DOI: 10.18372/2410-7840.20.13252
УДК 004.056.53(045)

АНАЛІЗ КОНФІДЕНЦІЙНОСТІ ПЕРЕДАВАННЯ ІНФОРМАЦІЇ У СИСТЕМАХ DSSS ЗА УМОВ ОБМЕЖЕНОСТІ СИСТЕМ ВИКОРИСТОВУВАНИХ СИГНАЛЬНО-КОДОВИХ КОНСТРУКЦІЙ

Олексій Голубничий

Технічний захист інформації у телекомунікаційних системах може бути реалізований на фізичному рівні цих систем шляхом забезпечення енергетичної та структурної прихованості передавання інформації. До телекомунікаційних технологій, які є найбільш придатними для реалізації таких методів захисту інформації, належать технології широкосмугових систем зв'язку, зокрема технологія DSSS (Direct Sequence Spread Spectrum). Забезпечення необхідного рівня структурної прихованості передавання інформації при використанні технології DSSS полягає в тому, що у цій технології використовуються системи сигнально-кодових конструкцій з достатньо великою кількістю сигналів у системі. До кожної з таких сигнально-кодових конструкцій висуваються вимоги до їх кореляційних властивостей, які відповідно до теореми Вінера-Хінчина визначають спектральні характеристики сигналів у телекомунікаційній системі і, як наслідок, структурну спектральну та енергетичну приховані передавання інформації. Проблема полягає в тому, що регулярні детерміновані методи синтезу систем сигнально-кодових конструкцій з малим рівнем бічних пелюсток автокореляційної функції для будь-якої довжини сигнально-кодової конструкції та кількості таких сигналів у системі сигналів невідомі, а складність цієї проблеми синтезу пов'язана з алгоритмічною нерозв'язністю довільних алгебраїчних діофантових рівнянь. У статті проаналізовано конфіденційність передавання інформації на фізичному рівні телекомунікаційних систем DSSS за умов використання ряду відомих синтезованих систем сигнально-кодових конструкцій з малим рівнем бічних пелюсток автокореляційної функції для випадку, коли несанкціонованим користувачем здійснюються атаки К-дії з використанням оптимальних для нього за результативністю методів обробки сигналів (оптимального розрізнювача біортогональних сигналів).

Ключові слова: *прихованість передавання інформації, конфіденційність, атаки на фізичному рівні телекомунікаційної системи, широкосмуговий зв'язок, технологія DSSS, псевдовипадкові послідовності.*

ВСТУП

Особливістю функціонування широкосмугових телекомунікаційних систем, які працюють за технологією DSSS (Direct Sequence Spread Spectrum), є використання сигнально-кодових конструкцій (СКК), до яких висуваються вимоги щодо їх кореляційних властивостей. Автокореляційна функція (АКФ) таких СКК повинна мати форму, наближену до δ-функції Дірака. Відповідно до теореми Вінера-Хінчина це забезпечуватиме широкий та рівномірний спектр сигналів за умови їх обмеженої потужності у телекомунікаційній системі [1, с. 104]. В свою чергу це також визначатиме високий рівень енергетичної та структурної спектральної прихованості передавання сигналів та є важливим при організації фізичного рівня телекомунікаційних систем, в яких є необхідність забезпечення захисту інформації. Таке забезпечення енергетичної та структурної прихованості передавання інформації є видом технічного захисту інформації (ТЗІ) та може бути складовою комплексної системи захисту інформації, а теоретичні засади та методи обробки сигналів та синтезу СКК посідають важливе значення у методології захисту інформації на фізичному рівні телекомунікаційних систем [2]-[4].

Забезпечення структурної прихованості передавання інформації у технології DSSS ґрунтується на тому, що вищевказаним вимогам до АКФ може відповідати множина (система) СКК, які використовуються при передаванні інформації вибірково у різні інтервали часу відповідно до використовуваного алгоритму зміни СКК та параметрів такого алгоритму, що становить собою елементи системи ключів **К** для захисту інформації на фізичному рівні телекомунікаційної системи. Для несанкціонованого користувача при здійсненні ним атак К-дії на фізичному рівні це створює апріорну невизначеність щодо конкретної СКК, яка повинна використовуватися на кожному інтервалі часу для коректної обробки сигналів та правильного виділення з них інформації, яка передається та підлягає захисту від несанкціонованого доступу. У випадку бінарної структури СКК формуються шляхом використання бінарних псевдовипадкових послідовностей (ПВП).

На рис. 1 показані структурні схеми передавального та приймального пристроїв телекомунікаційної системи DSSS, у якій реалізована функція ТЗІ на фізичному рівні (принципи побудови таких схем для передавання інформації є широко відомими у галузі широкосмугових систем зв'язку, а

особливості їх використання для ТЗІ описані, наприклад, у [4, с. 90-98] при побудові структурної схеми стеганографічної системи захисту інформації з використанням складних дискретних сигналів технології прямого розширення спектру). Особливістю передавального пристрою є те, що він містить два модулятори М1 та М2. Модулятор М1 здійснює розширення спектру інформаційного сигналу $I(t)$ та забезпечує при цьому структурну невизначеність сигналу для несанкціонованого користувача шляхом використання різних СКК з системи сигналів, яка складається з Q ПВП. Модулятор М2 виконує класичну функцію модуляції (схема на рис. 1 відповідає модуляції BPSK) та при стрибкоподібному перестроюванні частоти синтезатором частот забезпечує частотну невизначеність сигналу для несанкціонованого користувача шляхом використання L можливих частотних позицій, які обираються таким чином, щоб забезпечити ортогональність сигналів між різними частотними підканалами. Підсилювач потужності (ПП) та антенно-фідерний пристрій (АФП) виконують функції підсилення, передачі сигналу до антенної системи, узгодження її з фідером та вихідними каскадами передавального пристрою, випромінювання сигналу.

