DOI: 10.18372/2310-5461.48.15089

УДК 621.395.721.5

О. Г. Плющ, канд. техн. наук, доц.
Державний університет телекомунікацій
orcid.org/0000-0001-5310-0660
e-mail: opliusch@yahoo.com

МЕТОД ПІДВИЩЕННЯ ХАРАКТЕРИСТИК ТЕЛЕКОМУНІКАЦІЙНОГО КАНАЛУ ШЛЯХОМ КОМПЛЕКСНОГО ВИКОРИСТАННЯ ПСЕВДОВИПАДКОВИХ КОДОВИХ ПОСЛІДОВНОСТЕЙ

Вступ

Динаміка сучасного розвитку телекомунікаційних систем та мереж характеризується гострим протистоянням між тими, хто передає інформацію до законних її адресатів і тими, хто хоче її отримати не маючи на це повноважень, тобто зловмисникам або кібернетичним злочинцям. Дуже часто ціллю кібернетичних злочинців є не тільки намагання завадити передачі інформації або перехопити повідомлення в телекомунікаційній мережі, а і підробити інформацію з наступної відправкою її до адресата як справжньої.

Остання проблема особливо гостро постає в телекомунікаційних каналах керування безпілотними летальними апаратами. Цілком є зрозумілим, що серед усіх телекомунікаційних мереж найбільшою вразливістю відрізняються ті, що передають інформацію через ефір, тобто є бездротовими. Через це, для таких мереж прихованість та завадозахищеність є ключовими характеристиками.

Поміж усіх практичних засобів поліпшення зазначених характеристик бездротових телекомунікаційних каналів найбільш привабливим є використання широкосмугових сигналів. Розширення спектру сигналу зазвичай виконують за рахунок застосування різних кодових послідовностей, особливо тих, що відомі як псевдовипадкові.

Процедура розширення спектру сигналу в бездротових телекомунікаційних мережах полягає в тому, що кожний біт інформації обробляється обраною кодовою послідовністю, яка налічує в собі певну кількість чипів. Саме вибір кодової послідовності та кількості чипів в ній визначають прихованість і завадозахищеність телекомунікаційного каналу. До того ж, утаємниченість структури послідовності перетворює інформацію, що передається, на таку, яку дуже важко розпізнати. Передача даних в телекомунікаційному каналі, як правило, здійснюється у вигляді кадрів певного розміру.

У такому випадку, покращення характеристик передачі інформації можливо шляхом скремблювання даних за рахунок застосування додаткової псевдовипадкової кодової послідовності, що позначає межі кадрів.

Взаємно автокореляційні властивості зазначених псевдовипадкових кодових послідовностей відіграють вирішальну роль в їх застосуванні в широкосмугових телекомунікаційних мережах. Гарні кореляційні характеристики демонструють ті псевдовипадкові кодові послідовності, які синтезуються з примітивних поліномів певного порядку. Вони складають основу систем мобільного зв'язку третього покоління створених за технологією CDMA [1; 2]. Але в цих телекомунікаційних системах вони використовуються виключно для організації багатоабонентського доступу до мережі, в той час як дослідженню застосування зазначених кодових послідовностей для покращення завадозахищеності та скритності передачі інформації не приділено достатньої уваги. Слід додати, що просте використання двох псевдовипадкових кодових послідовностей при сучасному технічному рівні розвитку кібернетичних злочинців не застраховує від перехоплення та декодування ними повідомлень.

Одним з шляхів вирішення цієї проблеми є безперервна по-кадрова зміна характеристик псевдовипадкових кодових послідовностей в телекомунікаційному каналі. Серед ефективних шляхів досягнення цієї мети є використання циклічних зсувів однієї і тієї тривалої псевдовипадкової кодової послідовності, що сремблює данні та позначає межі кадрів. Іншим шляхом є комплексне використання псевдовипадкових кодових послідовностей отриманих із різних примітивних поліномів одного розміру із певними циклічними зсувами за якої пара «номер кодової послідовності – циклічний зсув» змінюється кожний раз за заздалегідь визначеним алгоритмом, що також приймає різні форми залежно від певних умов.

Виходячи з наведеного, дослідження питань практичного використання завадозахищених, прихованих телекомунікаційних каналів, що комплексно використовують певну кількість псевдовипадкових кодових послідовностей, синтезованих із примітивних поліномів і характеризуються циклічними зсувами є важливим і обумовлює потребу виконання досліджень у цій області.

Аналіз останніх досліджень та публікацій

Використання псевдовипадкових кодових послідовностей в стандартах мобільного зв'язку третього покоління системно викладено у працях [1] та [2]. У праці [1] окреслено сферу використання псевдовипадкових кодових послідовностей та представлені певні їх екземпляри, але це зроблено тільки стосовно організації багатоабонентського доступу в мережах мобільного зв'язку. Слід також додати, що у праці [1] кореляційні властивості послідовностей висвітлено з погляду розділення користувачів системи мобільного зв'язку, в той час як увага завадозахищеності та скритності передачі інформації не виказана. У праці [2] прискіпливо розглядаються практичні складові використання псевдовипадкових кодових послідовностей; в ньому не тільки наведено велику кількість пояснювальних матеріалів, але і опрацьована теорія та практика генерації зазначених послідовностей, включаючи і ті що створюються з циклічними зсувами, за допомогою примітивних поліномів. Недоліком цієї роботи є те, що вона концентрує всю увагу на псевдовипадкових кодових послідовностях як базових компонентах технології мобільного зв'язку CDMA2000, у той час як інші використання розглянуті недостатньо повно.

Праця [3] присвячена висвітленню загальної і, водночас, детальної інформації про псевдовипадкові кодові послідовності, що використовуються для розширення спектрів сигналів і які можуть бути застосовані в телекомунікаційних мережах відповідно до характеристик які вони демонструють.

