УДК 004.056.53

О.Г. Голубничий

АНАЛІЗ АТАК К-ДІЇ НА ФІЗИЧНОМУ РІВНІ ШИРОКОСМУГОВОЇ РАДІОСИСТЕМИ ПРИ МОЖЛИВОСТІ МОДИФІКАЦІЇ ПРИЙМАЛЬНОГО ПРИСТРОЮ

Постановка проблеми та її зв'язок з науковими та практичними завданнями. Висока прихованість передавання інформації [1, с. 206–222; 2, 3] разом з інтенсивним впровадженням широкосмугових технологій у існуючу інфраструктуру інформаційних систем визначає перспективність використання широкосмугових методів передачі у спеціальних телекомунікаційних системах (мережах), спеціальних телекомунікаційних системах (мережах) подвійного призначення у складі Національної системи конфіденційного зв'язку [4]. Важливим є аналіз атак, метою яких є порушення конфіденційності інформації при використанні таких методів передавання.

Аналіз останніх досліджень і публікацій. Роботи, присвячені проблемам захищеного передавання інформації у широкосмугових системах в основному пов'язані з синтезом технологій такого типу передавання [5, 6] та сигнально-кодових конструкцій для систем такого типу [7–9].

Постановка завдання. Метою статті є аналіз загроз порушення конфіденційності інформації, які можуть бути реалізовані на фізичному рівні широкосмугової радіосистеми при можливості доступу несанкціонованого користувача до системи обробки сигналів приймального пристрою та її модифікації (порушення рівня послуги НЦ-1 НД ТЗІ [10]).

Виклад основного матеріалу дослідження. У статті аналіз атак К-дії проаналізовано на прикладі широкосмугової радіосистеми передавання конфіденційної інформації з технологією розширення спектру DS-FHSS, в якій широкосмуговий сигнал (ШСС) є сигналом з частотно-фазовою маніпуляцією (ЧФМ), для передавання кожного біту повідомлення використовується комбінація "бінарна ПВП та частотна позиція", яка для кожного біту повідомлення визначається алгоритмом слідування цих комбінацій та ключем, що визначає параметри алгоритму. Несні частотних позицій модулюються елементами ПВП з використанням модуляції BPSK (характеризується високою енергетичною прихованістю).

Структура ШСС може бути представлена у вигляді матриці (рис. 1,а), яка показує, що при передаванні *i*-го біта конфіденційного повідомлення на інтервалі часу τ_i для розширення спектру інформаційного сигналу використовується псевдовипадкова послідовність (ПВП) з порядковим номером $X11_i$ з ансамблю ПВП об'ємом V та частотна позиція f з порядковим номером $X21_i$ з множини частотних позицій, загальна кількість яких становить D. Система порядкових номерів $X11_i$ та $X21_i$ визначається алгоритмом зміни комбінацій ПВП та частотної позиції ЧФМ ШСС, який розглянуто нижче.

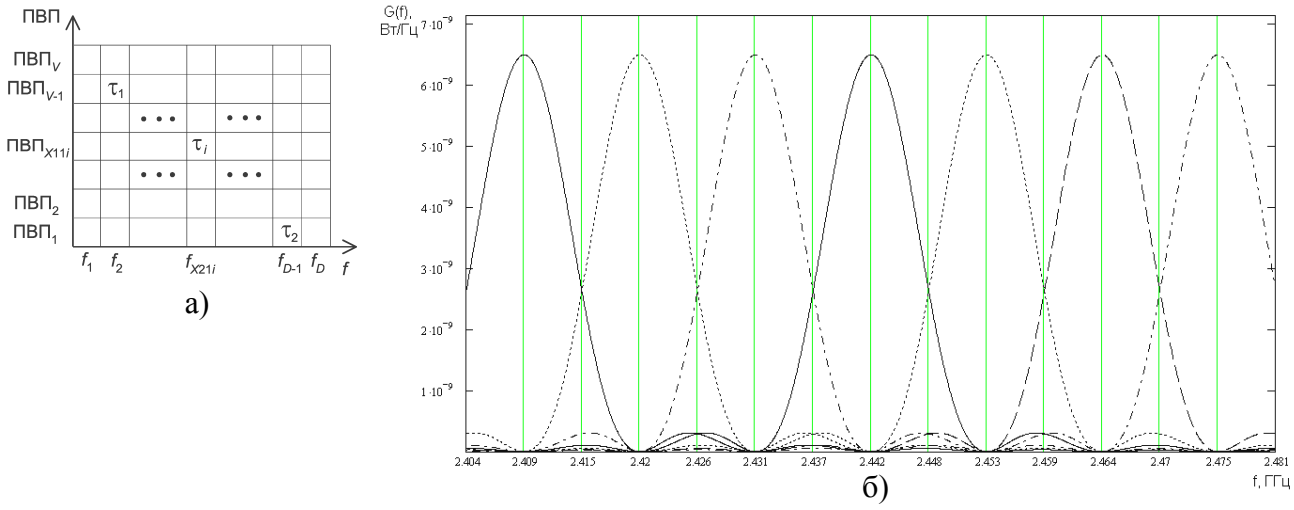


Рис. 1. Структура ЧФМ ШСС (а) та його спектр (б)

Голубничий О. Г. Аналіз атак К-дії на фізичному рівні широкосмугової радіосистеми при можливості модифікації приймального пристрою / О. Г. Голубничий // Сучасний захист інформації. – К.: ДУІКТ, 2011. – № 4. – С. 42–54.

Для здійснення аналізу було проведено комп'ютерне моделювання широкосмугової радіосистеми, особливістю якого є те, що можливі значення частотних позицій встановлюються таким чином, що нижня границя смуги шумового еквіваленту ЧФМ ШСС дорівнює або мінімально перевищує нижню границю ISM діапазону (2,4000...2,4835 ГГц), частотні позиції кратні значенню половини швидкості модуляції, що забезпечує нерозривність фази ЧФМ ШСС, інтервал між сусідніми частотними позиціями ЧФМ ШСС дорівнює швидкості модуляції. Інші параметри системи такі: швидкість передавання інформації R = 1 Мбіт/с; використовується ансамбль бінарних ПВП довжини N = 11 об'ємом V = 232 (містить 2 ПВП Баркера з $\max\{|R_{АКФ}|\} = 1/11$, 28 ПВП з $\max\{|R_{АКФ}|\} = 2/11$ та 202 ПВП з $\max\{|R_{АКФ}|\} = 3/11$, де $\max\{|R_{АКФ}|\}$ − максимальне значення модуля бічних пелюсток автокореляційної функції; склад ансамблю ґрунтується на основі припущення, що мінімальний об'єм ансамблю ПВП для захищених широкосмугових радіосистем становить $V_{min} = N^2$ [1]); швидкість модуляції несної $R_0 = R \cdot N$ = 11 Мсимв/с; кількість частотних позицій ЧФМ ШСС D = 7; значення частотних позицій: f_1 = 2,409 ГГц; f_2 = 2,42 ГГц; f_3 = = 2,431 ГГц; f_4 = 2,442 ГГц; f_5 = 2,453 ГГц; f_6 = 2,464 ГГц; f_7 = 2,475 ГГц (при вказаних параметрах ЧФМ ШСС буде зосереджено у смузі частот 2,4035...2,4805 ГГц за критерієм шумового або прямокутного еквіваленту); база ЧФМ ШСС $B = N \cdot D$ = 77; загальна кількість комбінацій "бінарна ПВП та частотна позиція" ЧФМ ШСС, що визначає ступінь структурної прихованості системи $V \cdot D$ = 1624; ключ, що визначає початкові параметри генераторів псевдовипадкових чисел у алгоритмі зміни комбінацій "бінарна ПВП та частотна позиція" ЧФМ ШСС: $X1_1$ = 3241793142; C1 = 1786885589; $X2_1$ = 3544621582; C2 = 745692845 (використані генератори з процедури А' ГОСТ Р 34.10-94 [11], розглянуті нижче); амплітуда ЧФМ ШСС 1 В; співвідношення сигнал/завади за потужністю h^2 = 0,25; модель конфіденційного повідомлення − псевдовипадкова послідовність статистично незалежних рівноймовірних бінарних символів ("0" та "1").