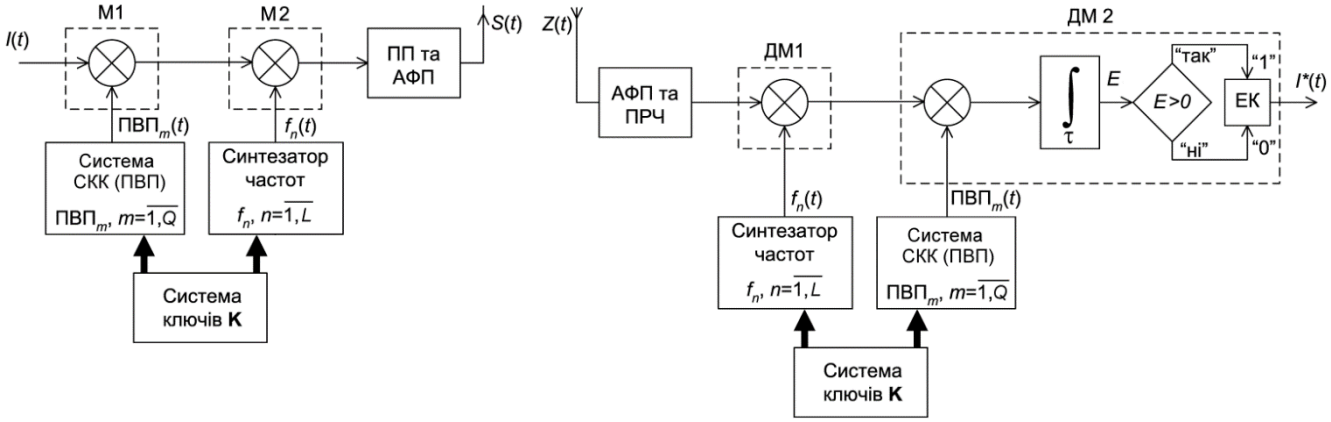

Рис. 1. Структурні схеми передавального та приймального пристроїв телекомунікаційної системи DSSS, у якій реалізована функція ТЗІ на фізичному рівні

Приймальний пристрій містить АФП та підсилювач радіочастоти (ПРЧ), демодулятори ДМ1 та ДМ2, перший з яких (ДМ1) при когерентній обробці сигналу з позицій ТЗІ усуває частотну невизначеність сигналу для санкціонованого користувача, а другий (ДМ2) – структурну невизначеність сигналу за умов роботи апаратури такого санкціонованого користувача у штатному режимі при використанні коректної системи ключів **К**, яка при обробці сигналів забезпечуватиме однаковість сигналів $ПВП_m(t)$ та $f_n(t)$ у кожен момент часу на приймальному та передавальному боці системи DSSS.

Актуальність дослідження полягає в тому, що технологія розширення спектру DSSS використовується для передавання інформації у багатьох сучасних телекомунікаційних системах, наприклад у безпроводових системах стандартів IEEE 802.11 b/g (Wi-Fi), IEEE 802.15.4 (безпроводові мережі малого радіусу дії), для організації багатостанційного доступу з кодовим розділенням каналів (CDMA) у системах мобільного зв'язку, для формування та обробки навігаційних сигналів у системі супутникової навігації GPS та у ряді інших радіотехнічних систем. Інформаційна безпека цих систем, зокрема захищеність їх фізичного рівня від здійснення атак, є важливою складовою забезпечення умов обробки державних інформаційних ресурсів або інформації з обмеженим доступом, які можуть передаватися з використанням таких систем.

Наукова новизна дослідження полягає в тому, що пропонуються та обґрунтовуються математичні моделі аналізу конфіденційності передавання інформації на фізичному рівні систем DSSS при використанні моделі атак К-дії на основі оптимального розрізнювача біортогональних сигналів за умов обмеженості кількості існуючих СКК з дельтаподібною АКФ, що використовуються в системі DSSS, та наявності у несанкціонованого користувача повних даних про використовувані СКК та частотні позиції, окрім конкретного порядку їх використання в часі при передаванні інформації. На відміну від менш жорстких умов щодо обізнаності та ресурсних можливостей несанкціонованого користувача це дозволяє формувати уточнені вимоги до параметрів СКК (довжина ПВП, об'єм системи ПВП), які забезпечуватимуть необхідний рівень захищеності інформації у системі DSSS.

ПОСТАНОВКА ПРОБЛЕМИ

Проблема забезпечення конфіденційності передавання інформації на фізичному рівні телекомунікаційної системи, яка працює за технологією DSSS, полягає у забезпеченні достатнього рівня частотної та структурної невизначеності сигналу для несанкціонованого користувача, яка визначається апріорною невизначеністю частотних позицій $f_n(t)$ та опорних сигналів ПВП$_m(t)$.

Проблема містить такі складові, які пов'язані з синтезом та обробкою сигналів:

1) виділення необхідного радіочастотного ресурсу для використання необхідної кількості L частотних позицій з урахуванням ширини спектру модульованого сигналу, який розміщуватиметься на несних частотах f_n, $n=\overline{1,L}$ – складова проблеми, яка характеризується організаційно-технічними заходами щодо виділення та використання радіочастотного ресурсу;

2) формування систем опорних СКК ПВП$_m(t)$ певної довжини та кількості СКК у системі сигналів – складова проблеми, яка пов'язана з синтезом систем бінарних послідовностей з дельтаподібною АКФ, яка характеризується суттєвою методологічною складністю і становить собою окрему наукову проблему: регулярні детерміновані методи синтезу систем бінарних послідовностей будь-якої довжини та об'єму (кількості послідовностей у системі) з малим рівнем бічних пелюсток АКФ відсутні [5, с. 23], а алгоритмічність розв'язку проблеми синтезу таких СКК пов'язана з проблемою розв'язання алгебраїчних діофантових рівнянь (десятою проблемою Гільберта), для якої у 1970 р. була показана її алгоритмічна нерозв'язність [6].

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Метою статті є аналіз конфіденційності передавання інформації на фізичному рівні телекомунікаційних систем, які працюють за технологією DSSS, за умов використання у якості СКК ряду відомих синтезованих систем бінарних послідовностей (ПВП) з дельтаподібною АКФ, коли сторона здійснення атак (несанкціонований користувач) має повну інформацію про використовувані СКК та частотні позиції, але не має відомостей про систему ключів **K**, яка визначає конкретний порядок їх використання при передаванні інформації, і ставить за мету реалізувати атаки К-дії оптимальним для себе за критеріями результативності чином шляхом аналізу широкосмугового сигналу системи DSSS на фоні завад.

АНАЛІЗ ВІДОМИХ СИГНАЛЬНО-КОДОВИХ КОНСТРУКЦІЙ (ПВП) ДЛЯ СИСТЕМ DSSS

На рис. 2 показано розподіл відомих [7], [8] синтезованих систем ПВП з найменшими значеннями максимального рівня бічних пелюсток нормованої АКФ ($\max|R| = \max\left\{\frac{1}{N}\left|\sum_{i=1+\tau}^{N} a_i a_{i-\tau}\right|\right\}$, $\tau = \overline{1,(N-1)}$, де $a_i \in \{\pm 1\}$, $i=\overline{1,N}$ – елементи ПВП) за їх довжиною N із зазначенням кількості таких ПВП у системі Q, а на рис. 3 – їх розподіл за довжиною N із зазначенням $\max|R|$. В табл. 1 наведено приклади відомих ПВП найбільшої довжини з найменшими значеннями $\max|R|$ [1, с. 108], [7]-[10].