Слід констатувати, що в цій праці характеристики відповідних кодових послідовностей що розширюють спектри сигналів у практичному телекомунікаційному каналі не дослідженні достатньо глибоко. Незважаючи на те, що це джерело розглядає способи синтезу псевдовипадкових кодових послідовностей, так само як і ті переваги які отримуються при їх використанні, воно демонструє більш теоретичну направленість. Це пояснюється, наприклад, відсутністю проведення імітаційного комп'ютерного моделювання для демонстрації практичних можливостей послідовностей.

Праця [4] містить в себе інформацію про практичне використання псевдовипадкових кодових послідовностей для конструювання практичних телекомунікаційних каналів контролю над безпілотними летальними апаратами.

Недоліком роботи є те, що аналіз завадозахищеності каналів керування такими апаратами, або дронами, не проведено. До того ж, не висвітлюються питання комплексування псевдовипадкових кодових послідовностях, включаючи їх циклічні зсуви, з метою підвищення як їх завадозахищенності, так і скритності управління за допомогою отриманого телекомунікаційного каналу.

Праці [5] та [6] містять достатньо змістовний огляд різних підходів та технологій, що використовуються в бездротових телекомунікаційних мережах. Водночас, ці роботи підкреслюють, що використання псевдовипадкових кодових послідовностей є тільки однією з багатьох технологій. У результаті цього, практична перевірка параметрів кодів не виконується і відсутнє імітаційне комп'ютерне моделювання реальних телекомунікаційних каналів.

Виходячи з огляду джерел та їх недоліків, в роботі зроблено спробу розв'язати проблему комплексного практичного застосування псевдовипадкових кодових послідовностей, включаючи ті, що мають циклічні зсуви, для побудови прихованих і завадозахищених телекомунікаційних каналів.

Постановка завдання

Одним з широко розповсюджених методів підвищення завадозахищенності та скритності передачі інформації а телекомунікаційних каналах є використання широкосмугових сигналів. Серед шляхів формування широкосмугових сигналів, перспективним вважається використання псевдовипадкових послідовностей що розширюють спектр сигналу. Із аналізу літературних джерел вбачається зрозумілим, що сьогодні псевдовипадкові кодові послідовності здебільшого використовуються для організації багато абонентського доступу в мережах мобільного зв'язку. В той же час, такі кодові послідовності отримані з примітивних поліномів можуть успішно використовуватися для підвищення завадозахищенності та скритності телекомунікаційних каналів. Зроблено припущення, що найбільшого рівня завадозахищенності можливо досягти при комплексному використанні певного набору псевдовипадкових кодових послідовностей з циклічними зсувами,

параметри яких змінюються від кадру до кадру. Як результат, виникає необхідність з'ясування шляхів практичної побудови телекомунікаційного каналу на основі комплексного використання псевдовипадкових кодових послідовностей та перевірки його ефективності.

У цій статті зроблена спроба вирішити ці нагальні питання.

Мета статті

Метою статті є дослідження можливості комплексного використання псевдовипадкових кодових послідовностей отриманих з примітивних поліномів з циклічними зсувами для реалізації завадозахищеного та скритного телекомунікаційного каналу.

Для досягнення поставленої мети розв'язуються такі наукові завдання:

– розроблення кодової та кадрової структури завадозахищеного та скритного телекомунікаційного каналу;

– отримання псевдовипадкових кодових послідовностей для побудови завадозахищеного телекомунікаційного каналу на основі примітивних поліномів з використанням циклічних зсувів;

– дослідження характеристик побудованого каналу на фоні власних шумів та завад шляхом комп'ютерного імітаційного моделювання.

Виклад основного матеріалу

Методика дослідження

В роботі пропонується структура завадозахищеного та скритного телекомунікаційного каналу побудованого з комплексним застосуванням псевдовипадкових кодових послідовностей отриманих з примітивних поліномів. Основу методики дослідження характеристик отриманого каналу передачі інформації складає комп'ютерне імітаційне моделювання. Це моделювання здійснювалося для таких умов:

• імітувався один кадр інформаційної бітової послідовності, що складається з визначеної кількості бітів. Перший біт завжди залишався рівним одиниці, тому що на цьому інтервалі було розташовано кадровий синхроімпульс, а значення (1 або –1) інших бітів інформації формувалося по псевдовипадковому закону з рівномірним розподіленням;

• усі біти, окрім першого, оброблялися однією з чотирьох коротких псевдовипадкових послідовностей тривалістю 256 чипів, за рахунок чого виконувалося розширення спектру;

• отримана бітова послідовність перемножувалася почипово з другою тривалою псевдовипадковою кодовою послідовністю з періодом що дорівнює тривалості кадру. В результаті здійснювалося додаткове скремблювання даних без подальшого розширення спектру та позначалися межі кадру;

• сформований кадр перетворювався у комплексні відліки з урахуванням знаку певного біту інформації з, відповідно, фазами 0 або π (бінарна модуляція);

• до корисного сигналу додавалися внутрішній шум каналу та завадовий сигнал;

• внутрішній шум каналу мав відносну потужність що дорівнює одиниці, та був представлений як комплексні відліки з нормальним розподіленням імовірності;

• завадовий сигнал так само був представлений як комплексні відліки з нормальним розподіленням імовірності і потужністю одиниця;

• створена сигнальна суміш пропускалася через стискаючий фільтр налаштований на виділення певної групи чипів тривалої кодової послідовності, формуючи таким чином сигнал початку кадру;

• створена сигнальна суміш почипово перемножувалася з тривалою кодовою послідовністю для дескремблювання даних;

• отримана в попередньому пункті сигнальна суміш пропускалася через стискаючий фільтр налаштований на виділення бітів інформації, що передавалися в телекомунікаційному каналі;

Імітаційне моделювання здійснювалося за допомогою середовища Matlab. Основною ціллю моделювання була перевірка працездатності телекомунікаційного каналу за різних циклічних зсувах та його спроможності передавати інформацію на фоні завадових сигналів.