Вибір вищезазначених параметрів фізичного рівня було обрано таким чином, щоб вони були максимально наближені до параметрів системи безпроводового зв'язку IEEE 802.11, а спектр ЧФМ ШСС максимально використовував діапазон частот ISM 2,4000...2,4835 ГГц. Структура спектру (спектральної щільності потужності) ЧФМ ШСС при наведених вище параметрах моделювання наведена на рис. 1,б.

Алгоритм зміни комбінацій ПВП та частотної позиції ЧФМ ШСС. Для визначення порядкових номерів бінарних ПВП у ансамблі та частотних позицій, комбінації яких використовується для передавання кожного біта застосовуються два масиви рівномірно розподілених чисел, сформованих на основі лінійного конгруентного давача процедури А' ГОСТ Р 34.10-94 [11]. Алгоритм формування порядкових номерів $X11_i$ та $X21_i$ при використанні цієї процедури полягає у наступному: визначення порядкового номеру бінарної ПВП у ансамблі для i-го біта повідомлення: $X11_i = 1 + X1_i \bmod V$; де $X1_i = (97781173\ X1_{i-1} + C1) \bmod 2^{32}$, $i > 1$; числа $0 < X1_1 < 2^{32}$ та непарне $0 < C1 < 2^{32}$ − елементи ключа для поточного сеансу зв'язку; визначення порядкового номеру частотної позиції для i-го біта повідомлення: $X21_i = 1 + X2_i \bmod D$; де $X2_i = (97781173\ X2_{i-1} + C2) \bmod 2^{32}$, $i > 1$; числа $0 < X2_1 < 2^{32}$ та непарне $0 < C2 < 2^{32}$ − елементи ключа для поточного сеансу зв'язку. Таким чином для сеансу зв'язку використовується ключ $\{X1_1; C1; X2_1; C2\}$, який може бути представлено 126-бітовою кодовою комбінацією (32 біт $X1_1$ + 31 біт непарні $C1$ + 32 біт $X2_1$ + 31 біт непарні $C2$).

Формування ЧФМ ШСС. Структурна схема передавального пристрою показана на рис. 2,а. У модуляторі 1 (Мод 1) на кожному інтервалі часу τ_i (тривалість передавання одного біта) здійснюється розширення спектру сигналу конфіденційного повідомлення $I(t)$ шляхом перемноження сигналу i-го біту конфіденційного повідомлення $I(t)$ та сигналу $ПВП_{X11i}(t)$. На рис. 3 показані часові діаграми реалізацій сигналів $I(t)$, ПВП(t) та сигналу на виході модулятора 1 на інтервалі часу $t \in [0; 4 \cdot 10^{-6}]$, які були отримані при моделюванні.

Голубничий О. Г. Аналіз атак К-дії на фізичному рівні широкосмугової радіосистеми при можливості модифікації приймального пристрою / О. Г. Голубничий // Сучасний захист інформації. – К.: ДУІКТ, 2011. – № 4. – С. 42–54.

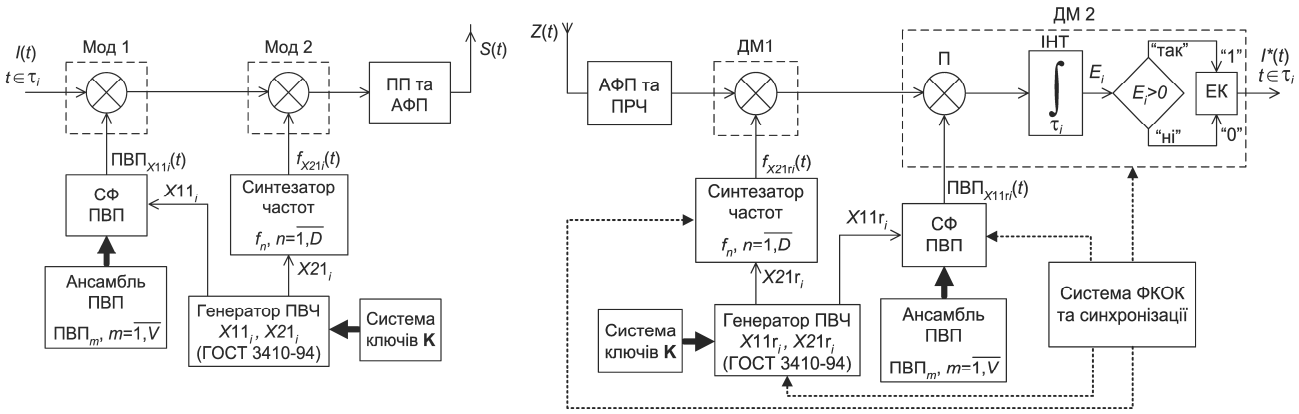


Рис. 2. Структурні схеми передавального (а) та приймального (б) пристроїв

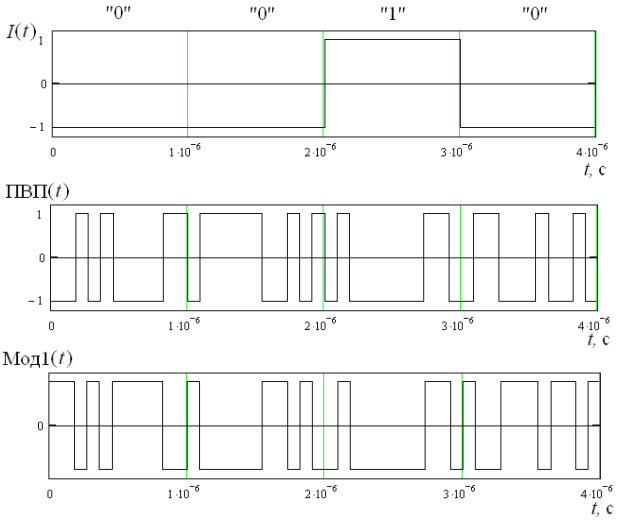


Рис. 3. Часові діаграми реалізацій сигналів конфіденційного повідомлення $I(t)$, ПВП(t), сигналу на виході модулятора 1

