КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№1 (9), 2020
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2020.9.126139
УДК 621.395.721.5

Плющ Олександр Григорович
кандидат технічних наук, доцент, професор кафедри Мобільних та відеоінформаційних технологій
Державний університет телекомунікацій, Київ, Україна
ORCID: 0000-0001-5310-0660
opliusch@yahoo.com

ВИКОРИСТАННЯ ЦИКЛІЧНИХ ЗСУВІВ ПСЕВДОВИПАДКОВОЇ КОДОВОЇ ПОСЛІДОВНОСТІ ДЛЯ ПІДВИЩЕННЯ ХАРАКТЕРИСТИК ТЕЛЕКОМУНІКАЦІЙНОГО КАНАЛУ

Анотація. Запропоновано підхід до побудови завадостійкого та скритного каналу передачі даних в телекомунікаційних мережах. Приділена увага забезпеченню скритності передачі інформації, так само як і захисту її від перехоплення зловмисниками. Підхід базується на здійсненні 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 псевдовипадкової послідовності. Друга синтезована псевдовипадкова кодова послідовність тривалістю 32768 чипів використовується для позначення тривалості кадру та додаткового скремблювання інформації. 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. Подальше підвищення захищеності інформації від перехоплення запропоновано робити за рахунок циклічних зсувів псевдовипадкової кодової послідовності тривалістю 32 768 чипів. Шляхом комп'ютерного імітаційного моделювання встановлено, що незнання циклічного зсуву призводить до неможливості перехоплення інформації зловмисниками. Отримані в роботі результати досліджень дозволяють стверджувати, що побудований телекомунікаційний канал з використанням циклічних зсувів псевдовипадкової кодової послідовності за певним прихованим законом 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.

1. ВСТУП

Постановка проблеми. Телекомунікаційні системи завжди були і є ціллю тих, хто хоче завадити передачі інформації, перехопити повідомлення, щоб дізнатися їх зміст, або і навіть зімітувати передачу хибної інформації як такої, що виглядає справжньою. Останнє особливо важливе в телекомунікаційних каналах управління безпілотними летальними апаратами або дронами. Взагалі, вразливість бездротових мереж є набагато більшою ніж інших, тому прихованість та завадозахищеність

телекомунікаційних мереж, в яких данні передаються через повітряний простір, відіграє вирішальну роль в їх практичних використаннях.

Застосування широкосмугових сигналів є одним з небагатьох дійсно ефективних методів поліпшення вказаних характеристик бездротових телекомунікаційних каналів. Формування сигналів з розширеним спектром найбільш часто виконується з використанням різних кодових послідовностей, серед яких виділяються своєю ефективністю ті, що є псевдовипадковими.

При розширені спектру в бездротових телекомунікаційних мережах кожний біт інформації піддається обробці відповідною кодовою послідовністю, яка складається з певної кількості чипів. Чим більше кількість чипів, тим вище прихованість та завадозахищеність, а утаємниченість структури послідовності робить інформацію дуже важкою для розпізнавання. Зазвичай, біти даних є цілком доцільним передавати у вигляді кадрів певного розміру, при цьому підвищений захист інформації можливо забезпечити шляхом використання додаткової псевдовипадкової кодової послідовності, яка не тільки скремблює данні, а і позначає межі кадру.

У вказаних застосуваннях, ключовими характеристиками псевдовипадкових кодових послідовностей є їхні взаємно та авто кореляційні властивості. Відомо, що гарні кореляційні показники мають ті псевдовипадкові послідовності, які отримуються з примітивних поліномів певного порядку. На таких псевдовипадкових послідовностях побудовані системи мобільного зв'язку третього покоління [1,2]. Але в цих мережах вони застосовуються тільки для побудови багатоабонентського доступу та розділення тих абонентів, які належать у певний проміжок часу до різних базових станцій. В той же час, питання використання зазначених кодових послідовностей для підвищення завадозахищеності та скритності передачі інформації в телекомунікаційних каналах опрацьовані недостатньо. До того ж, просте використання двох, навіть з найкращими характеристиками, псевдовипадкових кодових послідовностей при сучасному технічному рівні оснащення кібернетичних зловмисників не є достатнім заходом. Вважається необхідним постійно змінювати параметри псевдовипадкових кодових послідовностей в телекомунікаційному каналі. Одним з ефективних шляхів досягнення цієї мети є використання циклічних зсувів однієї і тієї ж тривалої псевдовипадкової кодової послідовності, що сремблює данні та позначає межі кадрів.

Виходячи з наведеного, вивчення практичної реалізації завадостійких, прихованих каналів передачі інформації з використанням псевдовипадкових кодових послідовностей, отриманих з примітивних поліномів та в яких застосовується циклічний зсув, є важливим і це обумовлює необхідність проведення досліджень в цьому напрямку.

Аналіз останніх досліджень і публікацій. Достатньо змістовно використання псевдовипадкових кодових послідовностей в стандартах мобільного зв'язку третього покоління представлено в літературних джерелах [1], [2]. В [1] виокремлено область застосування псевдовипадкових кодових послідовностей і наведені певні їх зразки, але все це виконано зважаючи на побудову багатоабонентського доступу до мобільної мережі. До того ж, кореляційні властивості розглянуто тільки що стосується розділення абонентів і увага завадозахищеності та скритності передачі інформації не приділена. Робота [2] надає велику увагу практичній складовій застосування псевдовипадкових кодових послідовностей, до того ж в ній представлено достатньо пояснювальних матеріалів та окреслена теорія та практика їх генерації, наразі і з циклічними зсувами, за допомогою примітивних поліномів. Незважаючи на вказане, ця праця приділяє

максимальну увагу псевдовипадковим кодовим послідовностям що використаються в технології CDMA2000, а інші розглянуті поверхнево.