Розробка кодової та кадрової структури завадозахищеного телекомунікаційного каналу

Як уже зазначалося вище, передача інформації в телекомунікаційному каналі здійснюється кадрами. Розмір кадру залежить від типу каналу, середовища його застосування та необхідної швидкості передачі інформації. Кожний біт, що передається, розширюється по спектру за рахунок однієї з чотирьох коротких псевдовипадкових послідовностей. При цьому коефіцієнт розширення визначається з одного боку необхідною швидкістю передачі інформації, а з іншого — наявною смугою частот. Припустимо, що потрібно забезпечити швидкість передавання даних в телекомунікаційному каналі 20 кБіт/сек при ширині смуги каналу 5 мГц. Виходячи з цього, можливий коефіцієнт розширення спектру становить 256 одиниць. Таким чином, коротка псевдовипадкова послідовність, що розширює спектр кожного біту, повинна складатися з 256 чипів.

Приймемо, що один кадр буде складатися з 128 бітів. У цьому випадку, тривала псевдовипадкова кодова послідовність, що визначає розмір кадру, повинна вміщувати 32 768 чипів.

У статті пропонується використовувати чотири різні послідовності з 256 чипів. При цьому для скремблювання та позначення меж кадру пропонується використовувати 10 різних псевдовипадкових послідовностей з 128 циклічними зсувами кожна. Таким чином, число різних комбінацій «коротка псевдовипадкова послідовність–тривала псевдовипадкова послідовність–циклічний зсув тривалої псевдовипадкової послідовності» буде складати 4*10*128 = = 5120 триплетів. Автором пропонується перехід від одного триплету до іншого, від кадру до кадру, або за певним законом або за певною таблицею переходів, яка в свою чергу також може змінюватися.

Таким чином, чипова та кадрова структура та алгоритм побудови телекомунікаційного каналу виглядають так:

- кожний кадр тривалістю 32768 чипів вміщує в собі 128 біт інформації по 256 чипів кожний;
- формуються чотири коротких псевдовипадкових кодових послідовності, які мають період 256 чипів, що дорівнює тривалості одного біту;
- формується десять псевдовипадкових кодових послідовностей, які мають період 32 768 чипів, що дорівнює тривалості кадру;
- обирається початкова комбінація «коротка псевдовипадкова послідовність–тривала псевдовипадкова послідовність–циклічний зсув тривалої псевдовипадкової послідовності» і на її основі формується перший кадр телекомунікаційного каналу;
- усі біти, окрім першого, розширюються по спектру за рахунок короткої кодової послідовності тривалістю 256 чипів із вибраного триплету;
- перший біт завжди має значення одиниця і не розширюється короткою кодовою послідовністю тривалістю 256 чипів а, навпаки, використовується для кадрової синхронізації;
- усі біти кадру обробляються другою кодовою послідовністю тривалістю 32768 чипів зі сформованих триплетів;
- кадрова синхронізація здійснюється за рахунок перших 256 чипів тривалої кодової послідовності зі 32768 чипів;
- зі зміною кадру здійснюється перехід від одного триплету до іншого.

Розглянемо, яким чином можуть бути отримані чотири короткі псевдовипадкові кодові послідовність з 256 чипів та 10 тривалих псевдовипадкових кодових послідовностей з 32 768 чипів і з циклічними зсувами.

Синтез псевдовипадкових кодових послідовностей для організації завадозахищеного телекомунікаційного каналу на основі примітивних поліномів

Для отримання гарних характеристик телекомунікаційного каналу, псевдовипадкові кодові послідовності повинні мати добрі автокореляційні властивості. Одним з шляхів синтезу таких кодових послідовностей є використання примітивних поліномів певного порядку. Примітивні поліноми відповідного порядку, що готові до використання, можливо знайти в джерелах інформації [2]. Також їх можливо отримати шляхом ділення поліномів. Для синтезу десяти тривалих псевдовипадкових послідовностей, що складаються з 32 768 чипів, потрібно використовувати примітивні поліноми 15-го ступеня.

У статті пропонується використовувати такі десять примітивних поліномів п’ятнадцятого ступеня над полем Галуа GF(2):

$$F_1(x) = 1 + x^5 + x^7 + x^8 + x^9 + x^{13} + x^{15}; \quad (1)$$

$$F_2(x) = 1 + x + x^2 + x^3 + x^6 + x^7 + x^{15}; \quad (2)$$

$$F_3(x) = 1 + x + x^5 + x^{10} + x^{15}; \quad (3)$$

$$F_4(x) = 1 + x^4 + x^5 + x^{10} + x^{15}; \quad 4)$$

$$F_5(x) = 1 + x + x^2 + x^4 + x^5 + x^{10} + x^{15}; \quad (5)$$

$$F_6(x) = 1 + x^3 + x^5 + x^7 + x^9 + x^{10} + x^{15}; \quad (6)$$

$$F_7(x) = 1 + x^3 + x^5 + x^8 + x^9 + x^{10} + x^{15}; \quad (7)$$

$$F_8(x) = 1 + x^2 + x^6 + x^7 + x^{11} + x^{15}; \quad (8)$$

$$F_9(x) = 1 + x + x^3 + x^{12} + x^{15}; \quad (9)$$

$$F_{10}(x) = 1 + x^2 + x^3 + x^4 + x^5 + x^{12} + x^{15}. \quad (10)$$

Будь-яка псевдовипадкова кодова послідовність отримана с застосуванням виразів (1)-(10) може бути вироблена використовуючи 15 елементний зсувний регістр. Так, наприклад, на рис. 1 зображено генератор псевдовипадкової кодової послідовності с застосуванням (1).