При зазначених вище параметрах моделювання номери бінарних ПВП та самі ПВП у ансамблі $X11_1$ = 71 (-1-11-11-1-1-1-1-111, $\max\{|R_{АКФ}|\} = 3/11$); $X11_2$ = 225 (-111111-1-11-11, $\max\{|R_{АКФ}|\} = 3/11$); $X11_3$ = 117 (-11-1-1-1-1-1-1-111-1, $\max\{|R_{АКФ}|\} = 2/11$); $X11_4$ = 177 (-111-1-1 -11-1-11-1, $\max\{|R_{АКФ}|\} = 3/11$). Схема формування ПВП (СФ ПВП) почергово виконує вибірку з ансамблю ПВП таких ПВП, номер яких у ансамблі відповідає поточному номеру $X11_i$ при передаванні i-го біту конфіденційного повідомлення. У модуляторі 2 (Мод 2) на кожному інтервалі часу τ_i (тривалість передавання одного біта) реалізується модуляція BPSK несної поточної частотної позиції f_{X21i} сигналом з виходу модулятора 1 (рис. 3). На рис. 4,а показана часова діаграма реалізації ЧФМ ШСС на інтервалі часу $t \in \left[2{,}995 \cdot 10^{-6}; 3{,}005 \cdot 10^{-6}\right]$ (0,01 мкс), отримана при моделюванні. При $t = 3 \cdot 10^{-6}$ с відбувається завершення передачі 3-го біту конфіденційного повідомлення (“1”) і початок передачі 4-го біту повідомлення (“0”).

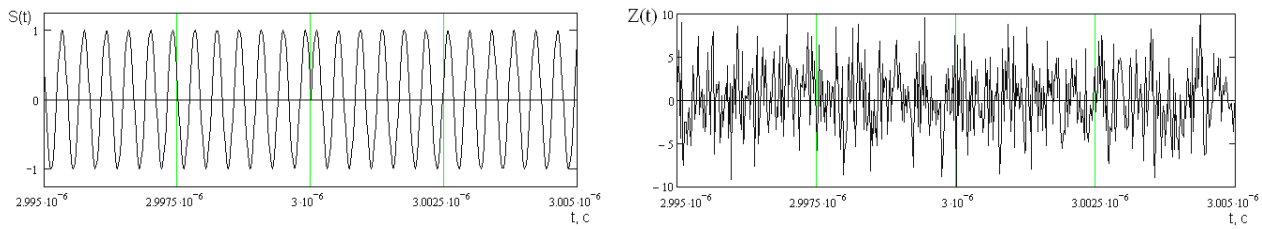


Рис. 4. Часова діаграма ЧФМ ШСС (а) та суміші ЧФМ ШСС та завад при $h^2 = 0{,}25$ (б)

При наведених вище параметрах моделювання для передавання 3-го біту була використана ПВП з порядковим номером 117 та частотна позиція f_1 = 2,409 ГГц, а для передавання 4-го біту − ПВП з порядковим номером 177 та частотна позиція f_3 = 2,431 ГГц. Синтезатор частот формує сигнал несної поточної частотної позиції, номер якої визначається поточним номером $X21_i$ при передаванні i-го біту конфіденційного повідомлення. При зазначених вище параметрах моделювання номери та відповідні їм значення частотних позицій $X21_1 = 6$ (f_6 = 2,464 ГГц); $X21_2 = 7$ (f_7 = 2,475 ГГц); $X21_3 = 1$ (f_1 = = 2,409 ГГц); $X21_4 = 3$ (f_3 = 2,431 ГГц). Генератор псевдовипадкових чисел (ПВЧ) формує псевдовипадкові числа $1 \le X11_i \le V$, які визначають порядковий номер бінарної ПВП у ансамблі для i-го біта конфіденційного повідомлення та псевдовипадкові числа $1 \le X21_i \le D$, які визначають порядковий номер частотної позиції для i-го біта конфіденційного повідомлення. Початкові параметри генератора ПВЧ для кожного сеансу зв'язку становлять систему ключів **К**. Алгоритм формування чисел $X11_i$ та $X21_i$ було розглянуто вище. Підсилювач потужності (ПП) та антенно-фідерний пристрій (АФП) призначені для підвищення потужності ЧФМ ШСС до заданого рівня, узгодження вихідних кіл передавального пристрою з антенною системою, випромінювання сигналу у середовище розповсюдження сигналу. При моделюванні ПП та АФП не моделювались, сигнально-завадова обстановка (співвідношення сигнал/завади) у місці розташування приймального пристрою моделювалась шляхом встановлення необхідної потужності завад при якій забезпечується задане співвідношення сигнал/завади, коефіцієнт передачі ЧФМ ШСС у середовищі розповсюдження дорівнює 1, затримка розповсюдження сигналу відсутня, амплітудно-частотна (АЧХ) та фазо-частотна (ФЧХ) характеристики каналу ідеальні − АЧХ "прямокутна" з необмеженою смугою пропускання, лінійна ФЧХ з кутом нахилу 45^0. Зазначені обмеження моделювання суттєвим чином зменшують час машинного моделювання та не виявляють високих вимог до апаратного забезпечення ЕОМ. У той же час ці обмеження при поставленій меті моделювання суттєво не впливають на результати аналізу за допомогою моделювання прихованої широкосмугової радіосистеми.

Обробка ЧФМ ШСС. Приймальний пристрій побудований за схемою оптимального кореляційного приймача бінарних сигналів з когерентним детектуванням високочастотного сигналу (рис. 2, б).

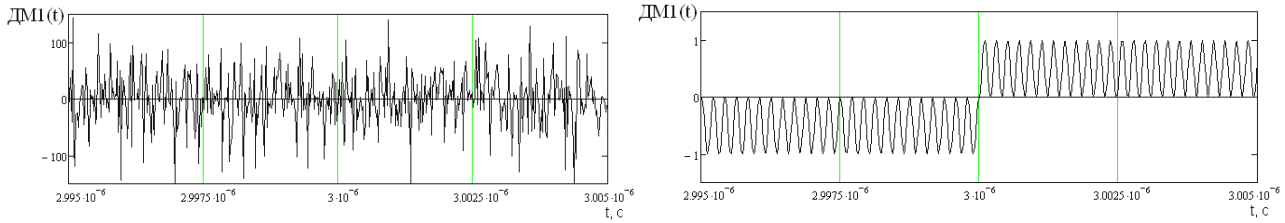
Проаналізуємо процеси обробки ЧФМ ШСС у приймальному пристрої для випадків:

1) санкціонованого користувача (користувачу відома система ключів К);

2) несанкціонованого користувача (користувачу невідома система ключів К, для здійснення спроби несанкціонованого доступу використовується випадковим чином обрана система ключів, можлива модифікація приймального пристрою).