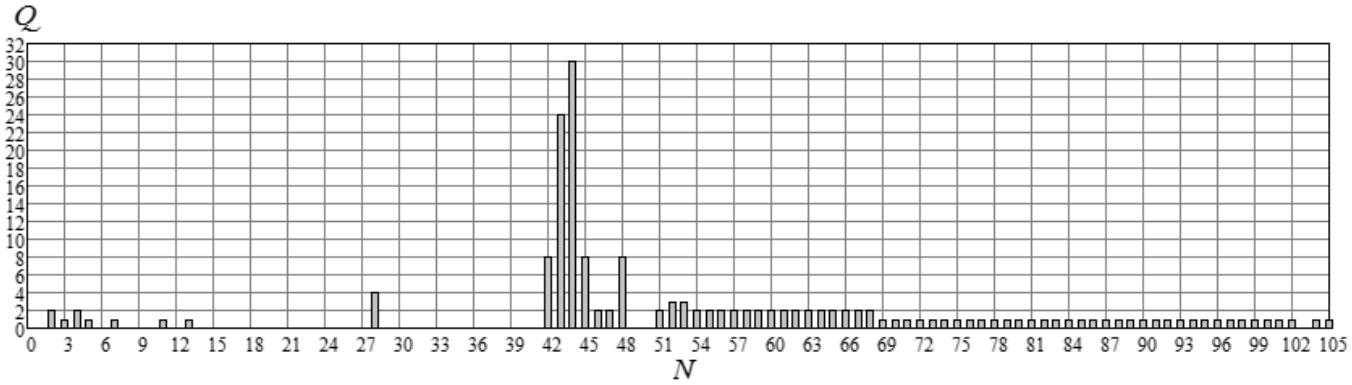

Рис. 2. Розподіл кількості ПВП у системі ПВП для відомих систем ПВП

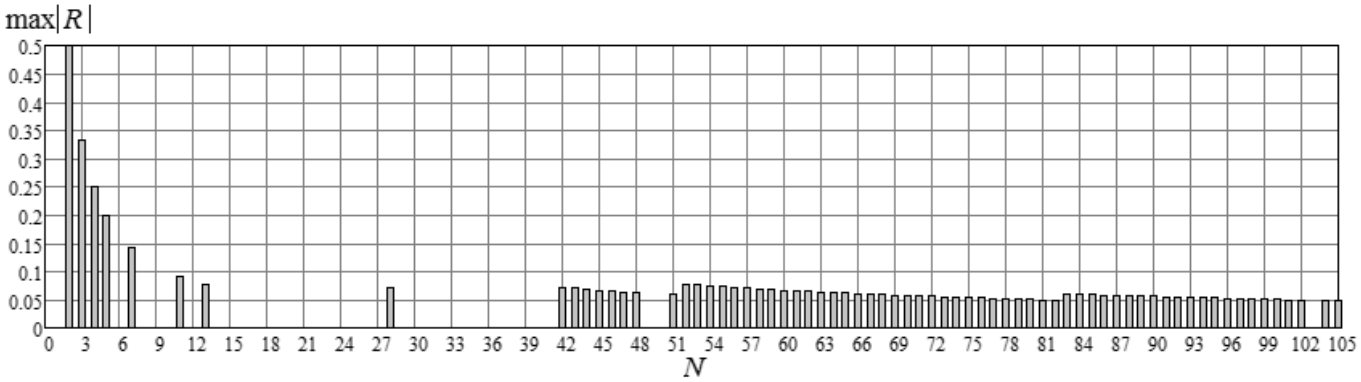

Рис. 3. Розподіл максимального рівня бічних пелюсток нормованої АКФ для відомих систем ПВП

Таблиця 1

Відомі синтезовані ПВП найбільшої довжини max$N$ з найменшими значеннями max|R|

max|R|	max$N$	ПВП
$1/N$	13	1; 1; 1; 1; 1; -1; -1; 1; 1; -1; 1; -1; 1 (послідовність Баркера)
$2/N$	28	1; -1; 1; 1; -1; 1; -1; -1; 1; -1; -1; -1; 1; -1; -1; -1; 1; -1; -1; -1; 1; 1; 1; 1; -1; -1; -1; 1
$3/N$	51	1; 1; 1; -1; -1; -1; 1; 1; 1; -1; -1; -1; -1; -1; -1; -1; 1; 1; 1; -1; 1; 1; 1; -1; -1; 1; 1; -1; 1; 1; 1; -1; 1; 1; -1; 1; -1; 1; -1; 1; 1; -1; 1; 1; -1; 1; 1; -1; 1; -1
$4/N$	82	1; 1; 1; 1; 1; -1; 1; -1; 1; -1; -1; 1; -1; 1; 1; -1; 1; -1; 1; -1; -1; 1; 1; -1; 1; 1; 1; -1; 1; 1; 1; -1; 1; 1; -1; 1; 1; 1; -1; -1; -1; 1; 1; 1; -1; -1; 1; 1; -1; -1; -1; -1; -1; -1; 1; 1; 1; -1; -1; 1; -1; 1; 1; -1; 1; -1; -1; 1; 1; 1; 1; 1
$5/N$	105	1; 1; 1; -1; -1; -1; 1; 1; -1; -1; -1; 1; 1; 1; -1; -1; -1; -1; 1; 1; 1; 1; 1; 1; 1; 1; 1; -1; 1; -1; 1; 1; 1; -1; 1; 1; -1; 1; -1; -1; 1; -1; -1; 1; 1; 1; 1; -1; 1; -1; 1; 1; -1; -1; 1; -1; -1; -1; 1; -1; -1; 1; -1; -1; 1; 1; -1; -1; 1; -1; 1; -1; 1; 1; -1; -1; -1; 1; 1; -1; 1; 1; 1; -1; -1; -1; 1; -1; 1

Основним розповсюдженим методом синтезу розглянутих систем ПВП є метод напрямленого перебору, недоліком якого є суттєве збільшення обчислювальної складності при збільшенні довжини ПВП N. Також розповсюдження набули методи синтезу пари "сигнал-фільтр", синтезу на основі відомих різницевих множин, синтезу на основі лінійних рекурентних послідовностей, синтезу шляхом гомоморфного відображення мультиплікативних груп простого та розширеного поля Галуа [5, с. 22-25]. Використання комбінованого підходу методів синтезу пари "сигнал-фільтр" та на основі відомих різницевих множин дозволило, наприклад, синтезувати узагальнені бінарні послідовності Баркера [11], [12] та їх мультиплікативно комплементарні структури [13], які для їх синтезу, на відміну від методу напрямленого перебору, мають регулярні детерміновані правила кодування (синтезу) і тому є перспективними для використання у технології DSSS.

АНАЛІЗ КОНФІДЕНЦІЙНОСТІ ПЕРЕДАВАННЯ ДАНИХ У СИСТЕМАХ DSSS

У цій статті моделлю приймальної апаратури несанкціонованого користувача є оптимальний розрізнювач біортогональних сигналів, який містить QL кореляторів, пристрій визначення максимальної за абсолютним значенням напруги на їх виходах та пристрій визначення знаку цієї напруги [14, с. 91]. Подальші операції обробки сигналу полягають у комутації у пороговій схемі прийняття рішень про прийнятий бінарний символ результату кореляційної обробки того корелятора, для якого виконується умова максимальної за абсолютним значенням напруги на його виході. На рис. 4 показана структурна схема приймальної апаратури несанкціонованого користувача, яка відповідає розглянутому принципу формування та обробки сигналів у системі DSSS.