На рис.1 представлено п’ятнадцять елементів зсувного регістру, тоді як на виходах п’ятого, сьомого, восьмого, дев’ятого та тринадцятого елементів виконується операція додавання за модулем два.

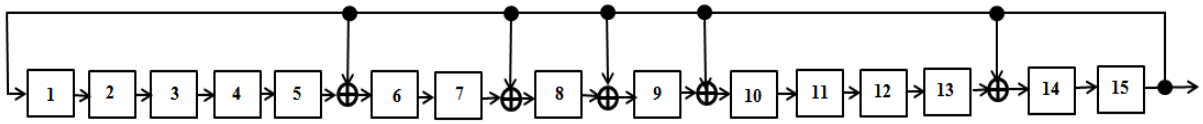

Рис. 1. Структурна схема генератора псевдовипадкової кодової послідовності тривалістю 32767 чипів

Схема на рис. 1 може формувати тільки послідовність зі 32 767 чипів, тому що в ній не може існувати на виході одночасно 15 нулів; у цьому випадку вона зупиниться. Для того, щоб отримати послідовність зі 32 768 чипів потрібно додати один додатковий нуль до 14 вже існуючих. Ця процедура може бути виконана за допомогою кількох способів і самим простим є формування на виході додаткового нуля без пересування даних по регістрам під час одного з 14 нулів.

Для формування чотирьох коротких бітових послідовностей з 256 чипів необхідно мати поліноми 8-го ступеня. В роботі пропонується використовувати чотири такі поліноми 8-го ступеня [2]:

$$F_{11}(x) = 1 + x^2 + x^3 + x^4 + x^8; \qquad (11)$$

$$F_{12}(x) = 1 + x + x^3 + x^5 + x^8; \qquad (12)$$

$$F_{13}(x) = 1 + x + x^5 + x^6 + x^8; \qquad (13)$$

$$F_{14}(x) = 1 + x^2 + x^5 + x^6 + x^8. \qquad (14)$$

Як і у випадку з примітивними поліномами (1)–(10), для генерування послідовності будується зсувний регістр і у послідовності, що він формує, потрібно додавати один додатковий нуль до серії з сімох уже існуючих. Таким чином отримується послідовність зі 256 чипів.

На рис. 2 представлена псевдовипадкова кодова послідовність зі 256 чипів синтезована згідно з виразом (11). Ця кодова послідовність сформована в логіці «1» та «–1» тому, що така логіка є більш зручною для використання в телекомунікаційному каналі.

Псевдовипадкова кодова послідовність сформована згідно з виразом (1) є занадто тривалою, тому на рис. 3 наведено тільки перші 1000 чипів цієї послідовності, які є важливими для виявлення сигналу що позначає початок кадрів.

Дослідження характеристик побудованого каналу на фоні власних шумів та завад шляхом комп'ютерного імітаційного моделювання

Для перевірки працездатності запропонованого телекомунікаційного каналу використовувалися псевдовипадкові послідовності побудовані згідно з примітивними поліномами (1) та (11) за допомогою зсувних регістрів застосовуючи методи імітаційного комп'ютерного моделювання наведені вище. Суміш корисного сигналу, власних шумів каналу та завади в приймальній частині бездротового телекомунікаційного каналу протягом одного кадру наведена на рис. 3.

Нагадаємо, що корисний сигнал представлений у вигляді бінарної модуляції послідовності з 128 бітів (кадр інформації), кожний з яких є розширений по спектру у 256 разів короткою псевдовипадковою кодовою послідовністю і скрембльований додатково тривалою псевдовипадковою кодовою послідовністю, протяжність якої дорівнює тривалості кадру. При цьому власний шум являє собою вибірки розподілені за нормальним законом з потужністю одиниця. Завадовий сигнал має такі самі розподілення вірогідності і потужність, як і власний шум каналу.

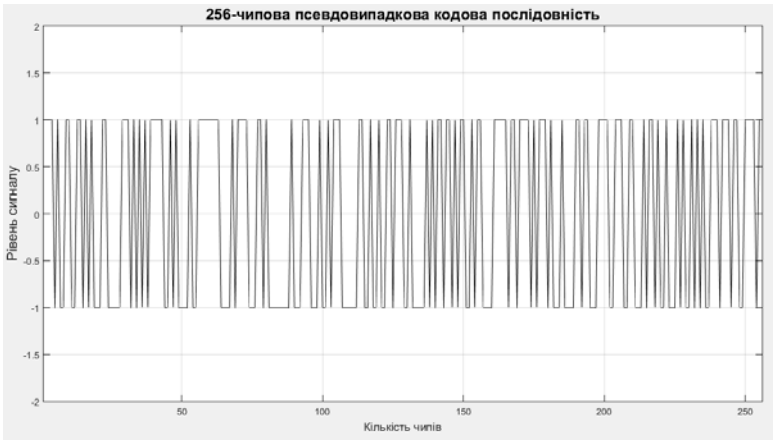

Рис. 2. Псевдовипадкова кодова послідовність зі 256-чипів створена за рахунок використання примітивного поліному (11)