В джерелі [3] здійснена спроба навести повну і, водночас, детальну інформацію про кодові послідовності, що розширюють спектри сигналів та за своїми характеристиками можуть бути застосовані в телекомунікаційних каналах та мережах. Нажаль, в цій роботі дослідженню характеристикам певних кодових послідовностей для розширення спектрів сигналів у практичному телекомунікаційному каналі не надано достатньої уваги. Хоча в цій роботі окреслюються способи формування псевдовипадкових кодових послідовностей та ті переваги які отримуються при їх застосуванні, вона має більш теоретичну направленість і не підкріплює представлену інформацію, наприклад, даними імітаційного комп'ютерного моделювання.

Підхід до практичного застосування псевдовипадкових кодових послідовностей для побудови каналів управління безпілотними летальними апаратами зроблено в роботі [4]. Але аналіз завадозахищеності каналів управління дронами не виконано і взагалі не розглядаються циклічні зсуви в псевдовипадкових кодових послідовностях з метою підвищення як цього показника, так і скритності управління через телекомунікаційний канал.

Досить змістовний огляд різних технологій, що застосовуються в бездротових телекомунікаційних мережах, представлено в [5] та [6]. Але в цих джерелах підкреслюється, що застосування псевдовипадкових кодових послідовностей є тільки однією з зазначених технологій, і, як результат, практичній перевірці характеристик кодів увага не приділяється.

Виходячи з огляду джерел, в роботі зроблено спробу розв'язання проблеми практичного застосування псевдовипадкових кодових послідовностей з циклічними зсувами для створення завадозахищених та прихованих телекомунікаційних каналів.

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

Для досягнення поставленої мети розв'язуються наступні наукові задачі:

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

– синтез псевдовипадкових кодових послідовностей для організації 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.

2. МЕТОДИКА ДОСЛІДЖЕННЯ

В роботі була синтезована структура телекомунікаційного каналу в якому забезпечується завадозахищенність та скритність передачі даних. Для дослідження характеристик отриманого каналу передачі інформації використовувалося комп'ютерне імітаційне моделювання. Воно виконувалося для наступних умов:

• Імітувався один кадр бітової послідовності, що складається з визначеної кількості бітів. Перший біт завжди залишався рівним одиниці, тому що на цьому

ISSN 2663 - 4023

проміжку було розташовано кадровий синхроімпульс, а значення (1 або -1) інших бітів інформації формувалося по псевдовипадковому закону з рівномірним розподіленням;

• Всі біти, окрім першого, оброблялися першою короткою псевдовипадковою послідовністю певної тривалості, 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 ймовірності;

• Завадовий сигнал так само був представлений як комплексні відліки з нормальним розподіленням ймовірності 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;

• Моделювання проводилося для різних циклічних зсувів псевдовипадкової послідовності що позначає тривалість кадрів.

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

3. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

3.1 Розробка кодової та кадрової структури завадозахищеного телекомунікаційного каналу

Як вже 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 короткої псевдовипадкової послідовності. При цьому коефіцієнт розширення визначається з одного боку необхідною швидкістю передачі інформації, а з іншого - наявною смугою частот. Припустимо, що потрібно забезпечити швидкість передачі 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. В цьому випадку, тривала псевдовипадкова кодова послідовність, що визначає розмір кадру, повинна вміщувати 32768 чипів.

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

• Кожний кадр тривалістю 32768 чипів вміщує в собі 128 біт інформації по 256 чипів кожний;

• Формується перша псевдовипадкова кодова послідовність, яка має період 256 чипів, що дорівнює тривалості одного біту;

• Формується друга псевдовипадкова кодова послідовність яка має період 32768 чипів, що дорівнює тривалості кадру;

• Всі біти окрім першого, розширюються по спектру за рахунок короткої кодової послідовності тривалістю 256 чипів;

• Перший біт завжди має значення одиниця і не розширюється короткою кодовою послідовністю тривалістю 256 чипів а, навпаки, використовується для кадрової синхронізації;

• Всі біти кадру обробляються другою кодовою послідовністю тривалістю 32768 чипів;

• Кадрова синхронізація здійснюється за рахунок перших 256 чипів тривалої кодової послідовності з 32768 чипів.

Розглянемо яким чином можуть бути отримані коротка псевдовипадкова кодова послідовність з 256 чипів та тривала псевдовипадкова кодова послідовність з 32768 чипів.

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

Для тримання гарних характеристик телекомунікаційного каналу, псевдовипадкові кодові послідовності повинні мати певні 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 тривалої псевдовипадкової послідовності, що складається з 32768 чипів, потрібно використовувати примітивний поліном 15-го ступеня.

В роботі було вибрано примітивний поліном п’ятнадцятого ступеня над полем Галуа GF(2), що має наступний вигляд [2]:

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

Псевдовипадкова кодова послідовність с застосуванням (1) може бути отримана використовуючи 15 елементний зсувний регістр зображений на рис. 1.

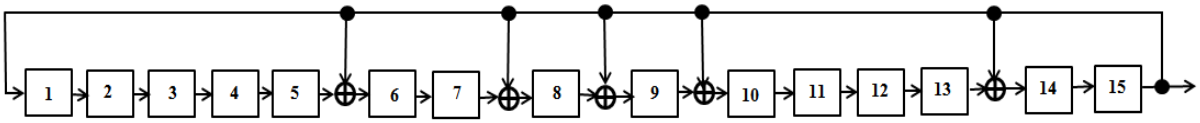

Рис. 1. Структурна схема генератора псевдовипадкової кодової послідовності тривалістю 32767 чипів

ISSN 2663 - 4023

На рис.1 наведено п'ятнадцять елементів зсувного регістру, в той час як на виходах п’ятого, сьомого, восьмого, дев’ятого та тринадцятого елементів виконується операція додавання по модулю два.