Кожен корелятор у такому типі апаратури узгоджений з певною комбінацією частотної позиції та опорного сигналу ПВП у складі сигналу системи DSSS. Кількість комбінацій частотної позиції та опорного сигналу ПВП може бути достатньо великою і для кожної такої комбінації у апаратурі несанкціонованого користувача використовується один корелятор. Тому загальна апаратна складність та вартість апаратури для здійснення несанкціонованого доступу може бути достатньо великою. Приймальна апаратура несанкціонованого користувача при апаратно або економічно обмежених ресурсних можливостях сторони здійснення атак може містити лише деяку, меншу від їх загальної кількості QL, кількість кореляторів. Тоді ця апаратура при аналізі сигналу у системі DSSS

буде охоплювати лише частину від повної кількості можливих комбінацій частотної позиції та опорного сигналу ПВП, що забезпечують структурну прихованість системи зв'язку. Ресурсні можливості системи здійснення атак можуть бути охарактеризовані показником α, який показує, яку частину від загальної кількості QL комбінацій частотних позицій та опорних сигналів ПВП становить кількість кореляторів у системі здійснення атак ($0 \le \alpha \le 1$).

З урахуванням показника α системи здійснення атак можна умовно поділити на три типи:

1) $\alpha = 1$ – система здійснення атак не обмежена за ресурсними можливостями та містить QL кореляторів для усунення структурної невизначеності по всім можливим Q опорним сигналам ПВП та по усім використовуваним L частотним позиціям;

2) $1/QL < \alpha < 1$ – система здійснення атак обмежена за своїми ресурсними можливостями, приймальна апаратура несанкціонованого користувача містить $QL\alpha$ кореляторів;

3) $\alpha = 1/QL$ – система здійснення атак має мінімальні ресурсні можливості, приймальна апаратура несанкціонованого користувача складається лише з одного корелятора; це відповідає наявності у несанкціонованого користувача приймального пристрою санкціонованого користувача (рис. 1) з відсутньою коректною системою ключів **К**, коли несанкціонований користувач при здійсненні спроби несанкціонованого доступу випадковим чином обирає значення поточної частотної позиції та опорного сигналу ПВП.

Якщо $\alpha = 0$, то система здійснення атак відсутня.

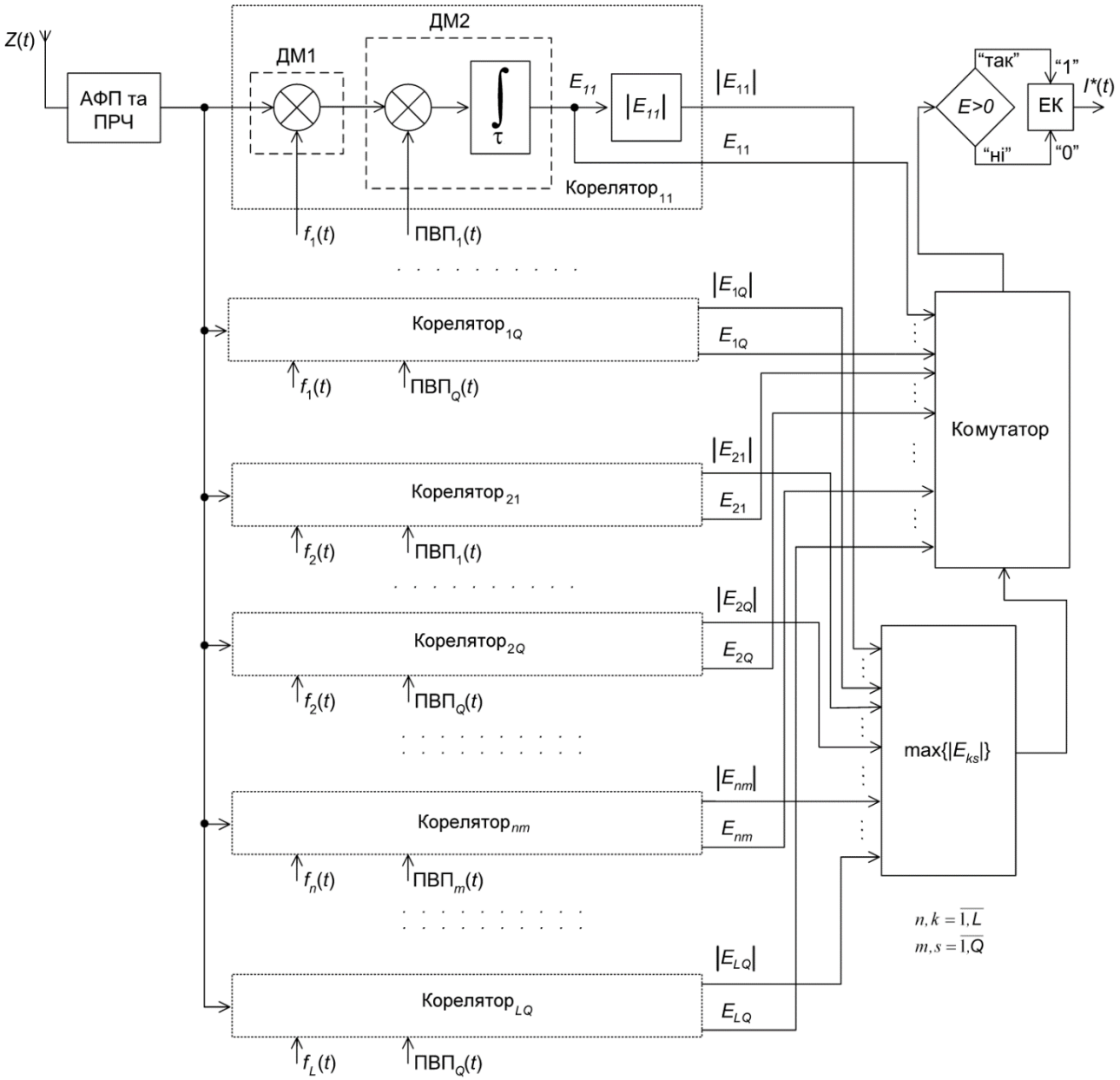

Рис. 4. Структурна схема приймальної апаратури несанкціонованого користувача для здійснення атак К-дії

Введемо показник ефективності атак К-дії на фізичному рівні системи DSSS − імовірність правильного прийому несанкціонованим користувачем одного біта конфіденційної інформації P_B. Зі збільшенням P_B ефективність атак К-дії збільшується (з позицій несанкціонованого користувача), а ефективність протидії атакам К-дії зменшується (з позицій ТЗІ санкціонованого користувача).