Аналіз складу та функціонування приймального пристрою для випадку санкціонованого користувача. Антенно-фідерний пристрій (АФП) та підсилювач радіочастоти (ПРЧ) призначені для приймання сигналу з середовища розповсюдження сигналу, узгодження антенної системи з вхідними колами приймального пристрою, підвищення потужності ЧФМ ШСС до необхідного для подальшої обробки рівня. При моделюванні зазначені елементи не моделювались аналогічно до ПП та АФП у передавальному пристрої. При моделюванні сигнально-завадової обстановки була використана модель завад наближена за статистичними властивостями до білого гауссівського шуму (прямокутний спектр з заданою спектральною щільністю потужності у смузі частот 0...49,61 ГГц). Було використане таке нормування відліків шуму (масиву нормально розподілених псевдовипадкових чисел з нульовим середнім), щоб у смузі частот шумового (прямокутного) еквіваленту ЧФМ ШСС забезпечувалося задане співвідношення сигнал/завади (h^2 = 0,25). Часова діаграма реалізації суміші $Z(t)$ ЧФМ ШСС та завад на вході приймача при $h^2 = 0{,}25$ на інтервалі часу $t \in \left[2{,}995 \cdot 10^{-6}; 3{,}005 \cdot 10^{-6}\right]$ (0,01 мкс) показана на рис. 4,б. У демодуляторі 1 (ДМ1) здійснюється когерентне детектування сигналу $Z(t)$, що приймається. Демодуляція у ДМ1 реалізується шляхом перемноження на кожному інтервалі

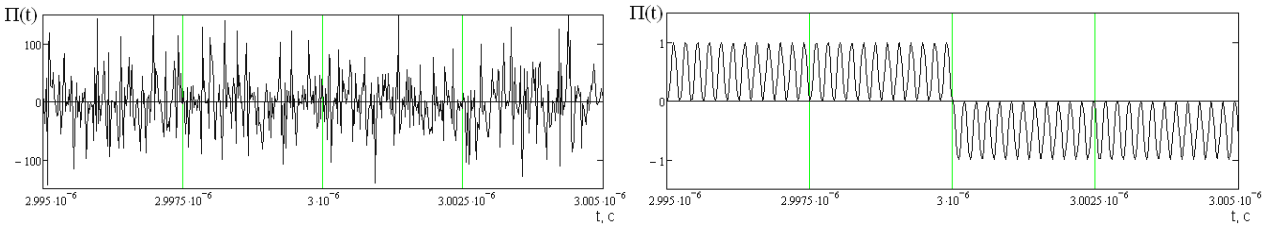
часу τ_i сигналу $Z(t)$ на сигнал несної частотної позиції f_{X21ri}, яка відтворюється у приймальному пристрої (опорне когерентне коливання). Сигнал несної частотної позиції f_{X21ri} формується синтезатором частот відповідно до алгоритму зміни частотних позицій ЧФМ ШСС та системи ключів К. Для санкціонованого користувача в умовах штатної експлуатації системи зв'язку (відсутні експлуатаційні відмови, санкціонований користувач використовує коректну систему ключів К) порядок формування та значення псевдовипадкових чисел $X21r_i$, які генеруються генератором ПВЧ приймального пристрою співпадають з порядком формування та значеннями псевдовипадкових чисел $X21_i$, які генеруються генератором ПВЧ передавального пристрою. При цьому $X21r_i = X21_i$ та $f_{X21ri} = f_{X21i}$. Часові діаграми реалізації сигналу на виході ДМ1 при $h^2 = 0{,}25$ та при відсутності завад ($h^2 \to \infty$) показані на рис. 5. Обидві реалізації були отримані при моделюванні та показані на інтервалі часу $t \in \left[2{,}995 \cdot 10^{-6}; 3{,}005 \cdot 10^{-6}\right]$ (0,01 мкс) аналогічно інтервалу часу на рис. 4.



а) б)

Рис. 5. Часові діаграми сигналів на виході ДМ1: а) – при $h^2 = 0{,}25$; б) – при відсутності завад

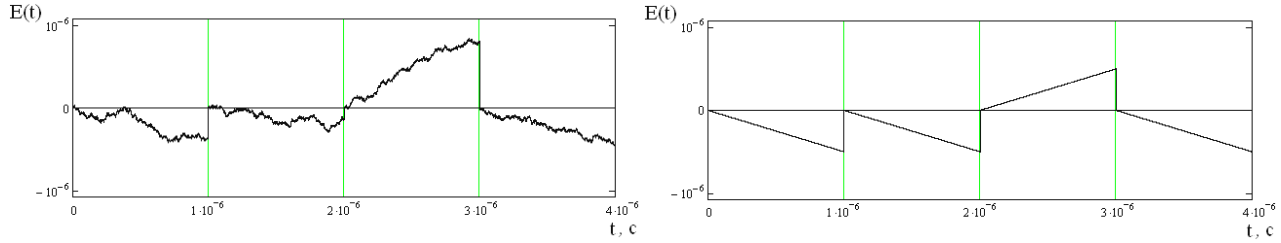
У демодуляторі 2 (ДМ2) здійснюється кореляційна обробка отриманих після ДМ1 сигналів. ДМ2 містить перемножувач сигналів (П), інтегратор (ІНТ), порогову схему прийняття рішень про прийнятий біт, електронний ключ (ЕК). Перемножувач (П) на кожному інтервалі часу τ_i здійснює перемноження сигналу з виходу ДМ1 (рис. 5) та сигналу $ПВП_{X11ri}(t)$, який формується схемою формування ПВП відповідно до алгоритму зміни ПВП та системи ключів К. Для санкціонованого користувача в умовах штатної експлуатації системи зв'язку (відсутні експлуатаційні відмови, санкціонований користувач використовує коректну систему ключів К) порядок формування та значення ПВЧ $X11r_i$, які генеруються генератором ПВЧ приймального пристрою співпадають з порядком формування та значеннями ПВЧ $X11_i$, які генеруються генератором ПВЧ передавального пристрою. При цьому $X11r_i = X11_i$ та $ПВП_{X11ri}(t) = ПВП_{X11i}(t)$. Синхронізація надходження елементів ПВП до перемножувача (П) у реальному приймальному пристрої забезпечується системою синхронізації (система формування опорних когерентних коливань ФКОК та синхронізації на рис. 2,б). Моделювання здійснювалось за умов ідеальної синхронізації сигналів. Часова діаграма реалізації сигналу $ПВП_{X11ri}(t)$ для санкціонованого користувача в умовах штатної експлуатації системи зв'язку співпадає з часовою діаграмою реалізації сигналу $ПВП_{X11i}(t)$ у передавальному пристрої (рис. 3). Часові діаграми реалізації сигналу на виході перемножувача (П) при $h^2 = 0{,}25$ та при відсутності завад ($h^2 \to \infty$) показані на рис. 6. Обидві реалізації були отримані при моделюванні та показані на інтервалі часу $t \in \left[2{,}995 \cdot 10^{-6}; 3{,}005 \cdot 10^{-6}\right]$ аналогічно інтервалу часу представлення сигналу на рис. 4, 5.