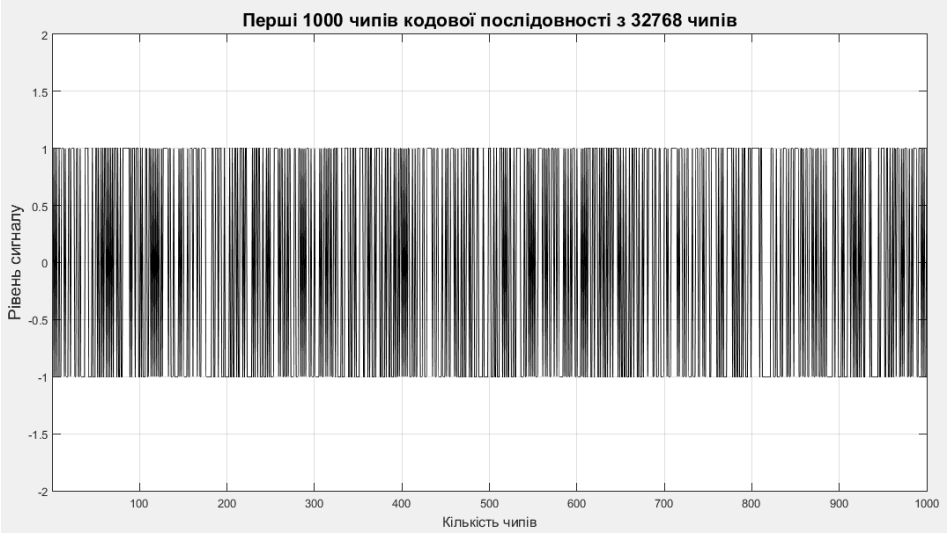

Рис. 3. Перші 1000 чипів послідовності з 32 768 чипів створеної згідно з виразом (1)

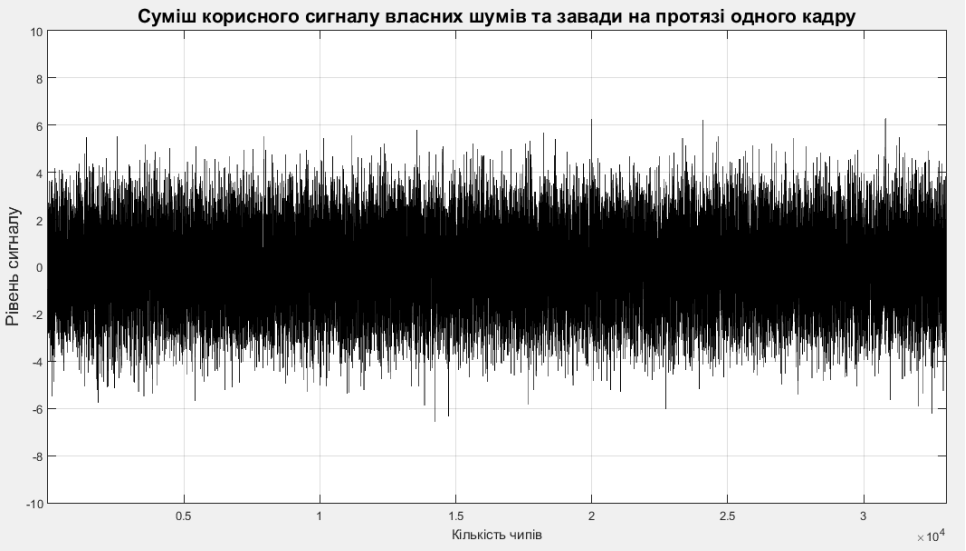

Рис. 4. Суміш корисного сигналу, власних шумів каналу та завади протягом одного кадру

Подальше дослідження спрямоване на встановлення того факту, чи можливо виділити з суміші зображеної на рис. 4 кадрову структуру передачі інформації та значення окремих біт.

На рис. 5 представлено сигнал на виході узгодженого фільтру стиснення кадрового імпульсу після обробки цим фільтром сигналу що зображено на рис. 4.

Виокремлений імпульс початку кадру телекомунікаційного каналу знаходиться на початковій ділянці кадру на рис. 5.

Виходячи з даних наведених на рис. 5, імпульс початку кадру добре виділяється на фоні власних шумів каналу та шумової завади, які за умовами імітаційного моделювання перевищують потужність корисного сигналу в два рази.

Після дослідження можливості виявлення імпульсу початку кадру, перейдемо до вивчення можливості виділення значень бітів корисної інформації з сигнальної суміші наведеній на рис. 4. Слід зауважити, що операція виділення сигналу початку кадру повинна виконуватися завжди першою, тому що це дозволяє провести дескремблювання сигнальної суміші зображеній на рис. 4 псевдовипадковою кодовою послідовністю синтезованою згідно з (1) та перші 1000 чипів якої представлені на рис. 3.

Рис. 6 ілюструє сигнал на виході узгодженого фільтру стиснення бітів, що обробляв сигнальну суміш зображену на рис. 4 з урахуванням її дескремблювання, відповідно, для одного кадру телекомунікаційного каналу.

Дослідження результатів показує, що за рахунок стискання біти корисного сигналу впевнено виділяється на фоні внутрішнього шуму каналу та завадового сигналу.