Значення P_B може бути оцінене з використанням формули повної імовірності таким чином:

$$P_B = 0,5(1-\alpha)+(1-P_0)\alpha\,, \qquad (1)$$

де P_0 − імовірність бітової помилки на виході системи здійснення атак, тобто приймальної апаратури несанкціонованого користувача.

Вираз (1) було отримано з таких міркувань. Умовна імовірність того, що при передаванні деякого біту конфіденційної інформації сигнал у системі DSSS буде характеризуватись такою комбінацією частотної позиції та опорного сигналу ПВП, для якої у системі здійснення атак (рис. 4) немає відповідного узгодженого корелятора, дорівнює (1–α). Тоді через стохастичність результатів кореляційної обробки у існуючих неузгоджених з сигналом кореляторах та детерміновану схему прийняття рішень про прийнятий бінарний символ імовірність правильного прийому одного біта становитиме 0,5. Умовна імовірність того, що при передаванні деякого біту конфіденційної інформації сигнал у системі DSSS буде характеризуватись такою комбінацією частотної позиції та опорного сигналу ПВП, для якої у системі здійснення атак присутній відповідний узгоджений корелятор, дорівнює α. При цьому імовірність правильного прийому одного біта становитиме (1–P_0).

Імовірність бітової помилки P_0 на виході приймальної апаратури несанкціонованого користувача у першу чергу пов'язана з імовірністю помилки ідентифікації біортогонального сигналу P_S. Можна показати [15, с. 258], що

$$P_0 = \frac{M/2}{M-1}P_S\,, \qquad (2)$$

де M − загальна кількість біортогональних сигналів, з якими узгоджена приймальна апаратура.

У контексті аналізу приймальної апаратури несанкціонованого користувача значення $M/2$ становить собою кількість кореляторів:

$$M/2 = QL\alpha\;;\; M = 2QL\alpha\,. \qquad (3)$$

Значення P_S для розглянутого оптимального розрізнювача біортогональних сигналів з урахуванням [14, с. 91], виграшу при обробці широкосмугового сигналу системи DSSS та формули (3) становить:

$$P_S = 1-\frac{1}{\sqrt{2\pi}}\int_0^{\infty}\left[2\Phi(z)-1\right]^{QL\alpha-1}\exp\left[-\frac{1}{2}\left(z-\sqrt{\theta}\right)^2\right]dz\,, \quad (4)$$

де $\theta = 2Nh^2 = 2NLh^2_{DSSS} = 2Bh^2_{DSSS}$.

Для визначення P_S у виразі (4) використовуються такі параметри та позначення:

1) $h^2 = \langle P_{DSSS}\rangle / \langle P_{\eta 1}\rangle$ − співвідношення сигнал/шум у смузі частот шумового (прямокутного) еквіваленту однієї частотної позиції широкосмугового сигналу у системі DSSS, де $\langle P_{DSSS}\rangle$ − середня потужність широкосмугового сигналу у системі DSSS, $\langle P_{\eta 1}\rangle$ − середня потужність завад у смузі частот шумового (прямокутного) еквіваленту однієї частотної позиції широкосмугового сигналу у системі DSSS, $\langle P_{\eta 1}\rangle = \Omega_0 \Delta f_1$, де Ω_0 − спектральна щільність потужності завад (білий гаусівський шум), Δf_1 − ширина смуги частот шумового (прямокутного) еквіваленту однієї частотної позиції широкосмугового сигналу у системі DSSS, яка чисельно дорівнює швидкості модуляції сигналу у системі DSSS (при моделюванні завад $\Omega_0 = 2\sigma_\eta^2 / F_Д$, де σ_η^2 − дисперсія некорельованих відліків нормально розподіленого випадкового процесу, які є моделлю завад, а $F_Д$ − частота дискретизації);

2) $h^2_{DSSS} = \langle P_{DSSS}\rangle / \langle P_\eta\rangle = \langle P_{DSSS}\rangle / L\langle P_\eta\rangle = h^2/L$ − співвідношення сигнал/шум у смузі частот шумового (прямокутного) еквіваленту широкосмугового сигналу у системі DSSS, де $\langle P_\eta\rangle$ − середня потужність завад у смузі частот шумового (прямокутного) еквіваленту широкосмугового сигналу у системі DSSS;

3) $B = NL$ − база сигналу у системі DSSS;

4) $\Phi(z) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{z}\exp\left(-x^2/2\right)dx$ − інтеграл імовірності.

За умов апріорної невизначеності зміни частотних позицій сигналу у системі DSSS апаратура несанкціонованого користувача (рис. 4) здійснюватиме аналіз сигналів у всьому діапазоні частот, в якому знаходяться частотні позиції сигналу системи DSSS. У цьому випадку обробка сигналів здійснюється при дії завад з середньою потужністю $\langle P_\eta\rangle$ та доцільно використовувати h^2_{DSSS}. За умов відсутності апріорної невизначеності щодо частотних позицій сигналу у системі DSSS (частинний випадок) апаратура несанкціонованого користувача здійснюватиме обробку сигналів зосереджено у смузі частот однієї частотної позиції. У цьому випадку обробка сигналів здійснюється при дії завад з середньою потужністю $\langle P_{\eta 1}\rangle$ та доцільно використовувати h^2.

З урахуванням (2) та (3) імовірність бітової помилки P_0 на виході приймальної апаратури несанкціонованого користувача становить (5).

$$P_0 = \frac{QL\alpha}{2QL\alpha - 1}\left[1 - \frac{1}{\sqrt{2\pi}}\int_0^{\infty}\left[2\Phi(z)-1\right]^{QL\alpha-1}\exp\left[-\frac{1}{2}\left(z-\sqrt{\theta}\right)^2\right]dz\right], \quad (5)$$

З урахуванням (1) та (5) імовірність правильного прийому одного біта конфіденційної інформації P_B приймальною апаратурою несанкціонованого користувача становить (6)

$$P_B = \frac{1-\alpha}{2} + \alpha\left\{1 - \frac{QL\alpha}{2QL\alpha - 1}\left[1 - \frac{1}{\sqrt{2\pi}}\int_0^{\infty}\left[2\Phi(z)-1\right]^{QL\alpha-1}\exp\left[-\frac{1}{2}\left(z-\sqrt{\theta}\right)^2\right]dz\right]\right\}. \quad (6)$$

Якщо сторона здійснення атак не обмежена за ресурсними можливостями ($\alpha = 1$), то з (6) маємо

$$P_B = 1 - \frac{QL}{2QL-1}\left[1 - \frac{1}{\sqrt{2\pi}}\int_0^{\infty}\left[2\Phi(z)-1\right]^{QL-1}\exp\left[-\frac{1}{2}\left(z-\sqrt{\theta}\right)^2\right]dz\right]. \quad (7)$$

Оцінки ефективності атак К-дії на фізичному рівні системи DSSS (6) та (7) дають оцінку значення P_B "зверху", тобто найбільш песимістичну оцінку з позицій захищеності інформації, оскільки вони отримані з позицій аналізу оптимального розрізнювача біортогональних сигналів, який використовує сторона здійснення атак. Окрім того, система використовуваних СКК на основі ПВП, як правило, не є повністю ортогональною (для одноканальної системи DSSS необхідне дотримання вимог лише до АКФ кожної СКК), а неортогональність системи СКК негативно впливає на точність розрізнення цих СКК у оптимальному розрізнювачі біортогональних сигналів.