Пристрій на рис.1 може формувати тільки послідовність з 32767 чипів, тому що в ньому не може існувати на виході одночасно 15 нулів. Для того, щоб отримати послідовність з 32768 чипів потрібно додати один додатковий нуль до 14 вже існуючих нулів. Існує багато способів виконання цієї процедури, і самим простим є формування на виході додаткового нуля без пересування даних під час одного з 14 нулів.

Для формування короткої бітової послідовності з 256 чипів необхідно мати поліном 8-го ступеня. Один з таких поліномів з [2] має наступний вигляд:

$$F(x) = 1 + x^2 + x^3 + x^4 + x^8 \quad (2)$$

Як і у випадку з примітивним поліномом (1), для генерування послідовності будується зсувний регістр і у послідовності, що він формує, потрібно додавати один додатковий нуль до серії з сімох вже існуючих. Таким чином отримується послідовність з 256 чипів.

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

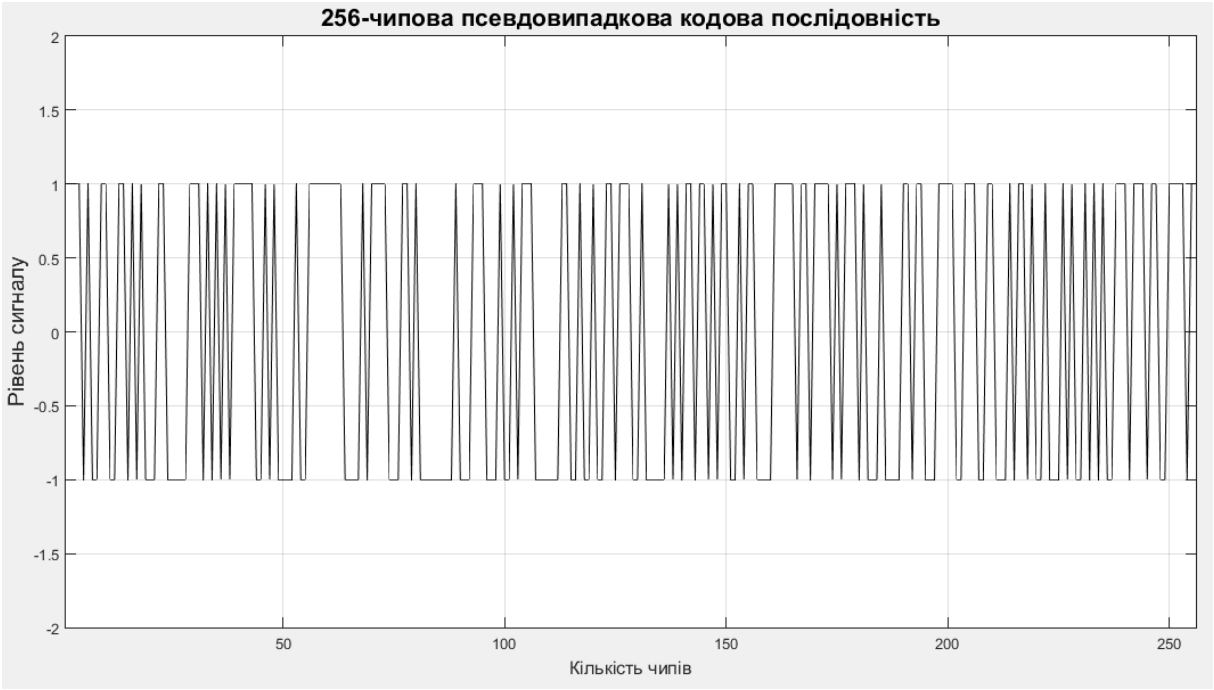

Рис. 2. Псевдовипадкова кодова послідовність з 256-чипів створена за рахунок використання примітивного поліному (2)

Псевдовипадкова кодова послідовність сформована згідно з (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.

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

ISSN 2663 - 4023

Суміш корисного сигналу, власних шумів каналу та завади в приймальній частині бездротового телекомунікаційного каналу на протязі одного кадру наведена на рис.4. Нагадаємо, що корисний сигнал є представленим 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 по нормальному закону з потужністю одиниця. Завадовий сигнал має такі ж самі розподілення вірогідності і потужність, як і власний шум каналу.

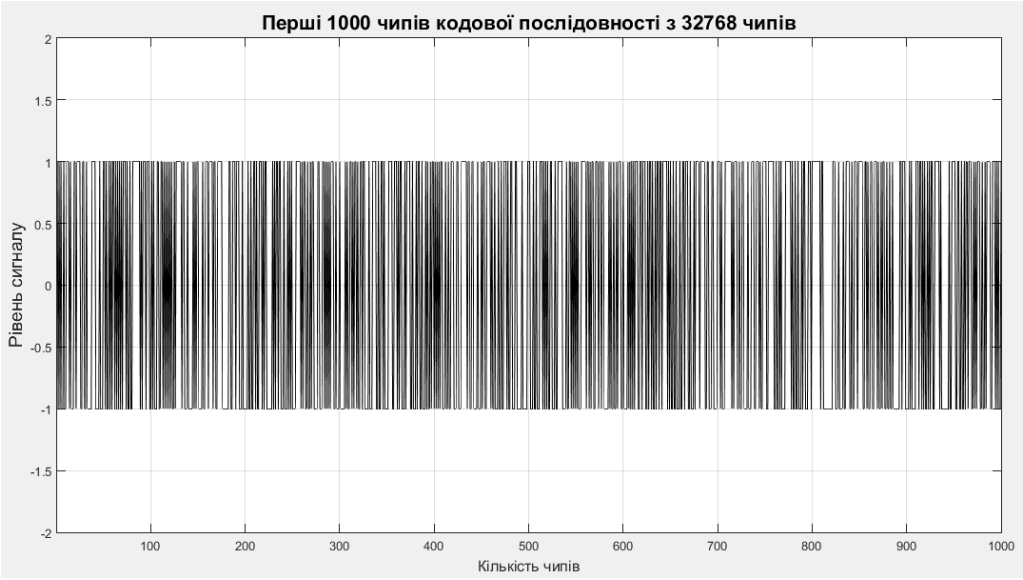

Рис. 3. Перші 1000 чипів послідовності з 32768 чипів створеної згідно з (1)