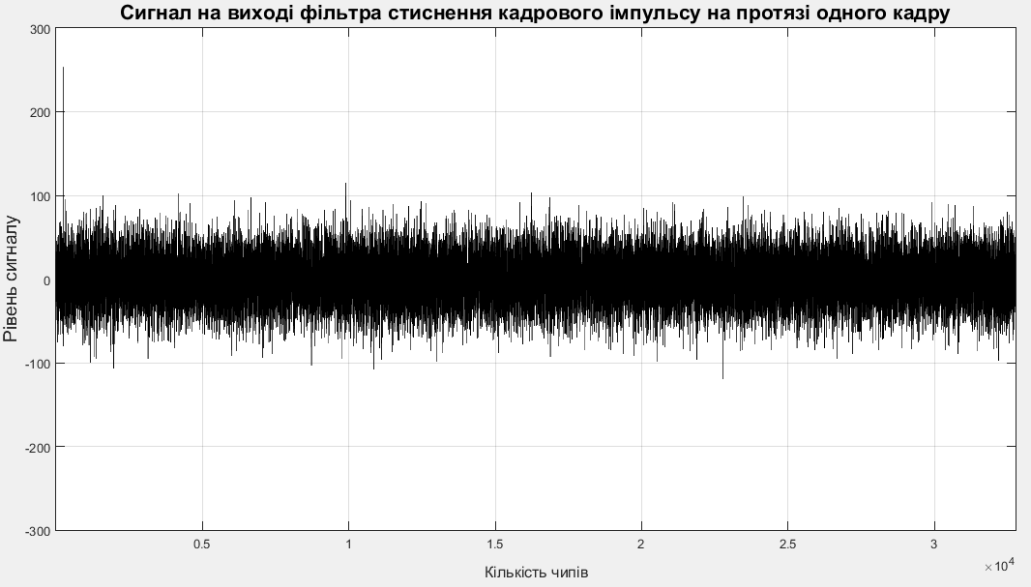

Рис. 5. Сигнал на виході узгодженого фільтру стиснення кадрового імпульсу після обробки цим фільтром сигналу зображеного на рис. 4

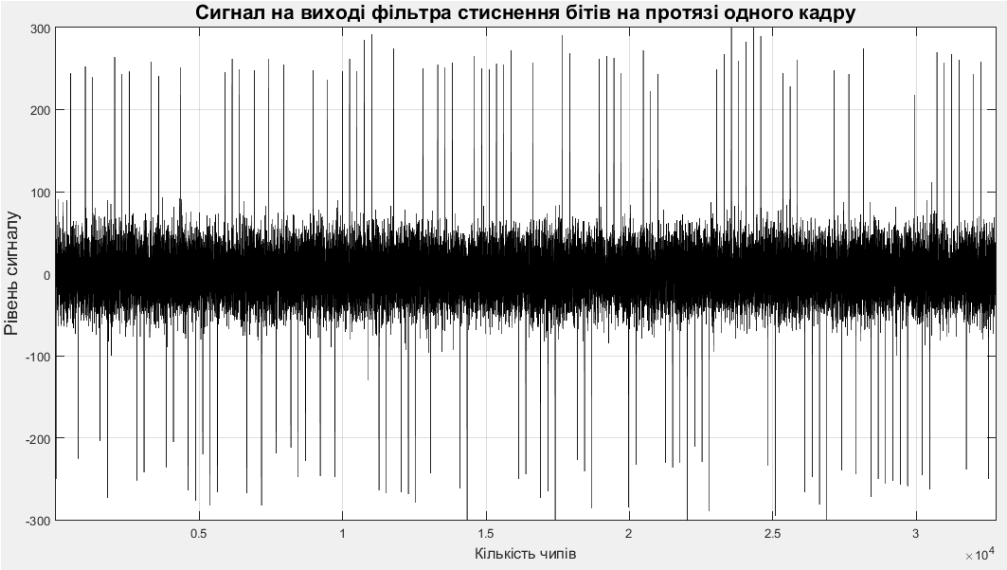

Рис. 6. Сигнал на виході узгодженого фільтра стиснення бітів протягом одного кадру телекомунікаційного каналу

Організація по-кадрової зміни параметрів кодів, що використовуються для побудови телекомунікаційного каналу

Сучасний рівень розвитку засобів кібернетичних зловмисників дозволяє вирішувати дуже складні завдання щодо перехоплення та декодування інформації в телекомунікаційних каналах. Тому, навіть наявність двох псевдовипадкових кодів не дозволяє повністю захиститися від вказаних проблем. Тому в роботі пропонується для більшого підвищення завадозахищеності та скритності передачі інформації використовувати 10 псевдовипадкових послідовностей що позначають розміри кадру з 128 циклічними зсувами кожна, а також чотири послідовності по 256 чипів, що розширюють спектр бітів.

Для виконання циклічних зсувів доцільно використовувати 15 бітові маски.

Структурна схема формування різних циклічних зсувів у тривалій бітовій послідовності з 32 768 чипів, сформованої згідно з виразом (1), наведена на рис. 7.

На рис. 7 кожний з п’ятнадцяти бітів маски циклічного зсуву поєднуються з сигналом на виході відповідного зсувного регістра по логіці «і». Після цього, вихідна, зсунута на певне число кратне 256 чипам, кодова послідовність, формується шляхом додавання всіх отриманих логічних сигналів за модулем 2.

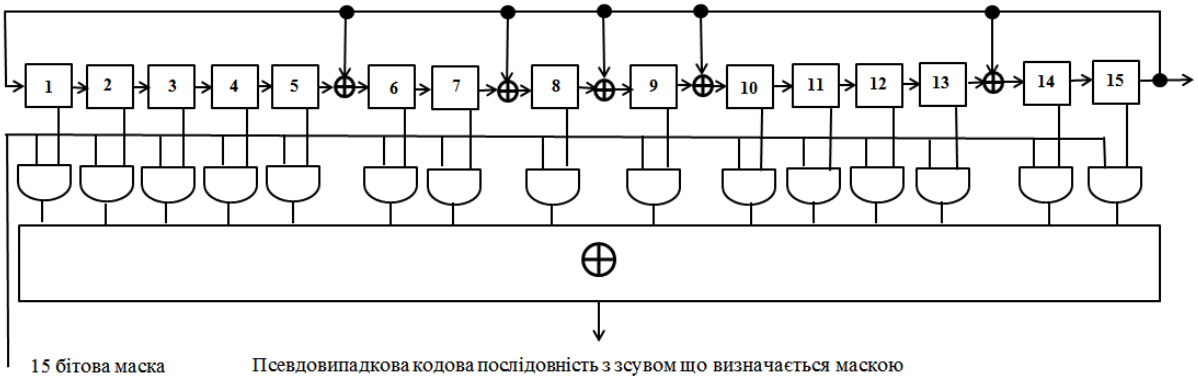

Рис. 7. Структурна схема генератора псевдовипадкової кодової послідовності тривалістю 32 768 чипів з циклічними зсувами що визначаються 15 бітними масками