При відсутності завад ($h^2, h^2_{DSSS} \to \infty$ та $\theta \to \infty$) ефективність атак К-дії на фізичному рівні системи DSSS прямує до значення $\lim\limits_{\theta\to\infty} P_B = \frac{1-\alpha}{2} + \alpha = \frac{1+\alpha}{2}$, а при не обмежених ресурсних можливостях сторони здійснення атак $\lim\limits_{\substack{\theta\to\infty \\ \alpha\to 1}} P_B = 1$.

На рис. 5 наведені залежності $P_B\left(h^2_{DSSS}\right)$ для різних значень бази сигналу B у системі DSSS при використанні не обмеженої за ресурсними можливостями системи здійснення атак ($\alpha = 1$) для випадків використання СКК на основі ПВП довжини N за умов їх обмеженої кількості Q у системі СКК, що визначається вимогами до їх АКФ (див. рис. 2; кількість СКК у системі було взято удвічі більшою з урахуванням можливих ізоморфних форм ПВП, коли одна і та сама ПВП може використовуватись як дві різні ПВП, маючи при цьому одну й ту ж саму форму АКФ: при її записі і використанні "зліва направо" та "справа наліво"; інверсно-ізоморфні форми при цьому не враховувалися, оскільки інверсія ПВП визначає значення інформаційного біту, що передається, тому не може бути включеною до системи СКК як окрема СКК):

1) послідовності Баркера ($N = 11$; $Q = 2$; $\max|R| = 1/11$);

2) ПВП з характеристиками $N = 28$; $Q = 8$; $\max|R| = 2/28$;

3) ПВП з характеристиками $N = 11$; $Q = 232$; $\max|R| = 3/11$; ця система ПВП має більшу кількість ПВП у порівнянні з п. 1 завдяки меш жорстким вимогам до бічних пелюсток АКФ та була знайдена автором статті методом прямого перебору послідовностей довжини $N = 11$;

4) ПВП з характеристиками $N = 28$; $Q = 2504$; $\max|R| = 3/28$; ця система ПВП має більшу кількість ПВП у порівнянні з п. 2 завдяки меш жорстким вимогам до викидів бічних пелюсток АКФ та була знайдена автором статті методом прямого перебору послідовностей довжини $N = 28$.

У випадку, коли ресурсні можливості системи здійснення атак є обмеженими ($\alpha < 1$), значення показника P_B при інших рівних умовах будуть нижчими, ніж для не обмеженої за ресурсними можливостями ($\alpha = 1$) системи здійснення атак.

На рис. 6 наведені залежності $P_B(\alpha)$ для різних значень бази сигналу B у системі DSSS та співвідношень сигнал/шум у місці здійснення атак при використанні обмеженої за ресурсними можливостями системи здійснення атак для випадків використання таких систем СКК на основі ПВП:

1) ПВП з характеристиками $N = 11$; $Q = 232$; $\max|R| = 3/11$;

2) ПВП з характеристиками $N = 28$; $Q = 2504$; $\max|R| = 3/28$.

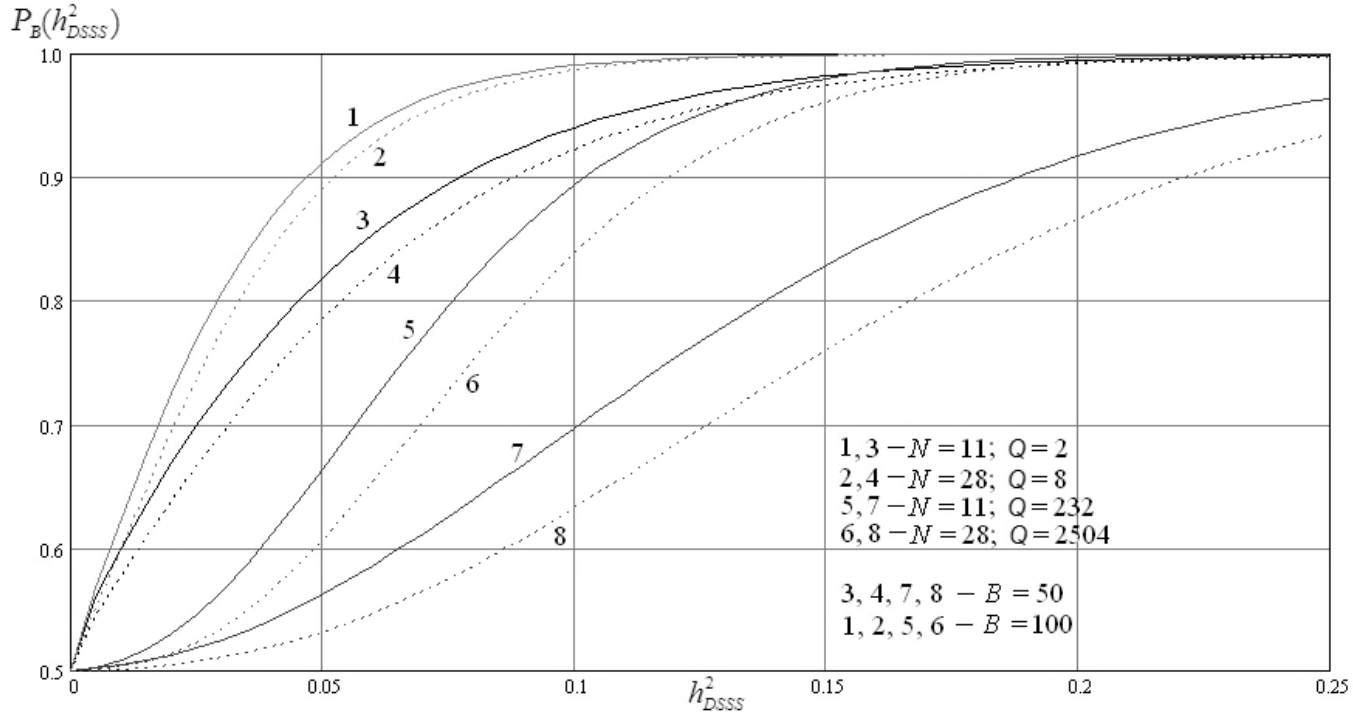

Рис. 5. Залежності ефективності атак К-дії на фізичному рівні системи DSSS від співвідношення сигнал/шум для не обмеженої за ресурсними можливостями системи здійснення атак при використанні різних систем СКК

