляючої послідовності) може бути визначено за виразом:

$$\left(P_{\text{нав/пов}}\right)=\left(2^{-k}\right)^{n}, \quad (6)$$

де 2^{-k} - число можливих станів джерела управляючої послідовності, яке визначається ансамблем дискретних сигналів - переносників інформації; n - довжина повідомлення, що надана в бітах.

У таблиці 3 наведено значення імовірності нав'язування $\left(P_{\text{нав/пов}}\right)$ повідомлення для дискретних сигналів, отриманих на основі маніпуляції несучої по закону М-послідовностей, ПФВКТ і нелінійних КП. Як розмірність повідомлення обрано значення n=32. У розрахунках $\left(P_{\text{нав/пов}}\right)$, для випадку застосування в системі нелінійних КС, були відібрані послідовності, кореляційні характеристики яких близькі до оптимальних граничних значень з точки зору ПФВК $\left(R_{\max}\le 1{,}5\sqrt{N}\right)$.

Таблиця 3

Значення імовірності нав'язування повідомлення для дискретних сигналів

Період сигналу	Значення $\left(P_{\text{нав/пов}}\right)$ для систем сигналів:		
	М-послідовності	ПФВКТ	Нелінійні КС
31	2^{-96}	2^{-288}	2^{-672}
63	2^{-96}	2^{-320}	2^{-768}
127	2^{-160}	2^{-448}	2^{-640}
1023	2^{-192}	2^{-608}	2^{-736}

Аналіз даних таблиці 3 показує, що в ІКС, які застосовують технології мультиплексування сигналів з ортогональним частотним розподілом каналів, значення $\left(P_{\text{нав/пов}}\right)$ для нелінійних КС значно менші, ніж у випадку використання лінійних класів сигналів.

Висновки. Однією з основних тенденцій розвитку сучасних бездротових систем зв'язку широкосмугового доступу є стрімке поширення таких технологій як OFDM і MIMO (множинний вхід – множинний вихід / multiple-input multiple-output). Зазначені технології дозволяють досягти збільшення інформаційної ефективності в умовах багатопроменевого поширення і, як наслідок, забезпечити постійно зростаючі потреби користувачів мереж бездротового зв'язку в високошвидкісних з'єднаннях і специфічних мультимедійних сервісах. Для деяких додатків ІКС визначальним фактором при їх проектуванні та функціонуванні є стан захищеності систем обробки та зберігання даних, при якому забезпечено збереження конфіденційності, цілісності та доступності інформації, а також інших властивостей інформації та послуг: автентичності, спостереженості, незаперечності і надійності. При цьому розробка захищених бездротових систем зв'язку, які могли б надійно підтримувати мультимедійні додатки, що з'являються, стикається з низкою технологічних викликів, які вимагають серйозних дослідницьких зусиль. Один з таких викликів обумовлений вибором класів дискретних послідовностей, властивості яких в значній мірі визначають властивості фізичних переносників даних в ІКС. У роботі на основі аналізу структури OFDM сигналу наводяться оцінки захищеності ІКС від нав'язування помилкових сигналів і повідомлень шляхом застосування в якості фізичного переносника даних нелінійних дискретних криптографічних сигналів

ЛІТЕРАТУРА:

1. Harish Kumar Pal, Anand Kumar Singh PAPR Reduction technique using advanced peak windowing method of OFDM System. International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-2, May 2013.

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. Замула О.А. Технологии формирования OFDM сигналов в современных информационно-коммуникационных системах. Радиотехника: Всеукраинский межведомственный научно – технический сборник - 2018 г. - Вип. 193. – С. 152 – 159.

4. Горбенко, І.Д., Горбенко, Ю.І. Прикладна криптологія. Теорія. Практика. Застосування: монографія / І.Д. Горбенко, Ю.І Горбенко. – Харків : Форт, 2012. – 880 с.

5. Горбенко, Ю.І. Методи побудування та аналізу, стандартизація та застосування криптографічних систем / Ю.І. Горбенко. – Харків : Форт, 2016. – 959 с.