а) б)

Рис. 6. Сигнали на виході перемножувала: а) – при $h^2 = 0{,}25$; б) – при відсутності завад

Інтегратор зі скиданням (ІНТ) на кожному інтервалі часу τ_i здійснює інтегрування сигналу з виходу перемножувача (П) (рис. 6). Інтегрування сигналу починається з нульового значення на початку кожного інтервалу часу τ_i. У кінці кожного інтервалу часу τ_i здійснюється реєстрація результату інтегрування E_i та скидання інтегратора у нульовий стан. Роботою інтегратора (реєстрація результату інтегрування та скидання у нульовий стан) у реальному приймальному пристрої керує система синхронізації (система ФКОК та синхронізації на рис. 2,б). Часові діаграми реалізації сигналу на виході інтегратора при співвідношенні $h^2 = 0{,}25$ та при відсутності завад ($h^2 \to \infty$) показані на рис. 7. Обидві реалізації були отримані при моделюванні та показані на інтервалі часу $t \in [0;4\cdot10^{-6}]$ аналогічно інтервалу часу представлення сигналів на рис. 3.



а) б)

Рис. 7. Сигнал на виході інтегратора: а) – при $h^2 = 0{,}25$; б) – при відсутності завад

Порогова схема прийняття рішень за результатами кореляційної обробки приймає рішення про значення бінарного символу, що передавався шляхом порівняння результату інтегрування $E_i = E(i\tau)$ з нульовим рівнем. Електронний ключ (ЕК) формує сигнал оцінки $I^*(t)$ конфіденційного повідомлення, що передавалось.

Аналіз складу та функціонування приймального пристрою для випадку несанкціонованого користувача. При моделюванні атак вважалось, що несанкціонований користувач забезпечив синхронізацію приймального пристрою не гірше, ніж у випадку здійснення зв'язку санкціонованими користувачами у штатному режимі експлуатації спеціальної телекомунікаційної системи і використовує систему ключів, при якій значення початкових параметрів генераторів псевдовипадкових чисел з процедури А' ГОСТ Р 34.10-94 у алгоритмі зміни комбінацій "ПВП та частотна позиція" ЧФМ ШСС мінімально відрізняються у більшу сторону у порівнянні з відповідними параметрами для санкціонованого користувача (табл. 1).

Таблиця 1

Початкові параметри генераторів ПВЧ процедури А' ГОСТ Р 34.10-94

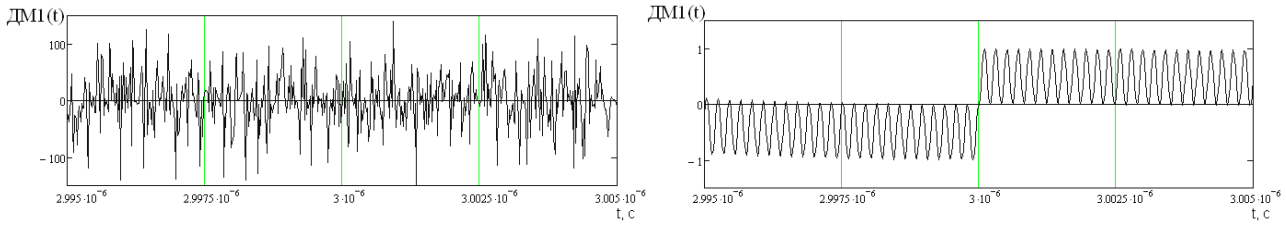
Параметри генераторів	Санкціонований користувач	Несанкціонований користувач
$X1_1$	3241793142	3241793143
$C1$	1786885589	1786885591
$X2_1$	3544621582	3544621583
$C2$	745692845	745692847

ПВЧ $X11r_i$; $X21r_i$ у приймачі санкціонованого користувача та $X11a_i$; $X21a_i$ у приймачі несанкціонованого користувача, отримані з використанням параметрів з табл. 1, а також відповідні значення частотних позицій для перших 10-и бітів повідомлення, що передається наведені у табл. 2. Сигнали на входах приймальних пристроїв санкціонованого та несанкціонованого користувачів однакові (рис. 4). Результат когерентного детектування у демодуляторі 1 (ДМ1) приймального пристрою несанкціонованого користувача при параметрах вказаних у табл. 1, 2 показано на рис. 8 (при $h^2 = 0{,}25$ та відсутності завад). Обидві реалізації сигналів були отримані при моделюванні та показані на інтервалі часу $t \in \left[2{,}995\cdot10^{-6};3{,}005\cdot10^{-6}\right]$ аналогічно інтервалу часу представлення сигналів на рис. 4–6.

Таблиця 2

ПВЧ для приймальної апаратури санкціонованого та несанкціонованого користувачів та значення частотних позицій (ГГц), що їм відповідають

№ біта	$i = 1$	$i = 2$	$i = 3$	$i = 4$	$i = 5$	$i = 6$	$i = 7$	$i = 8$	$i = 9$	$i = 10$
$X11r_i$	71	225	117	177	9	209	145	1	25	54
$X11a_i$	72	137	185	25	145	17	81	89	129	137
$X21r_i$	6	7	1	3	3	2	5	6	2	1
$X21a_i$	7	3	3	2	1	1	3	3	6	5
f_{X21ri}	2,464	2,475	2,409	2,431	2,431	2,42	2,453	2,464	2,42	2,409
f_{X21ai}	2,475	2,431	2,431	2,42	2,409	2,409	2,431	2,431	2,464	2,453



а) б)

Рис. 8. Часові діаграми реалізації сигналу на виході ДМ1 для випадку несанкціонованого користувача: а) – при $h^2 = 0{,}25$; б) – при відсутності завад

Перемножувач (П) на кожному інтервалі часу τ_i здійснює перемноження сигналу з виходу ДМ1 (рис. 8) та сигналу $\text{ПВП}_{X11ai}(t)$, який формується схемою формування ПВП відповідно до алгоритму зміни ПВП та системи ключів, що використовує несанкціонований користувач (табл. 1). Часова діаграма реалізації сигналу $\text{ПВП}_{X11ai}(t)$, що формується у приймальному пристрої, який використовує несанкціонований користувач при системі ключів за табл. 1 показана на рис. 9.

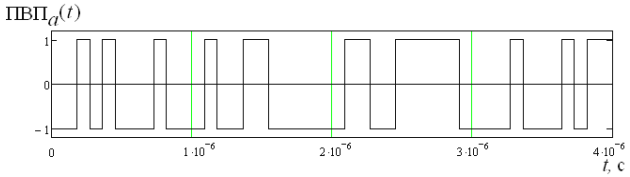


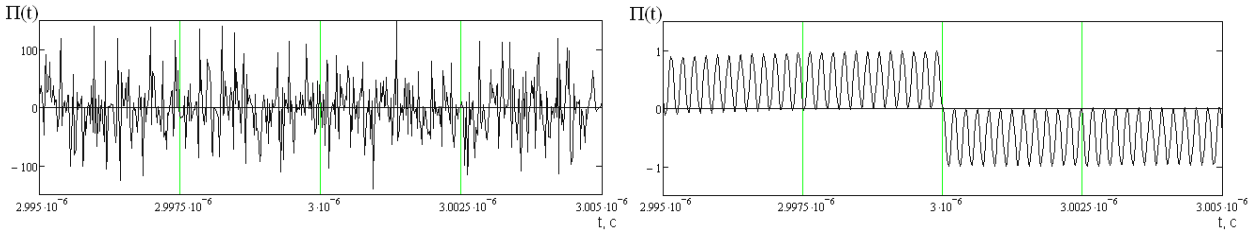
Рис. 9. Часова діаграма реалізації сигналу $\text{ПВП}_{X11ai}(t)$

Сигнал $\text{ПВП}_{X11ai}(t)$ для випадку несанкціонованого користувача на інтервалі часу $t \in [0;\ 4\cdot10^{-6}]$ складається з бінарних ПВП, номери яких у ансамблі та самі ПВП $X11_1 = 72$ (-1 -11-11-1-1-11-1-1, $\max\{|R_{\text{АКФ}}|\} = 3/11$); $X11_2 = 137$ (-11-1-111-1-1-1-1-1, $\max\{|R_{\text{АКФ}}|\} = 2/11$); $X11_3 = 185$ (-111-1-111111-1, $\max\{|R_{\text{АКФ}}|\} = 3/11$); $X11_4 = 25$ (-1-1-11-1-1-11-111, $\max\{|R_{\text{АКФ}}|\} = 3/11$).