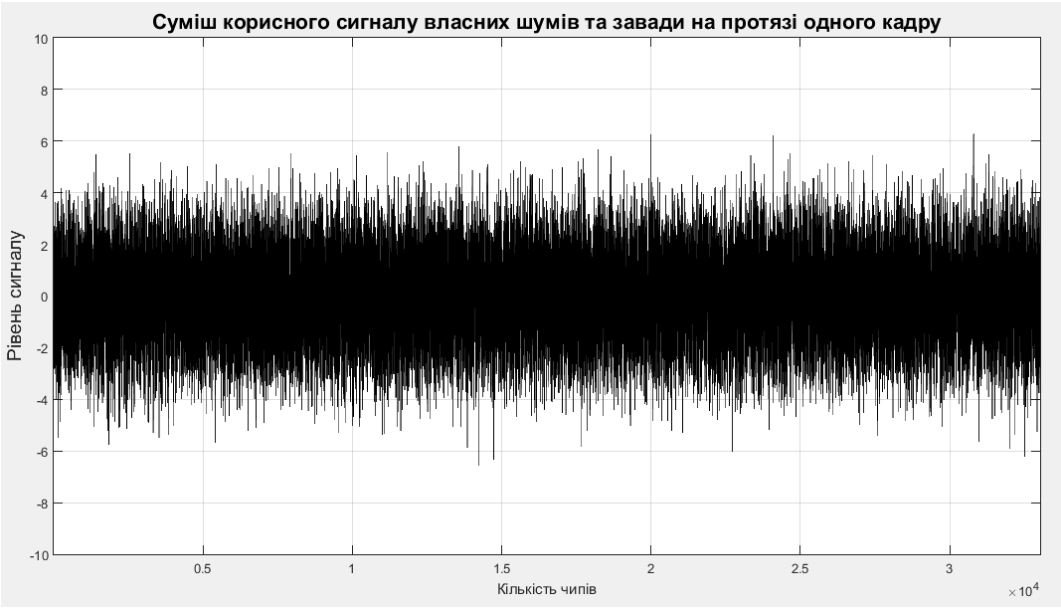

Рис.4. Суміш корисного сигналу, власних шумів каналу та завади на протязі одного кадру

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.

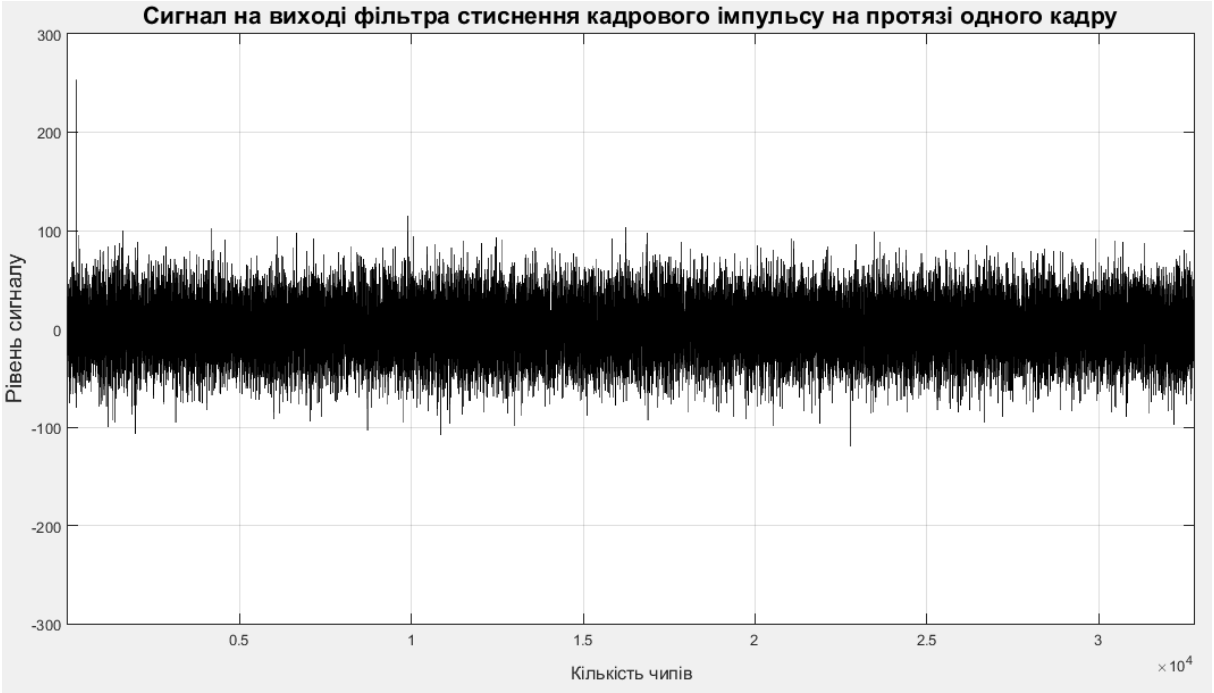

Рис. 5. Сигнал на виході узгодженого фільтру стиснення кадрового імпульсу після обробки цим фільтром сигналу зображеного на рис.4

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.