6. Gorbenko, I.D., Zamula, A.A., Morozov. V.L. Information security and noise immunity of telecommunication systems under conditions of various internal and external impacts // Telecommunications and Radio Engineering Volume 76, 2017 Issue 19, pages 1705-1717.

7. Замула А.А., Морозов В.Л. Информационные технологии передачи данных в современных телекоммуникационных системах // Радиотехника: Всеукраинский межведомственный научно – технический сборник - 2016 г. - Вып. 186. – С. 24 – 32.

8. Simmons, G. J. “Authentication theory coding theory”, 1985.

9. Gorbenko, I.D., Zamula, A.A., Semenko, Ye.A. Ensemble and correlation properties of cryptographic signals for telecommunication system and network applications // Telecommunications and Radio Engineering. - Volume 75, 2016 Issue 2. Pages 169-178.

10. Gorbenko, I. D., Zamula, A. A. Cryptographic signals: requirements, methods of synthesis, properties, application in telecommunication systems // Telecommunications and Radio Engineering Volume 76, 2017. Issue 12, pages 1079-1100.

11. Gorbenko,I. D., Zamula, A.A., Semenko A. E., Morozov V.L. Method for synthesis of performed signals systems based on cryptographic discrete sequences of symbols // Telecommunications and Radio Engineering. Volume 76, 2017 Issue 17, pages 1523-1533.

12. Gorbenko. I.D., Zamula, A.A., Semenko, A.E., Morozov, V. L. Method for complex improvement of characteristics of orthogonal ensembles based on multiplicative combining of signals of different classes// Telecommunications and Radio Engineering. Volume 76, 2017 Issue 18, pages 1581-1594 .

13. Горбенко І.Д., Замула О.А. Моделі та методи синтезу криптографічних сигналів та їх оптимізація за критерієм часової складності // Математичне та комп’ютерне моделювання. Серія: Фізико-математичні науки: збірник наук. праць / Інститут кібернетики імені В.М. Глушкова Національної академії наук України, 2017. Вип. 15. 272 с.

14. Sarvate, D.V. Crosleration Properties of Pseudorandom and Related Sequences / D.V. Sarvate, M.V. Pursley // IEEE Trans. Commun, 1980. – Vol. Com 68 – P. 59–90.

15. Свердлик М. Б. Оптимальные дискретные сигналы. / Свердлик М. Б. М: *Радио и связь*, 1975. – 200 с.

REFERENCES:

1. Harish Kumar Pal and Anand Kumar Singh PAPR Reduction technique using advanced peak windowing method of OFDM System. International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-2, May 2013.

2. Bakulin, M.G., Kreindelin, V.B., Shloma, A.M. and Shumov, A.P. (2015), “Technologiya OFDM” [OFDM technology], Educational manual for high schools, Moscow, Goryachaya liniya - Telekom, 360 p.

3. Zamula, A.A. (2018), “Tekhnologii formirovaniya OFDM signalov v sovremennykh informatsionno-kommunikatsionnykh sistemakh. ” [Technologies of forming OFDM signals in modern information and communication systems.], Radiotekhnika: Vseukrainskiy mezhvedomstvennyy nauchno – tekhnicheskiy sbornik, No. 193, pp. 152 -159.

4. Gorbenko, I.D. and Gorbenko, Yu.I. (2012), “Prykladna kryptolohiya. Teoriya. Praktyka. Zastosuvannya.” [Applied cryptology. Theory. Practice. Application], // Monograph / I.D. Gorbenko, Yu.I Gorbenko. Kharkiv: Fort, 880 p.

5. Gorbenko, Yu.I. (2016), “Metody pobuduvannya ta analizu, standartyzatsiya ta zastosuvannya kryptohrafichnykh system” [Methods of construction and analysis, standardization and application of cryptographic systems], // Yu.I Gorbenko. Kharkiv: Fort 959 p.