Результат перемноження сигналу з виходу демодулятора (ДМ1) та сигналу $\text{ПВП}_{X11ai}(t)$ у перемножувачі (П) демодулятора 2 (ДМ2) приймального пристрою несанкціонованого користувача при параметрах вказаних у табл. 1, 2 показано на рис. 10 (при $h^2 = 0{,}25$ та відсутності завад). Обидві реалізації сигналів були отримані при моделюванні та показані на інтервалі часу $t \in \left[2{,}995\cdot10^{-6};3{,}005\cdot10^{-6}\right]$ аналогічно інтервалу часу представлення сигналів на рис. 4–6, 8.

Сигнали на рис. 8 та рис. 10 у своїй структурі містять складову биттів, тобто коливань різницевої частоти, що дорівнює модулю різниці поточної частотної позиції $f_{X21i} = f_{X21ri}$ у ЧФМ ШСС та коливання частотної позиції f_{X21ai}, яке формує синтезатор частот приймального пристрою, який використовує несанкціонований користувач. На рис. 8 та рис. 10 частота

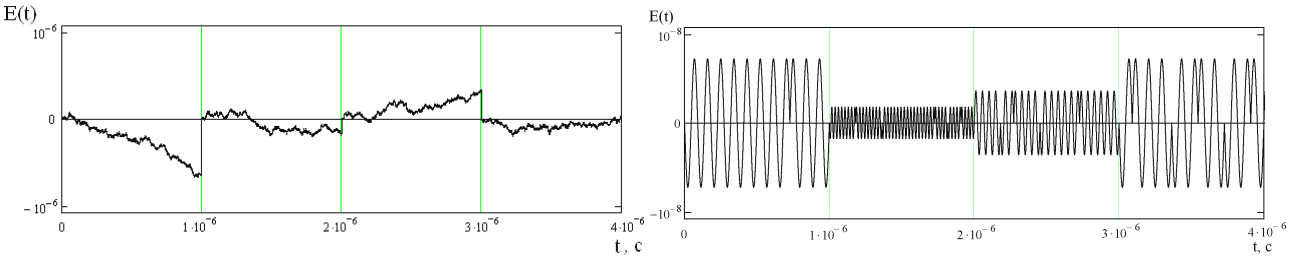
біттів на інтервалі часу представлення сигналів $t \in \left[2{,}995 \cdot 10^{-6}; 3 \cdot 10^{-6}\right]$ [завершення передавання 3-го біту ($i = 3$) конфіденційного повідомлення] складає $\left|f_{X21i} - f_{X21ai}\right|$ = |2,409–2,431| = 0,022 (ГГц), а на інтервалі часу представлення сигналів $t \in \left[3 \cdot 10^{-6}; 3{,}005 \cdot 10^{-6}\right]$ [початок передавання 4-го біту ($i = 4$) конфіденційного повідомлення] складає $\left|f_{X21i} - f_{X21ai}\right|$ = |2,431–2,42| = 0,011 (ГГц) (табл. 2).



а) б)

Рис. 10. Часові діаграми реалізації сигналу на виході перемножувача (П) для випадку несанкціонованого користувача: а) – при $h^2 = 0{,}25$; б) – при відсутності завад

Часові діаграми реалізації сигналу на виході інтегратора для випадку несанкціонованого користувача (при $h^2 = 0{,}25$ та відсутності завад) показані на рис. 11. Обидві реалізації були отримані при моделюванні та показані на інтервалі часу $t \in \left[0; 4 \cdot 10^{-6}\right]$ аналогічно інтервалу часу представлення сигналів на рис. 3, 7, 9.



а) б)

Рис. 11. Часові діаграми реалізації сигналу на виході інтегратора для випадку несанкціонованого користувача а) – при $h^2 = 0{,}25$; б) – при відсутності завад

У розглянутому прикладі, який було отримано при моделюванні, несанкціонований користувач, який здійснює атаку К-дії шляхом використання приймального пристрою санкціонованого користувача та випадковим чином обрану систему ключів (табл. 1) правильно отримає на виході приймального пристрою перші три біти конфіденційного повідомлення і неправильно 4-й біт (слід зауважити, що це стохастична ситуація, яка отримана для конкретних зазначених параметрів моделі і в цілому не характеризує ймовірнісні характеристики успішної реалізації атак).

Аналіз можливих шляхів підвищення ефективності здійснення атак К-дії несанкціонованим користувачем. Аналіз часової діаграми реалізації сигналу на виході інтегратора при відсутності завад (рис. 11,б) показує, що результат інтегрування у цьому випадку $E_i = E(i\tau) = 0$ (що і слід було очікувати для ортогональних сигналів різних частотних позицій), а структура сигналу на виході інтегратора ІНТ демодулятора 2 (ДМ2) приймального пристрою (рис. 2,б) дозволяє аналітику сторони здійснення атак К-дії радіотехнічними засобами провести аналіз, у результаті якого визначити структуру ЧФМ ШСС і далі, використовуючи цю інформацію, відновити конфіденційне повідомлення, що передається за відсутності інформації про ключ (для розглянутої у статті організації передавання інформації у широкосмуговій радіосистемі). Це потребує аналізу сигналів, які існують всередині приймача та його модифікації, що викладено нижче.

Основні принципи аналізу стороною здійснення атак К-дії сигналу на виході інтегратора ІНТ демодулятора 2 (ДМ2) приймального пристрою при відсутності завад полягають у наступному.

1. Визначити частоту сигналу на інтервалах часу τ_i (фазові зсуви сигналу при вимірюванні частоти необхідно попередньо усунути). Значення цієї частоти буде відповідати значенню $\left|f_{X21i} - f_{X21ai}\right|$, тобто модулю різниці між значенням поточної частотної позиції ЧФМ ШСС та значенням частотної позиції, яка формується синтезатором частот приймального пристрою при когерентному детектуванні сигналу. Амплітуда коливання на виході інтегратора обернено пропорційна до частоти цього коливання (рис. 11,б).

Таким чином з точністю до знака різниці $f_{X21i} - f_{X21ai}$ усувається частотна невизначеність ЧФМ ШСС.