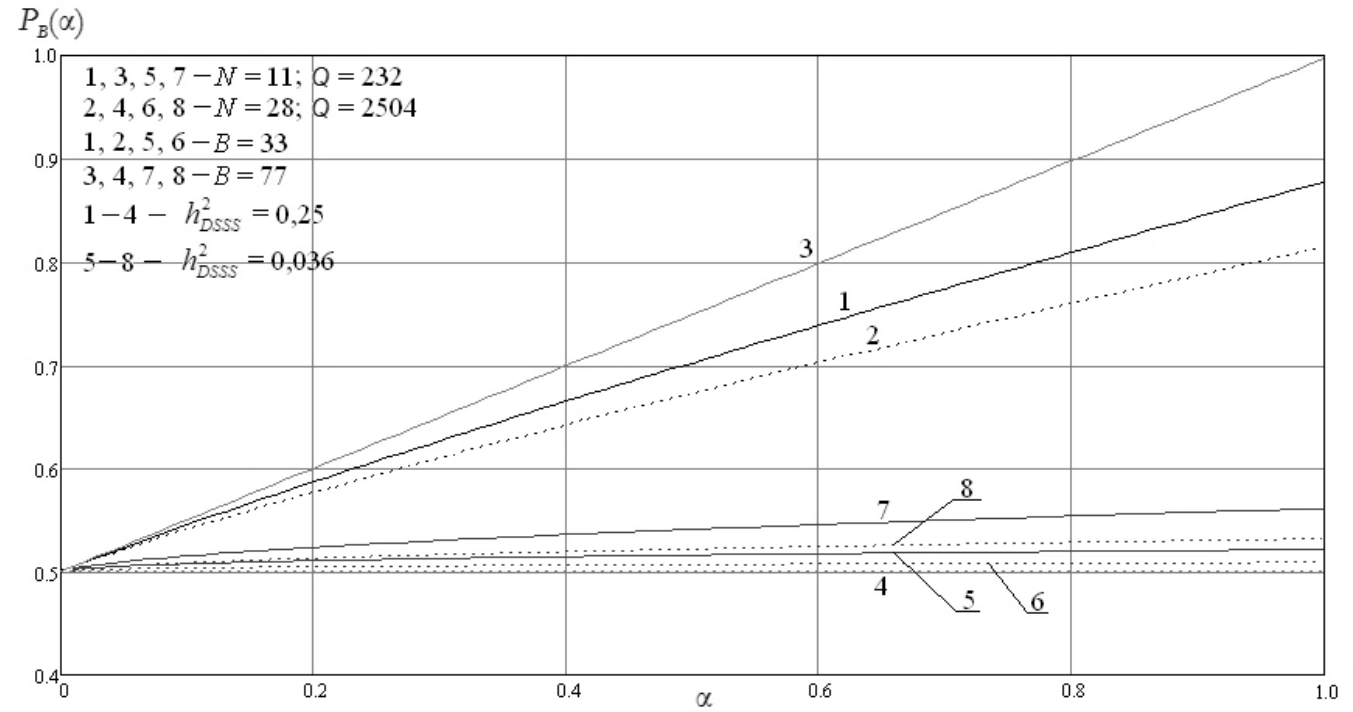

Рис. 6. Залежності ефективності атак К-дії на фізичному рівні системи DSSS від ресурсних можливостей системи здійснення атак при використанні різних систем СКК

ВИСНОВКИ

Проблема відсутності регулярних детермінованих методів синтезу систем бінарних послідовностей будь-якої необхідної довжини з низьким рівнем бічних пелюсток АКФ, яка визначає обмеженість систем СКК для одноканальних телекомунікаційних систем, що працюють за технологією розширення спектру DSSS, визначає такі особливості забезпечення конфіденційності передавання інформації при використанні цієї технології для ТЗІ на фізичному рівні телекомунікаційних систем.

1. Відносно несуттєве зменшення вимог до

АКФ ПВП, тобто збільшення допустимого значення $\max|R|$, призводить до можливості синтезу систем ПВП значно більшого об'єму Q: при довжині ПВП $N = 11$ збільшення допустимого значення $\max|R|$ у 3 рази (з 1/11 до 3/11) дає можливість використовувати систему ПВП у 116 раз більшого об'єму Q (2 та 232 відповідно); при довжині ПВП $N = 28$ збільшення допустимого значення $\max|R|$ у 1,5 рази (з 2/28 до 3/28) дає можливість використовувати систему ПВП у 313 раз більшого об'єму Q (8 та 2504 відповідно). Таким чином, при збільшенні довжини використовуваних ПВП N незначне зменшення вимог до їх кореляційних властивостей призводить до можливості використання суттєво більшого об'єму системи ПВП Q, що у свою чергу суттєво підвищує конфіденційність передавання інформації у системі DSSS (рис. 5).

2. Суттєвий виграш у конфіденційності передавання інформації у системі DSSS від використання систем ПВП більшого об'єму спостерігається при відносно малих співвідношеннях сигнал/шум (рис. 5), тому невиправдане збільшення енергетики каналів зв'язку системи DSSS (наприклад, забезпечення у такій системі великих значень запасу на завмирання) є недоцільним з точку зору ТЗІ та зменшує конфіденційність передавання інформації при здійсненні атак.

3. Великі значення бази сигналу B сприятливо впливають на енергетичну прихованість системи зв'язку, але у той же час з точки зору забезпечення структурної прихованості передавання інформації покращують завадостійкість обробки широкосмугових сигналів у системі DSSS як для санкціонованого користувача, так і для системи здійснення атак, яка використовує розглянутий у статті оптимальний розрізнювач біортогональних сигналів. Тому для підвищення конфіденційності передавання інформації у системі DSSS доцільно використовувати великі значення бази сигналу за умов, коли вони реалізовані завдяки великим значенням довжини ПВП N (при великому значенні об'єму використовуваних ПВП Q), а не завдяки лише кількості частотних позицій L.

4. Ефективність атак К-дії на фізичному рівні системи DSSS має приблизно лінійну функціональну залежність від ресурсних можливостей системи здійснення атак (рис. 6).

ЛІТЕРАТУРА

[1]. В.П. Бабак, А.Я. Білецький, *Детерміновані сигнали і спектри*: навч. посіб. для студ. вищ. навч. закл., К.: Техніка, 2003, 455 с.

[2]. А. Белецкий, "Оптимальные Уолша и Уолше-подобные базисы дискретного преобразования Фурье", *Захист інформації*, Т. 20, № 2, С. 104-119, 2018.

[3]. С. Евсеев, С. Остапов, И. Белодед, "Исследования свойств гибридных крипто-кодовых конструкций", *Захист інформації*, Т. 19, № 4, С. 278-290, 2017.