6. Gorbenko, I.D., Zamula, A.A. and Morozov, V.L., “Information security and noise immunity of telecommunication systems under conditions of various internal and external impacts” // Telecommunications and Radio Engineering Volume 76, 2017 Issue 19, pages 1705-1717.

7. Zamula, A.A. and Morozov, V.L. (2016), “Informatsionnyye tekhnologii peredachi dannykh v sovremennykh telekommunikatsionnykh sistemakh” [Information technology of data transmission in modern telecommunication systems] // Radiotekhnika: Vseukrainskiy mezhvedomstvennyy nauchno – tekhnicheskiy sbornik, No. 193, pages 24 –32.

8. Simmons, G.J. (1985) “Authentication theory coding theory”.

9. Gorbenko, I.D., Zamula, A.A. and Semenko, Ye.A. (2016) “Ensemble and correlation properties of cryptographic signals for telecommunication system and network applications”. Telecommunications and Radio Engineering. Volume 75, Issue 2. Pages 169-178.

10. Gorbenko, I.D. and Zamula, A.A. (2017) “Cryptographic signals: requirements, methods of synthesis, properties, application in telecommunication systems”. Telecommunications and Radio Engineering. Volume 76,. Issue 12, pages 1079-1100.

11. Gorbenko, I.D., Zamula, A.A., Semenko A.E., Morozov V.L. (2017) “Method for synthesis of performed signals systems based on cryptographic discrete sequences of symbols”. Telecommunications and Radio Engineering. Volume 76, Issue 17, pages 1523-1533.

12. Gorbenko. I.D., Zamula, A.A., Semenko, A.E. and Morozov, V.L. (2017) Method for complex improvement of characteristics of orthogonal ensembles based on multiplicative combining of signals of different classes// Telecommunications and Radio Engineering. Volume 76, Issue 18, pages 1581-1594 .

13. Gorbenko. I.D. and Zamula, A.A. (2017) “Modeli ta metody syntezu kryptohrafichnykh syhnaliv ta yikh optymizatsiya za kryteriyem chasovoyi skladnosti” [Models and methods of synthesis of cryptographic signals and their optimization on the criterion of time complexity] // Matematychne ta komp″yuterne modelyuvannya. Seriya: Fizyko-matematychni nauky: zbirnyk nauk. prats′ / Instytut kibernetyky imeni V.M. Hlushkova Natsional′noyi akademiyi nauk Ukrayiny, Issue 15, 272 p.

14. Sarvate, D.V. Crosleration Properties of Pseudorandom and Related Sequences / D.V. Sarvate, M.V. Pursley // IEEE Trans. Commun, 1980. – Vol. Com 68, pages 59–90.

15. Sverdlik, M. B. (1975), “Optimal'nyye diskretnyye signaly.” [Optimal discrete signals.] // Sverdlik, M. B.: Moscow, Radio i svyaz', 200 p.

д.т.н., проф. Горбенко И.Д., д.т.н., проф. Замула А.А., Вдовенко С.Г.

ОЦЕНКА ПОКАЗАТЕЛЕЙ ЗАЩИЩЕНОСТИ СОВРЕМЕННЫХ БЕСПРОВОДНЫХ СИСТЕМ СВЯЗИ ШИРОКОРОЛОСНОГО ДОСТУПА НА ОСНОВЕ ОСОБЕНОСТЕЙ ТЕХНОЛОГИИ OFDM