Слід зазначити, що аналіз проводиться у відносно низькочастотній смузі (верхня границя при вимірюванні частоти сигналу не перевищує значення ширини смуги частот прямокутного еквіваленту ЧФМ ШСС).

Для отриманого на рис. 11,б випадку значення виміряних таким чином частот складають 11 МГц; 44 МГц; 22 МГц; 11 МГц (відповідні значення $f_{X21i} = f_{X21ri}$ та f_{X21ai} наведені у табл. 2).

Усунути невизначеність знака $\left|f_{X21i} - f_{X21ai}\right|$ можна шляхом такої модифікації приймального пристрою, при якій синтезатор частот завжди буде формувати когерентне гармонічне коливання найнизькочастотнішої частотної позиції (у розглянутому випадку реалізації широкосмугової радіосистеми f_1 = 2,409 ГГц). Тоді частотна невизначеність ЧФМ ШСС усувається повністю: частота сигналу на виході інтегратора ІНТ демодулятора 2 (ДМ2) дорівнюватиме $f_{X21i} - f_1$.

2. Усунути часову невизначеність ЧФМ ШСС (яка ґрунтується на використанні різних ПВП з ансамблю для передавання кожного біту конфіденційного повідомлення) для розглянутої моделі ЧФМ ШСС можна шляхом визначення фазоманіпульованих сегментів сигналу на виході інтегратора ІНТ демодулятора 2 (ДМ2) [рис. 11,б] з використанням додаткового фазового детектору, підключеного до виходу ІНТ ДМ2.

На кожному інтервалі часу τ_i у інтервали часу між моментами часу, в які здійснюється фазовий зсув сигналу на π відповідні сегменти сигналу $ПВП_{X11ai}(t)$ (сигнал, який формується схемою формування ПВП приймального пристрою відповідно до алгоритму зміни ПВП та системи ключів, що використовує несанкціонований користувач) інвертуються відносно сегментів сигналу $ПВП_{X11ri}(t)$ (сигналу, який формувався би схемою формування ПВП приймального пристрою відповідно до алгоритму зміни ПВП та системи ключів, що використовує санкціонований користувач). Ілюстрація цієї частини аналізу для параметрів табл. 1 на інтервалі часу $t \in \left[0;4\cdot10^{-6}\right]$ (4 мкс − передавання перших чотирьох біт змодельованого конфіденційного повідомлення) показана на рис. 12.

У випадку, якщо аналітик попередньо усуне частотну невизначеність ЧФМ ШСС, наприклад, шляхом злому (правильного підбору параметрів $X1_1$ та $C1$ генератора ПВЧ) тієї частини генератора ПВЧ, яка формує числа $X11r_i$ (аналітику будуть відомі значення та порядок слідування цих чисел), структура сигналу $E(t)$ на виході ІНТ ДМ2 при відсутності завад матиме вигляд, показаний на рис. 13. Структура ламаної $E(t)$ у цьому випадку з неточністю до знака відповідатиме значенню модуля взаємно кореляційної функції (для поточного моменту часу t') між сигналами $ПВП_{X11ai}(t)$ та $ПВП_{X11ri}(t)$; знак ламаної (положення відносно осі часу) визначатиметься переданим бітом та умовами зворотної роботи при модуляції BPSK. Результат інтегрування $E_i = E(i\tau)$ для цього випадку буде пропорційним коефіцієнту кореляції (його модулю) між бінарними ПВП, що використовує несанкціонований та санкціонований користувач.

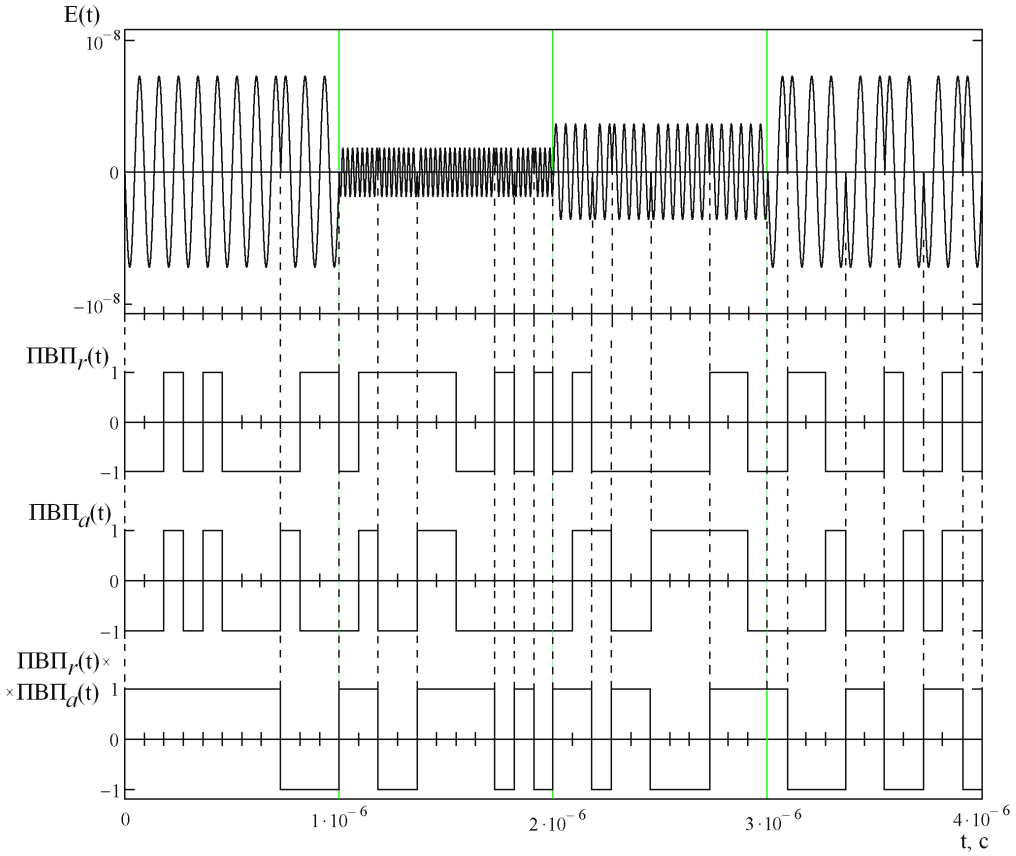


Рис. 12. Ілюстрація аналізу несанкціонованим користувачем сигналу на виході ІНТ ДМ2 при здійсненні атаки К-дії з використанням приймального пристрою санкціонованого користувача (завади відсутні)