ISSN 2663 - 4023

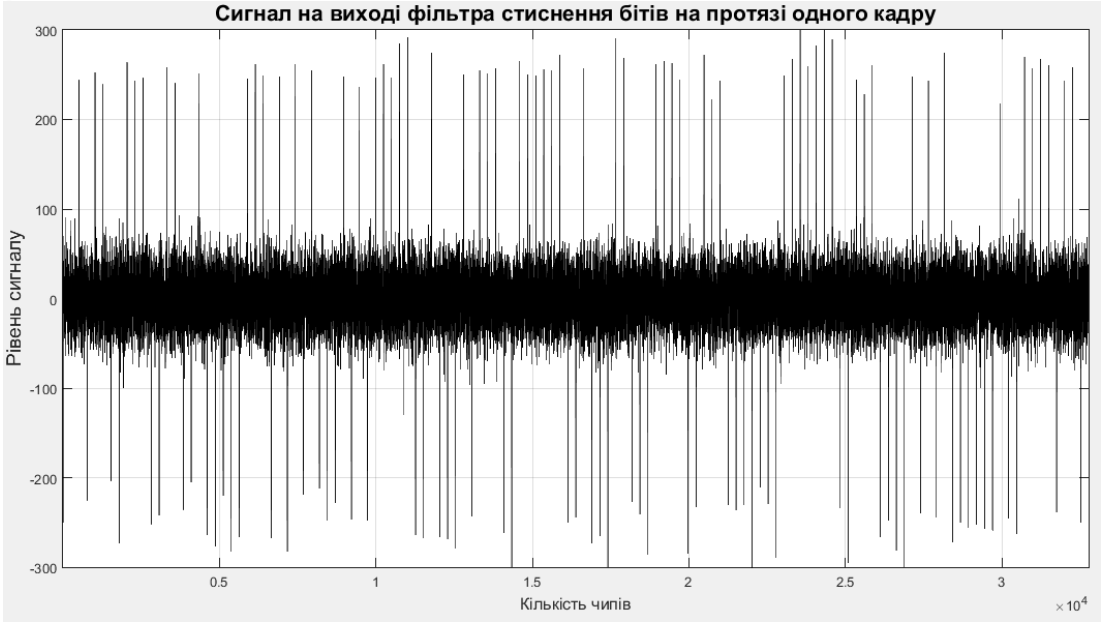

Рис.6. Сигнал на виході узгодженого фільтра стиснення бітів на протязі одного кадру телекомунікаційного каналу

3.4 Дослідження характеристик побудованого каналу з використанням циклічних зсувів тривалої кодової послідовності

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. Для ще більшого підвищення завадозахищеності та скритності передачі інформації, в роботі пропонується додатково використовувати циклічні зсуви тривалої кодової послідовності від кадру до кадру на число чипів кратне 256. Таких циклічних зсувів може бути 128, що дорівнює кількості бітів в кадру. При цьому циклічні зсуви можуть виконуватись за певними таємними алгоритмами, що можуть постійно оновлюватися.

Для виконання циклічних зсувів доцільно використовувати 15 бітові маски. Структурна схема формування різних циклічних зсувів у тривалій бітовій послідовності з 32768 чипів наведена на рис. 7.

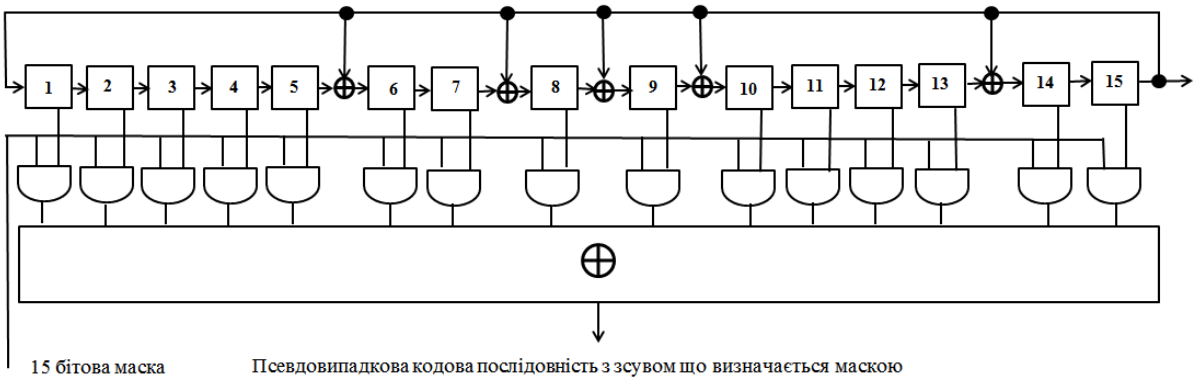

Рис. 7. Структурна схема генератора псевдовипадкової кодової послідовності тривалістю 32768 чипів з циклічними зсувами що визначаються 15 бітними масками

ISSN 2663 - 4023

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 по модулю 2.

Для перевірки ефективності запропонованого підходу до підвищення завадозахищеності та скритності телекомунікаційного каналу, було сформовано сигнал подібний до того, що зображено на рис. 4, але зі зсувом тривалої кодової послідовності на 5 циклів по 256 чипів. Такий сигнал зображено на рис. 8.