Степень информатизации государства определяеться прежде всего развитием развитием инфокомуникаций, как совокупности сетевых ресурсов, предназначеных для производства и оказания телекомуникационных, информационных и других услуг. С появленим нових инфокомуникационных технлогий (ИКТ), использованием различных сред передачи (оптоволокно, радиочастотный ресурс), систем мобильной связи появилась возможность существенно повысить продуктивность, ефективность и качество обслуживания телекомуникационных сетей, а также расширить спектр услуг, которые ими предоставляються. Функционирование целого ряда современных ИКТ осуществляеться в условиях внешних и внутренних влияний, обусловленых, с одной стороны, действием естественных помех, помех от других радиотехнических систем, которые функционируют на соседних частотах или на общем участе диапазона частот, с другой стороны - умышленых помех, создаваемых станциями противодействия с целью радио электронного подавления действующих систем. Возможными стратегиями станции противодействия являються: определение смысла сообщения при использовании легальными абонентами алгоритмов криптографической защиты данных; фальсификация сообщений; нарушение целостности даннях; постановка разных типов помех и др. Поэтому, к ИКТ, особенно относящимся к критической инфраструктуре, пред’являються все болем жосткие требования относительно обеспечения ефективности их функционирования (скорости передачи информации, достоверности передачи информации, живучести, помехостойкости, информационной безопасности). Повышеные требования к быстроте принятия решения и доведение до исполнителей (пользователей) информации в условиях внутренних и внешних влияний, в зачительной мере не учитываються существующими информационными технологиями. Существуют противоречия между жорсткими требованиями к обеспечению скритности, конфиденциальности, целостности, достоверности даннях, которые хранятся и передаються по проводным и беспрводным линиям связи, с одной стороны, и существующимими моделями, методами и технологиями управления телекомуникационными сетями, информационной безопасностью, услугами и качеством

обслуживания, с другой стороны. Основными путями решения данного противоречия являеться повышение помехозащищенности (особенно энергетической, структурной и информационной скрытности), а также информационной безопасности ИКС на основе усовершенствования методологических основ построения ИКТ путем разработки методов информационного обмела, методов синтеза нових клас сов сигналов с необходимыми ансамблевими, кореляционными и структурными свойствами.

Ключевые слова: безопасность информации, защищенность информации, имитозащита, имитостойкость, криптографический сигнал, мультиплексирование сигналов з ортогональным частотным разделением каналов, пропускная способность.

prof. I.Gorbenko , prof. A. Zamula, S.Vdovenko

EVALUATION OF INDICATORS OF PROTECTION OF MODERN WIRELESS COMMUNICATION SYSTEMS OF BROAD-BORN ACCESS ON THE BASIS OF FEATURES OF OFDM TECHNOLOGY

The degree of state informatization is determined primarily by the development of information communications, as a collection of network resources intended for the production and provision of telecommunications, information and other services. With the emergence of new information communication technologies (ICT), the use of various transmission media (optical fiber, radio frequency resource), mobile communication systems, it became possible to significantly increase the productivity, efficiency and quality of service of telecommunications networks, as well as expand the range of services provided by them. A variety of modern ICTs operate under conditions of external and internal influences caused, on the one hand, by natural interference, interference from other radio systems that operate on neighboring frequencies or on a common part of the frequency range, on the other hand, deliberate interference caused by counter stations for the purpose of radio electronic suppression of existing systems. Possible strategies of a counter station are: determining the meaning of a message when legal subscribers use cryptographic data protection algorithms; falsification of messages; violation of the integrity of the data; staging different types of interference, etc. Therefore, ICTs, especially those related to critical infrastructure, are increasingly subject to strict requirements regarding the efficiency of their operation (information transfer speed, reliability of information transfer, survivability, interference resistance, information security). Increased requirements for speed of decision making and bringing to the performers (users) of information in the context of internal and external influences, in a significant measure are not taken into account by existing information technologies. There are contradictions between the requirements for ensuring the privacy, confidentiality, integrity and reliability of data stored and transmitted over wired and wireless communication lines, on the one hand, and existing models, methods and technologies for managing telecommunication networks, information security, services and quality of service, on the other hand. The main ways to solve this contradiction is to increase the noise immunity (especially energy, structural and information secrecy), as well as information security of the ICS by improving the methodological foundations of ICT construction by developing methods of information measurement, methods for synthesizing new classes of signals with the necessary assemblies, correlation and structural properties.

Key words: information security, imitation protection, imitation resistance, cryptographic signal, multiplexing of signals with orthogonal frequency division of channels, throughput.