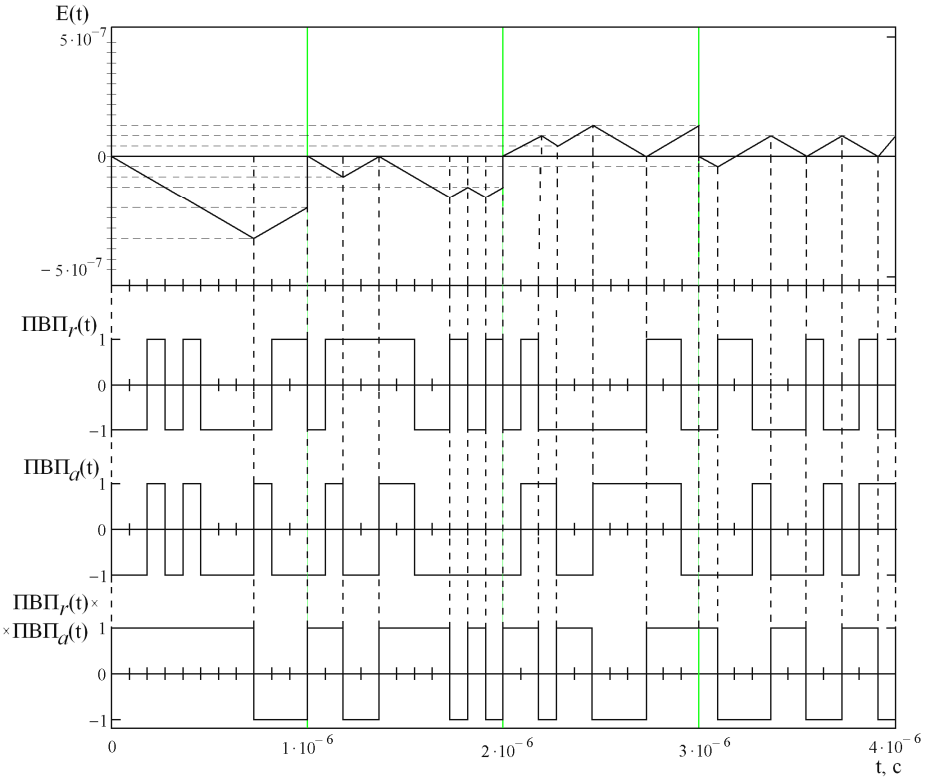


Рис. 13. Ілюстрація аналізу несанкціонованим користувачем сигналу на виході ІНТ ДМ2 при здійсненні атаки К-дії з використанням приймального пристрою санкціонованого користувача (частотна невизначеність попередньо усунута, завади відсутні)

Висновки та перспективи подальших досліджень. Проаналізовано загрози порушення конфіденційності інформації, які можуть бути реалізовані на фізичному рівні широкосмугової радіосистеми при можливості доступу несанкціонованого користувача до системи обробки сигналів приймального пристрою та її модифікації.

1. Доступ до електричних кіл та радіокомпонентів приймального пристрою та його модифікація сторонніми особами повинні бути унеможливленими.

2. Найбільш небезпечним з позицій ТЗІ у приймальному пристрої є сигнал на виході інтегратора (узгодженого фільтра) демодулятора, оскільки його аналіз при відсутності завад та будь-якій випадковим чином обраній системі ключів дозволяє усунути (частково − без модифікації приймального пристрою, повністю − з модифікацією приймального пристрою, пов'язаною з синтезатором частот) частотно-часову невизначеність ЧФМ ШСС і відновити конфіденційне повідомлення, що передається;

3. Повністю усунути частотну невизначеність ЧФМ ШСС при аналізі сигналу на виході інтегратора можна шляхом такої модифікації приймального пристрою, при якій синтезатор частот завжди буде формувати когерентне гармонічне коливання найнижькочастотнішої частотної позиції ЧФМ ШСС.

4. Можливим шляхом протидії розглянутим загрозам є збільшення ширини смуги ЧФМ ШСС та довжини ПВП (бази ШСС), а також об'єму ансамблю, що призведе до збільшення значень $\left|f_{X21i} - f_{X21ai}\right|$ та ускладнення при їх вимірюванні, а також до ускладнення при визначенні фазоманіпульованих сегментів сигналу на виході інтегратора.

Список літератури:

1. Куприянов А.И. Теоретические основы радиоэлектронной борьбы: [учеб. пособие] / А.И. Куприянов, А.В. Сахаров. − М.: Вузовская книга, 2007. − 356 с.: ил.

2. Паук С.М. Аналіз скритності широкосмугових систем зв'язку / С.М. Паук, А.К. Кавасмі // Нові проблеми авіоніки. − 1998. − С. 14-18.

3. Голубничий А.Г. Оценка скрытности передачи данных на основании анализа структуры спектра сигналов / А.Г. Голубничий // Інтегровані інформаційні технології та системи: наук.-практ. конф., 21-23 листопада 2005 р.: матеріали. – К., 2005. − С. 139-141.

4. Закон України "Про Національну систему конфіденційного зв'язку". − Офіц. вид. − Відомості Верховної Ради (ВВР). − 2002. − № 15. − С. 103.

5. Пат. 82053 Україна, МПК H 04 J 11/00. Спосіб багатоканальної передачі дискретної інформації / Голубничий О.Г., Любімов О.Д.; заявники та власники Голубничий О.Г., Любімов О.Д. − № 20040402844; заявл. 19.04.04; опубл. 11.03.08; Бюл. № 5.

6. Борисов В.И. Помехозащищенность систем радиосвязи с расширением спектра сигналов методом псевдослучайной перестройки рабочей частоты / Борисов В.И., Зинчук В.М., Лимарев А.Е. − М.: РадиоСофт, 2008. − 512 с.

7. Применение режима СИЧ в перспективных войсковых радиостанциях УКВ-связи [Електронний ресурс] / Клименко Н.Н. − Режим доступу: http://www.qrz.ru/vhf/klimenko/u1_7.shtml

8. Помехозащищенность систем радиосвязи с расширением спектра сигналов модуляцией несущей псевдослучайной последовательностью / [В.И. Борисов, В.М. Зинчук, А.Е. Лимарев и др.]. − М.: Радио и связь, 2003. − 640 с.

9. Мазурков М.И. Метод защиты информации на основе совершенных двоичных решёток / М.И. Мазурков, В.Я. Чечельницкий, П. Мурр // Радиоэлектроника. – 2008. – Том 51. – № 11. – С. 53-57.

10. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 2.5-004-99. − 1999. − 53 с.

11. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма: ГОСТ Р 34.10-94.

Голубничий О. Г. Аналіз атак К-дії на фізичному рівні широкосмугової радіосистеми при можливості модифікації приймального пристрою / О. Г. Голубничий // Сучасний захист інформації. – К.: ДУІКТ, 2011. – № 4. – С. 42–54.

АНОТАЦІЯ

УДК 004.056.53

Голубничий Олексій Георгійович

Аналіз атак К-дії на фізичному рівні широкосмугової радіосистеми при можливості модифікації приймального пристрою

Проаналізовано загрози порушення конфіденційності інформації, які можуть бути реалізовані на фізичному рівні широкосмугової радіосистеми при можливості доступу несанкціонованого користувача до системи обробки сигналів приймального пристрою та її модифікації.

Ключові слова: інформаційна безпека, конфіденційність, широкосмуговий зв'язок

ABSTRACT

UDC 004.056.53

Alexei Holubnychyi

Analysis of confidentiality breaches attacks in the spread-spectrum radiosystem's physical layer with the possibility of receiver modifying

Threats for a confidentiality violation of the information, which can be implemented in the spread-spectrum radiosystem's physical layer with the possibility of unauthorized user access to the signal processing system of receiver and its modification, are worked out.

Keywords: information security, confidentiality, wideband communications