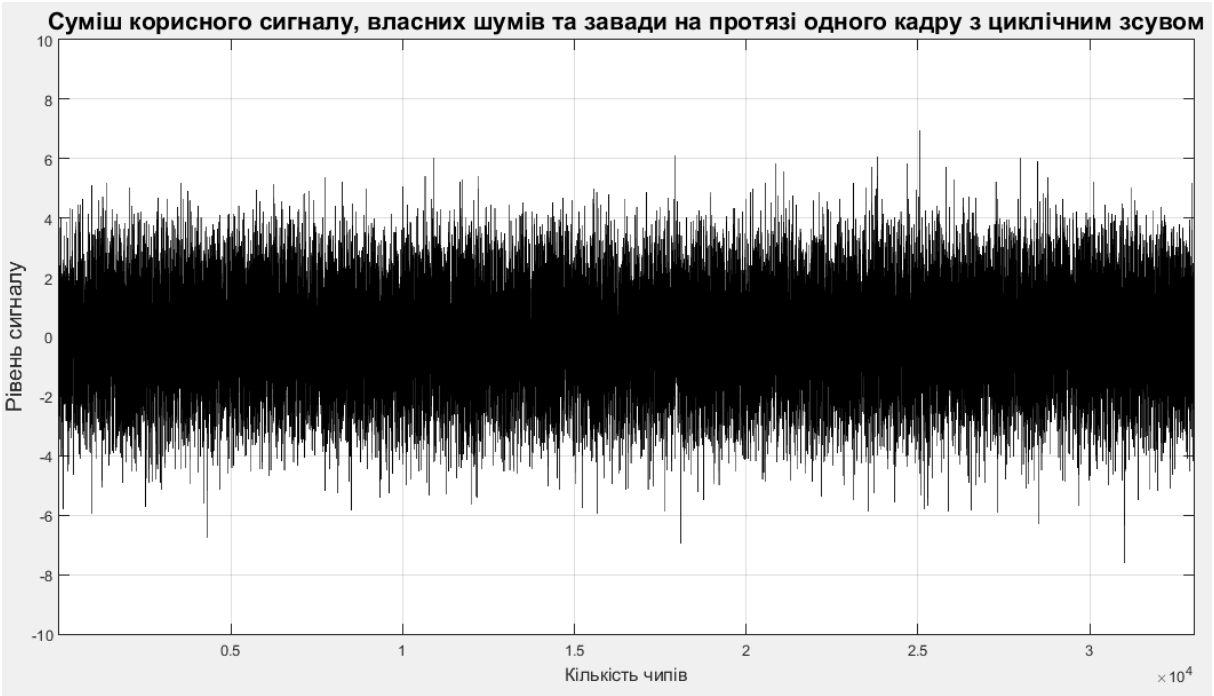

Рис.8. Суміш корисного сигналу, власних шумів каналу та завади на протязі одного кадру з циклічним зсувом

Припустимо, що зловмисники не мають інформації про циклічний зсув, але якимось чином дізналися про структуру короткої псевдовипадкової послідовності з 256 чипів та тривалої послідовності з 37268 чипів без зсуву. В такому випадку, при спробі перехоплення, вони отримають кадровий синхроімпульс та відповідну бітову послідовність, що наведені на рис. 9 та рис.10. Як вбачається з цих рисунків, при циклічному зсуві зловмисники будуть не в змозі декодувати структуру кадру та виділити біти корисної інформації.

На рис.11 та рис.12 наведені сигнали на виході пристрою стиснення кадрового імпульсу та пристрою стиснення бітів з урахуванням циклічного зсуву. Як свідчать данні на цих рисунках, при урахуванні вказаного циклічного зсуву, відповідна обробка дозволяють виділити кадровий імпульс та бітову послідовність. Додатково, стрілочка на рис. 11 показує розташування кадрового імпульсу.

ISSN 2663 - 4023

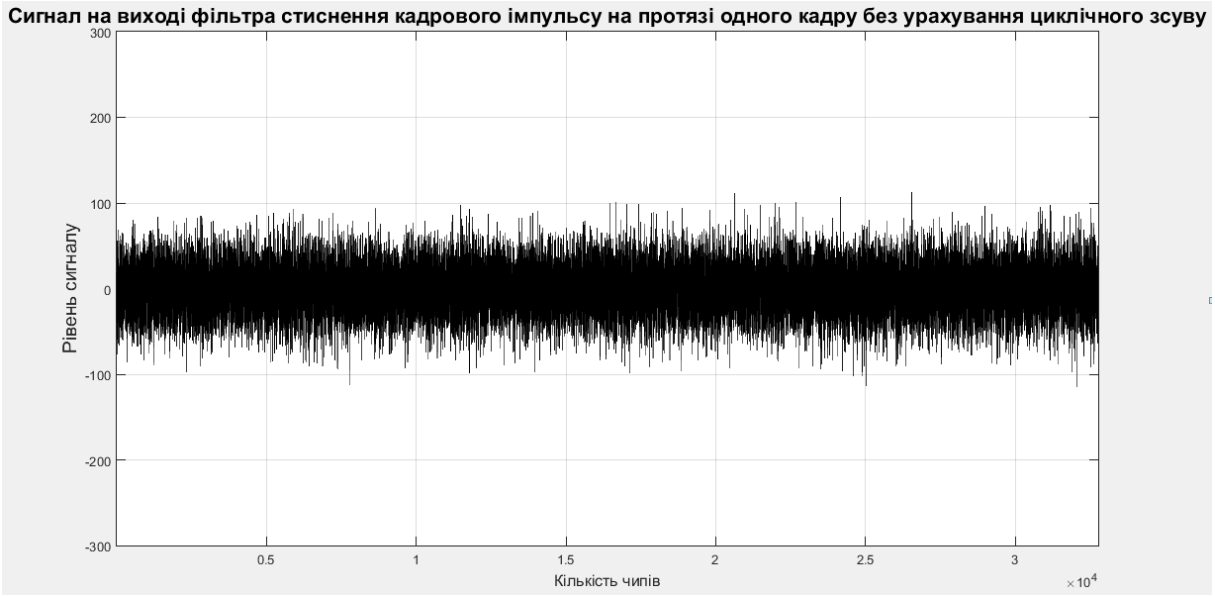

Рис.9. Сигнал на виході фільтра стиснення кадрового імпульсу на протязі одного кадру без урахування циклічного зсуву