Таким чином, для побудови завадозахищеного телекомунікаційного каналу в якому будуть комплексно використовуватися десять різних псевдовипадкових послідовностей по 32 768 чипів з циклічними зсувами та чотири псевдовипадкових послідовностей по 256 чипів достатньо мати десять 15-ти розрядних зсувних регістрів з додатковою логікою для застосування маски та чотири 8-ми розрядні зсувні регістри. При цьому застосування певної послідовності з чотирьох для розширення спектру бітів та відповідної послідовності з 32768 чипів зі зсувом, що позначає розмір кадру, буде проходити за певною процедурою, що визначається або відповідною формулою або таблицею переходів.

Висновки

Телекомунікаційні канали передавання даних завжди знаходяться серед пріоритетних цілей кібернетичних зловмисників. Виходячи з цього, в даній роботі приділено велику увагу підвищенню завадозахищеності та скритності передачі інформації в таких каналах.

Для покращення цих показників, запропоновано використовувати псевдовипадкові кодові послідовності створені з примітивних поліномів певного ступеня, які забезпечують розширення спектру сигналів та мають гарні авто- та взаємно кореляційні властивості.

У статті запропоновано побудова завадозахищеного та скритного каналу з псевдовипадкових кодових послідовностей двох розмірів: для розширення спектру бітів корисної інформації використовується послідовність з 256 чипів, у той час як для позначення меж кадру та забезпечення додаткового скремблювання інформації використовується послідовність з 32 768 чипів. При цьому зроблено висновок, що для забезпечення прийнятного рівня захисту телекомунікаційного каналу потрібно комплексно використовувати чотири псевдовипадкові кодові послідовності по 256 чипів для розширення спектру бітів та десять псевдовипадкових кодових послідовностей розміром 32 768 чипів з циклічними зсувами для позначення розміру кадрів та додаткового скремблювання інформації.

Для максимального захисту інформації запропоновано змінювати вигляд кадру до кадру триплети «коротка псевдовипадкова послідовність–тривала псевдовипадкова послідовність–циклічний зсув тривалої псевдовипадкової послідовності» з 5120 можливих варіантів за певним алгоритмом або таблицею переходів.

Характеристики побудованого телекомунікаційного каналу досліджувалися шляхом комп'ютерного імітаційного моделювання. Було з'ясовано, що запропонований підхід дозволяє впевнено виявити кадрову структуру інформації яка передається та виділити значення бітів корисної інформації на фоні адитивної суміші корисного сигналу с завадами, що перевищують корисний сигнал у два рази за потужністю.

Виходячи з цього, подальші дослідження слід спрямувати на пошук такого алгоритму покадрового вибору триплетів, який забезпечить найкращі характеристики з погляду завадозахищенності телекомунікаційного каналу та його скритності.

ЛІТЕРАТУРА

1. **Andreas Springer,** Robert Weigel. UMTS: The Physical Layer of the Universal Mobile Telecommunications System. USA: Springer Science & Business Media, 2013. 298 p.

2. **Lee Jhong S.,** Miller Leonard E. CDMA systems engineering handbook. Boston, London: Artech House, 1998. 1228 p.

3. **Byeong G. Lee,** Seok C. Kim. Scrambling Techniques for Digital Transmission. USA: Springer Science & Business Media, 2012. 448 p.

4. **Edited by Kamesh Namuduri,** Serge Chaumette, Jae H. Kim, James P. G. Sterbenz. UAV Networks and Communications. UK: Cambridge University Press, 2017. 242 p.

5. **Evgenii Krouk,** Sergei Semenov. Modulation and Coding Techniques in Wireless Communications. USA: John Wiley & Sons, 2011. 680 p.

6. **Clint Smith,** Daniel Collins. Wireless Networks. USA: McGraw Hill Professional, 2013. 752 p.

Плющ О. Г.

МЕТОД ПІДВИЩЕННЯ ХАРАКТЕРИСТИК ТЕЛЕКОМУНІКАЦІЙНОГО КАНАЛУ ШЛЯХОМ КОМПЛЕКСНОГО ВИКОРИСТАННЯ ПСЕВДОВИПАДКОВИХ КОДОВИХ ПОСЛІДОВНОСТЕЙ

В роботі запропоновано підхід до побудови завадостійкого та скритного каналу передачі даних в телекомунікаційних мережах. Підхід базується на виконанні розширення спектру бітів корисної інформації та додатковому її скремблюванні на основі псевдовипадкових кодових послідовностей отриманих з примітивних поліномів восьмого та п'ятнадцятого порядку, що мають гарні авто та взаємно кореляційні властивості. Вивчалися характеристики телекомунікаційного каналу що складається с кадрів тривалістю 128 бітів, кожний з яких спектрально розширюється в 256 разів за допомогою синтезованої короткої псевдовипадкової послідовності. Друга синтезована тривала псевдовипадкова кодова послідовність протяжністю 32768 чипів використовується для позначення меж кадру та додаткового скремблювання інформації. Для забезпечення максимального захисту від перехоплення, в роботі пропонується використовувати десять тривалих псевдовипадкових послідовностей з 128 циклічними зсувами та чотири коротких псевдовипадкових послідовності. При цьому передбачається утворення 5120 різних комбінацій - «коротка псевдовипадкова послідовність-тривала псевдовипадкова послідовність-циклічний зсув тривалої псевдовипадкової послідовності», або триплетів, перехід між якими здійснюється від кадру до кадру. Правили переходу може визначатися певним алгоритмом або заздалегідь відомою таблицею переходів. Як алгоритм, так і таблиця, час від часу можуть змінюватися. Для дослідження характеристик побудованого телекомунікаційного каналу використовувалося комп'ютерне імітаційне моделювання. За результатами моделювання, зроблено висновок, що обробка адитивної суміші корисного сигналу с завадами, що перевищують корисний сигнал в два рази по потужності, узгодженими стискаючими фільтрами дозволяє впевнено виявити кадрову структуру інформації, що передається, за рахунок виділення імпульсу початку кадрів, та встановити значення біт корисної інформації. Отримані в роботі результати досліджень дозволяють стверджувати, що побудований телекомунікаційний канал з комплексним використанням десяти тривалих псевдовипадкових послідовностей з циклічними зсувами та чотирьох коротких послідовностей може успішно застосовуватися при реалізації завадозахищених, скритних телекомунікаційних мереж.