[4]. А.А. Смирнов, *Методы и средства компьютерной стеганографии с применением сложных дискретных сигналов для защиты информации в компьютерных сетях:* монография, Кировоград: "КОД", 2012, 352 с.

[5]. В.Е. Гантмахер, Н.Е. Быстров, Д.В. Чеботарев, *Шумоподобные сигналы. Анализ, синтез, обработка,* СПб.: Наука и техника, 2005. 400 с.

[6]. Ю.В. Матиясевич, *Десятая проблема Гильберта,* М.: Наука: Физико-математическая литература, 1993, 223 с.

[7]. Project "Peak Sidelobe (PSL) Level of Binary Sequences Research Kit" [Electronic resource]. Access: https://github.com/Gluttton/PslRK/blob/master/Reports/LowPslCodes.xml.

[8]. Maryam Amin Nasrabadi, Mohammad Hassan Bastani, "A Survey on the Design of Binary Pulse Compression Codes with Low Autocorrelation", in Trends in Telecommunications Technologies (Edited by Christos Bouras), Ch. 3, pp. 39-61, 2010.

[9]. Mark A. Richards, *Fundamentals of Radar Signal Processing, Second Edition*, McGraw-Hill Education, 2014, 656 p.

[10]. C.J. Nunn, G.E. Coxson, "Best-Known Autocorrelation Peak Sidelobe Levels for Binary Codes of Length 71 to 105", *IEEE Trans. Aerosp. Electron. Syst.*, vol. 44, no. 1, pp. 392-395, 2008.

[11]. А.Г. Голубничий, "Правила кодирования и структура обобщенных бинарных последовательностей Баркера", *Проблеми інформатизації та управління*, Т. 4, № 44, С. 20-26, 2013.

[12]. А.Г. Голубничий, "Корреляционные свойства обобщенных бинарных последовательностей Баркера", *Проблеми інформатизації та управління*, Т. 2, № 50, С. 48-55, 2015.

[13]. А.Г. Голубничий, Г.Ф. Конахович, "Мультипликативно комплементарные бинарные сигнально-кодовые конструкции", *Известия высших учебных заведений. Радиоэлектроника*, Т. 61, № 10, С. 551-565, 2018.

[14]. В.А. Борисов, В.В. Калмыков, Я.М. Ковальчук и др., *Радиотехнические системы передачи информации: учеб. пособие для вузов*, М.: Радио и связь, 1990, 304 с.

[15]. Б. Скляр, *Цифровая связь. Теоретические основы и практическое применение*, М.: "Вильямс", 2004, 1104 с.

АНАЛИЗ КОНФИДЕНЦИАЛЬНОСТИ ПЕРЕДАЧИ ИНФОРМАЦИИ В СИСТЕМАХ DSSS В УСЛОВИЯХ ОГРАНИЧЕННОСТИ СИСТЕМ ИСПОЛЬЗУЕМЫХ СИГНАЛЬНО-КОДОВЫХ КОНСТРУКЦИЙ

Техническая защита информации в телекоммуникационных системах может быть реализована на физическом уровне этих систем путём обеспечения энергетической и структурной скрытности передачи информации. К телекоммуникационным технологиям, наиболее подходящим для реализации таких методов защиты информации, принадлежат технологии систем связи с шумоподобными сигналами, в частности технология DSSS (Direct Sequence Spread Spectrum). Обеспечение необходимого уровня структурной скрытности передачи информации при использовании технологии DSSS заключается в том, что в этой технологии используются системы сигнально-кодовых конструкций с достаточно большим количеством сигналов в системе. К каждой из таких сигнально-кодовых конструкций предъявляются требования к их корреляционным свойствам, которые в соответствии с теоремой Винера-Хинчина определяют спектральные характеристики сигналов в телекоммуникационной системе и, как следствие, структурную спектральную и энергетическую скрытность передачи информации. Проблема заключается в том, что регулярные детерминированные методы синтеза систем сигнально-кодовых конструкций с низким уровнем боковых лепестков автокорреляционной функции для произвольной длины сигнально-кодовой конструкции и количества таких сигналов в системе сигналов неизвестны, а сложность этой проблемы синтеза связана с алгоритмической неразрешимостью произвольных алгебраических диофантовых уравнений. В статье проанализирована конфиденциальность передачи информации на физическом уровне телекоммуникационных систем DSSS при условии использования ряда известных синтезированных систем сигнально-кодовых конструкций с низким уровнем боковых лепестков автокорреляционной функции для случая, когда несанкционированным пользователем осуществляются атаки К-действия с использованием оптимальных для него по результативности методов обработки сигналов (оптимального различителя биортогональных сигналов).

Ключевые слова: скрытность передачи информации, конфиденциальность, атаки на физическом уровне телекоммуникационной системы, системы связи с шумоподобными сигналами, технология DSSS, псевдослучайные последовательности.

ANALYSIS OF CONFIDENTIALITY OF INFORMATION TRANSFER IN DSSS SYSTEMS IN CONDITIONS OF LIMITED SYSTEMS OF USED SIGNAL CONSTRUCTIONS

Information security in telecommunications can be provided at the physical level of telecommunication systems by means of energy and structural secrecy of information transfer. Spread-spectrum telecommunications, in particular the DSSS (Direct Sequence Spread Spectrum) technique, are the most suitable for the implementation of such approach to information security. Ensuring the necessary level of structural secrecy of information transfer using DSSS technique is that this technique uses systems of signal constructions with a sufficiently large number of signals in the system. There are requirements to correlation properties of each such signal construction, because in accordance with the Wiener-Khinchin theorem they determine the spectral characteristics of signals in a telecommunication system and, as a result, the structural spectral and energy secrecy of information transfer. The problem boils down to the fact that the systematic deterministic methods for synthesizing systems of signal constructions with a low peak sidelobe level of the autocorrelation function for the case of an arbitrary length of signal constructions and the number of ones in the system of signals are unknown, and the complexity of this problem is associated with an algorithmic undecidability of arbitrary algebraic Diophantine equations. The confidentiality of information transfer at the physical level of DSSS telecommunication systems while using some known systems of signal constructions with a low peak sidelobe level of the autocorrelation function and in the case of attacks, which are performed by an unauthorized user by means of optimal signal processing methods (optimal detection of biorthogonal signals), is analyzed in the article.

Keywords: secrecy of information transfer, confidentiality, attacks at the physical level of telecommunication system, spread-spectrum telecommunications, DSSS technique, pseudorandom sequences.

Голубничий Олексій Георгійович, кандидат технічних наук, доцент, доцент кафедри телекомунікаційних систем Національного авіаційного університету.
E-mail: a.holubnychyi@nau.edu.ua.
Голубничий Алексей Георгиевич, кандидат технических наук, доцент, доцент кафедры телекоммуникационных систем Национального авиационного университета.
Holubnychyi Alexei, PhD in Eng., Associate Professor at the Department of Telecommunication Systems, National Aviation University.