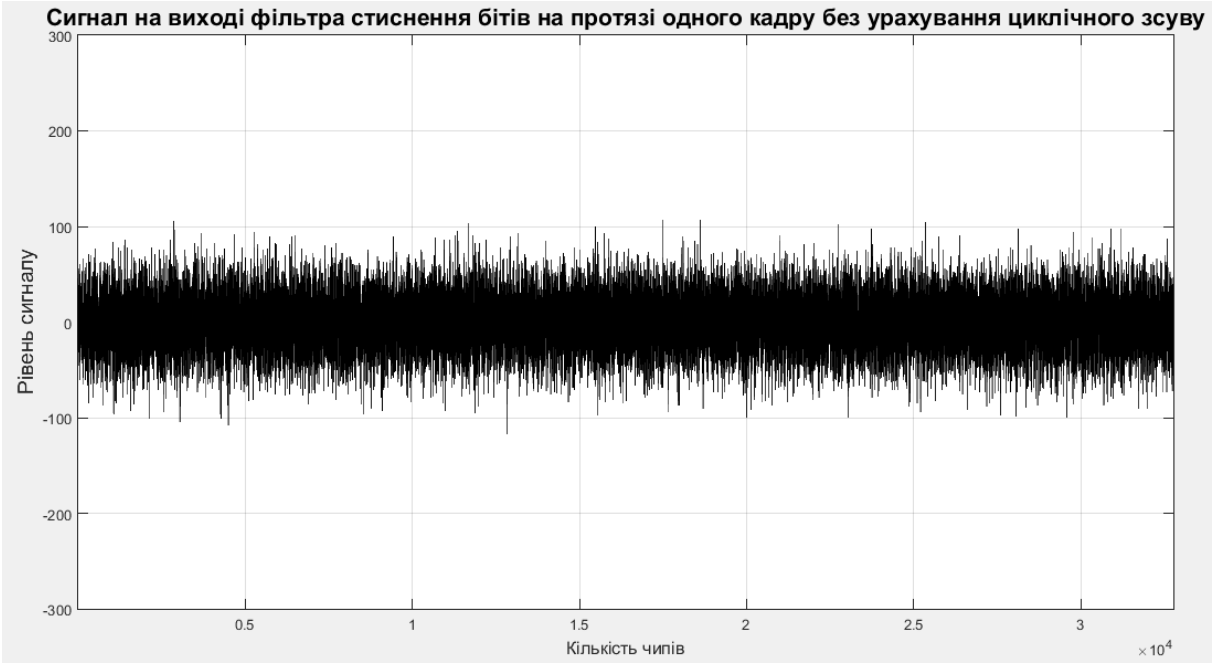

Рис.10. Сигнал на виході фільтра стиснення бітів на протязі одного кадру без урахування циклічного зсуву

ISSN 2663 - 4023

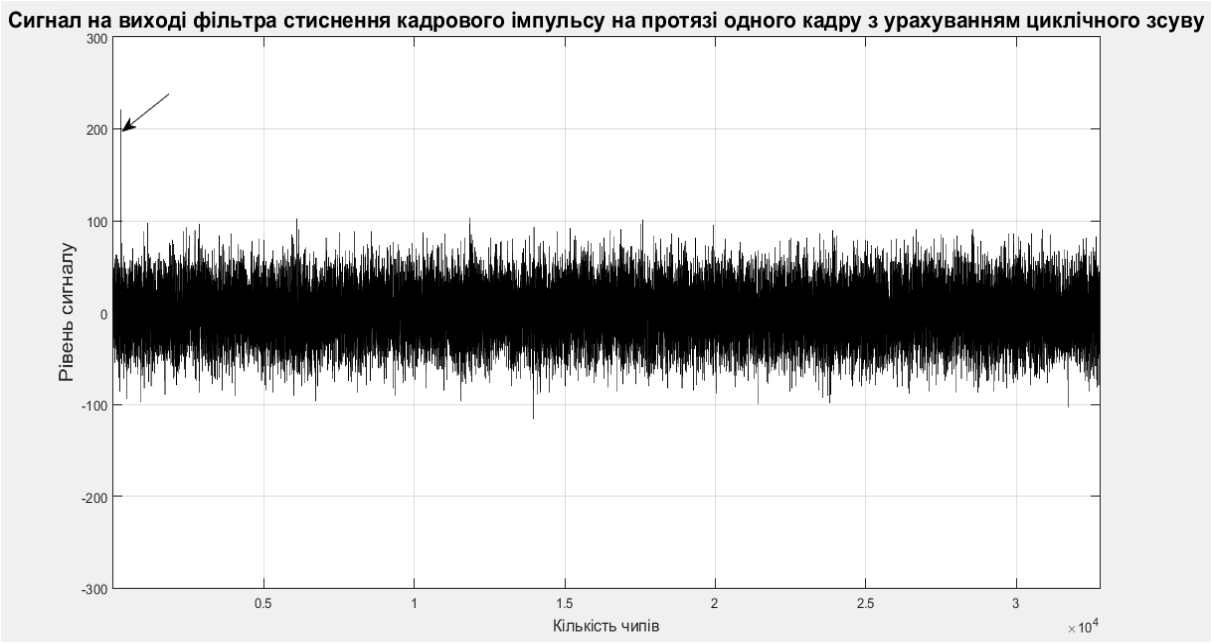

Рис.11. Сигнал на виході фільтра стиснення кадрового імпульсу на протязі одного кадру з урахуванням циклічного зсуву