Ключові слова*:* телекомунікаційна мережа; примітивний поліном; псевдовипадкові кодові послідовності; комп'ютерне моделювання; розширення спектру; циклічний зсув послідовності.

Pliushch O.

METHOD OF TELECOMMUNICATION CHANNEL PERFORMANCE IMPROVEMENT BY COMPLEX USE OF PSEUDO NOISE CODING SEQUENCES

The paper proposes an approach to design of noise immune and concealed data transmission channel in telecommunication networks. The approach is based on performing spectrum spreading of the useful information bits, as well as its additional scrambling. For this purpose, pseudo noise coding sequences are used derived from the primitive polynomials of the order eight and fifteen, which possess good auto and inter correlational properties. It is studied performance of the telecommunication channel that includes frames of 128 bit length, each of which is spectrally spread 256 times with the help of a synthesized pseudo noise coding sequence. The second 32768 chip-long pseudo noise coding sequence is used to mark the frame duration and perform additional information scrambling. To ensure maximum protection from interception, the paper proposes to use ten long pseudo noise sequences with 128 cyclic shifts and four short pseudo noise coding sequences. In this case, it is conceived to form 5120 different combinations - «short pseudo noise coding sequence – long pseudo noise coding sequence – cyclic shift of the long pseudo noise sequence», or triplets, transitions between which are performed on a frame-by-frame basis. Transition rules can be defined by a certain algorithm or beforehand known transition table. Both the algorithm and the table can undergo changes from time to time. To assess performance of the designed telecommunication channel, computer simulation was used. With account of the simulation results, the inference is made that the processing of the additive mixture of the desired signal and interfering ones, which surpass the desired signal two times in terms of power, by the matched filters permits to confidently reveal the information frame structure being transmitted by determining frame beginning pulse and establish the bit values of the desired information. Research findings, obtained in this paper,

permit to claim that the designed telecommunication channel, with complex use of the ten long pseudo noise coding sequences with cyclic shifts and four short pseudo noise coding sequences can be successfully used for implementation in noise immune concealed telecommunication networks.

Keywords: telecommunication network; primitive polynomial; pseudo noise coding sequences; computer simulation; spectrum spreading; cyclic sequence shift.

Плющ А. Г.

МЕТОД ПОВЫШЕНИЯ ХАРАКТЕРИСТИК ТЕЛЕКОММУНИКАЦИОННОГО КАНАЛА ПУТЕМ КОМПЛЕКСНОГО ИСПОЛЬЗОВАНИЯ ПСЕВДОСЛУЧАЙНЫХ КОДОВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

В работе предложен подход к построению помехоустойчивого и скрытного канала передачи данных в телекоммуникационных сетях. Подход базируется на использовании расширения спектра бит полезной информации и дополнительном ее скремблировании на основе псевдослучайных кодовых последовательностей полученных с примитивных полиномов восьмого и пятнадцатого порядков, которые имеют хорошие авто и взаимно корреляционные свойства. Изучались характеристики телекоммуникационного канала, который состоит из кадров длительностью 128 бит, каждый из которых спектрально расширяется в 256 раз с помощью синтезированной короткой псевдослучайной последовательности. Вторая синтезированная длительная псевдослучайная последовательность протяжением 32768 чипов используется для обозначения границ кадра и дополнительного скремблирования информации. Для обеспечения максимальной защиты от перехвата, в работе предлагается использовать десять длительных псевдослучайных последовательностей с 128 цикличными сдвигами и четыре коротких псевдослучайных последовательности. При этом предусматривается создание 5120 разных комбинаций - «короткая псевдослучайная последовательность - длительная псевдослучайная последовательность - циклический сдвиг длительной псевдослучайной последовательности», или триплетов, переход между которыми осуществляется от кадра к кадру. Правила перехода могут устанавливаться определенным алгоритмом или заранее известной таблицей переходов. Как алгоритм, так и таблица, время от времени могут меняться. По результатам моделирования, сделан вывод, что обработка аддитивной смеси полезного сигнала с помехами, которые превышают полезный сигнал в два раза по мощности, согласованными сжимающими фильтрами позволяет уверенно выявить кадровую структуру информации, которая передается, за счет выделения импульса начала кадров, и установления значений бит полезной информации. Полученные в работе результаты исследований позволяют утверждать, что разработанный телекоммуникационный канал с комплексным использованием десяти длительных псевдослучайных последовательностей с цикличными сдвигами и четырех коротких последовательностей может успешно применяться при реализации помехозащищенных, скрытных телекоммуникационных сетей.

Ключевые слова: телекоммуникационная сеть; примитивный полином; псевдослучайные кодовые последовательности; компьютерное моделирование; расширение спектра; цикличный сдвиг последовательности.

Стаття надійшла до редакції 30.10.2020 р.
Прийнято до друку 10.12.2020 р.