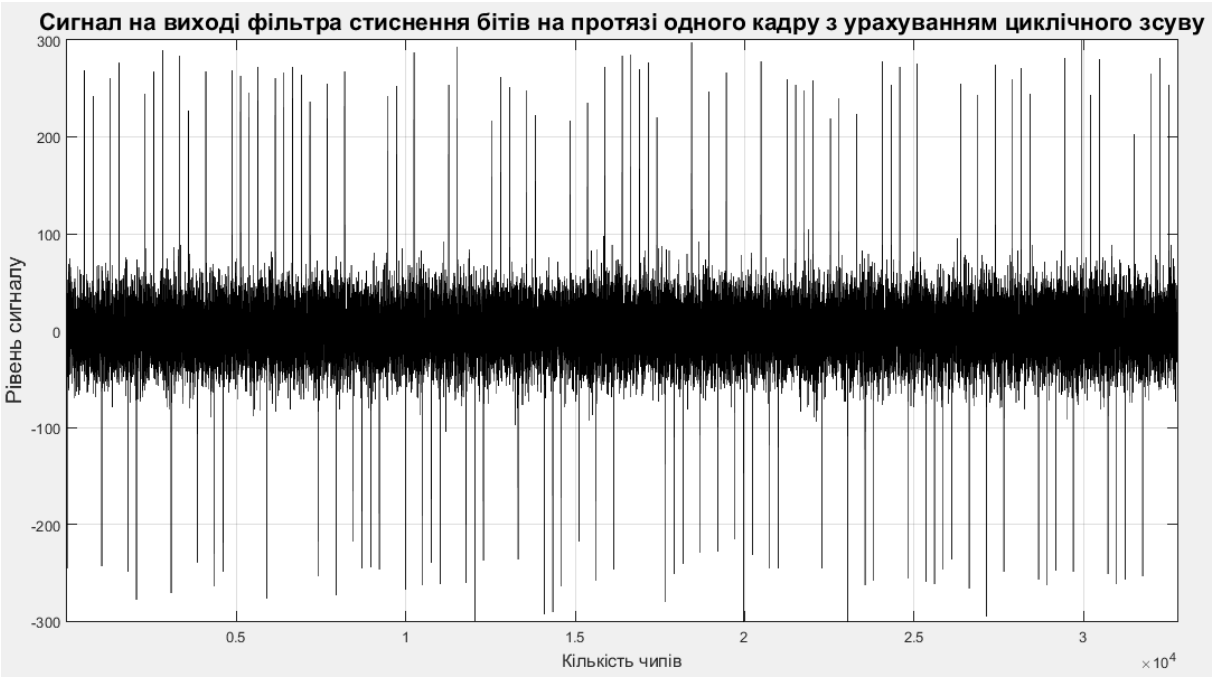

Рис.12. Сигнал на виході фільтра стиснення бітів на протязі одного кадру з урахуванням циклічного зсуву

4. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Телекомунікаційні канали передачі даних завжди знаходяться серед пріоритетних цілей кібернетичних зловмисників. Виходячи з цього, підвищенню завадозахищеності

та скритності передачі інформації в таких каналах в даній роботі приділено велику увагу.

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.

В роботі запропоновано побудова завадозахищеного та скритного каналу з двох псевдовипадкових кодових послідовностей: для розширення спектру бітів корисної інформації використовується послідовність з 256 чипів, в той час як для позначення меж кадру та забезпечення додаткового скремблювання інформації використовується послідовність з 32768 чипів.

Характеристики побудованого телекомунікаційного каналу досліджувалися шляхом комп'ютерного імітаційного моделювання.

На першому етапі було з'ясовано, що запропонований підхід дозволяє впевнено виявити кадрову структуру інформації яка передається, та виділити значення біт корисної інформації на фоні адитивної суміші корисного сигналу с завадами, що перевищують корисний сигнал в два рази по потужності.

На другому етапі, для подальшого підвищення захисту інформації від кібернетичних зловмисників запропоновано використовувати по-кадрові циклічні зсуви псевдовипадкової послідовності тривалістю 32768 чипів. Шляхом комп'ютерного моделювання було доведено, що при незнанні циклічних зсувів зловмисники не є в змозі перехопити інформацію, що передається. Для цього, теоретично, їм потрібно обробляти прийняті сигнали з усіма можливими циклічними зсувами, яких налічується 128. В такому випадку, завдання кібернетичних зловмисників значно ускладнюються.

Відомо [2], що існує 1800 примітивних поліномів 15 ступеня, які за своїми характеристиками ідентичні тому (1), що застосовано в роботі. За рахунок використання не тільки одного поліному з різними циклічними зсувами, а і всіх 1800, можливо ще більше підвищити скритність та завадозахищеність телекомунікаційного каналу.

Виходячи з цього, подальші дослідження слід спрямувати на вивчення характеристик телекомунікаційного каналу при використанні всіх поліномів з 1800 зазначених з різними циклічними зсувами. Авторам роботи цей напрямок вбачається дуже важливим та перспективним.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[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. 752p.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (9), 2020
ISSN 2663 - 4023

Oleksandr G. Pliushch
PhD in technical sciences, docent, professor of the department of Mobile and video information technologies
State University of Telecommunications, Kyiv, Ukraine
ORCID: 0000-0001-5310-0660
opliusch@yahoo.com

USE OF PSEUDO NOISE CODING SEQUENCE CYCLIC SHIFTS FOR TELECOMMUNICATION CHANNEL PERFORMANCE IMPROVEMENT

Abstract. An approach is proposed to design of noise immune and concealed data transfer channel for telecommunication networks. Attention is paid to securing hidden information transmission, as well as its protection from interception by rogue actors. The approach is based on the desired bits spectrum spreading and their additional scrambling by using pseudo noise coding sequences derived from primitive polynomials of eighth and fifteenth orders, which possess good auto and inter correlation 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.
Computer simulation is used to study performance of the designed telecommunication channel. The computer simulation helped to establish 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. Further improvement of information protection from interception is proposed to achieve by using cyclic shifts of 32768 chip-long pseudo noise coding sequence. Computer simulation helped to find out that ignorance of the cyclic shift leads to inability of information interception by the rogue elements. Research results, obtained in this paper, permit to claim that the designed telecommunication channel, with cyclic shifts according to a secret rule, could be successfully used in practical implementations of noise immune and concealed telecommunication networks.

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

REFERENCES

[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. 752p.