

Плющ О. Г., Вишнівський В. В., Прокопов С. В., Іщеряков С. М.

Державний університет телекомунікацій, Київ

ДОСЛІДЖЕННЯ ВИКОРИСТАННЯ СКРЕМБЛЮЮЧОЇ КОДОВОЇ ПОСЛІДОВНОСТІ В ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ ІНФОРМАЦІЙНИХ СИСТЕМ

Анотація: Розглянуті питання забезпечення завадозахищеності та прихованості передачі інформації в телекомунікаційних мережах інформаційних систем. Запропоновано використовувати для підвищення цих характеристик скремблюючі кодові послідовності, що здійснюють розширення спектру бітів, що пересилаються. З метою синтезу нових скремблюючих кодових послідовностей використовується примітивний поліном десятого порядку. Досліджено автокореляційні характеристики синтезованої скремблюючої кодової послідовності. Зроблено висновок про певні обмеження, що визначаються цими характеристиками. Для з'ясування можливостей використання синтезованої скремблюючої кодової послідовності в каналах передачі даних телекомунікаційних мереж, проведено комп'ютерне моделювання процесу пересилання набору бітів, спектр яких розширено отриманою послідовністю. В процесі здійснення комп'ютерного моделювання формувалася суміш з корисного сигналу у вигляді скрембленої бітової послідовності, внутрішніх шумів каналу передачі інформації та завадового шумового сигналу. В той час, як потужність внутрішнього шуму та завадового сигналу залишалася постійною, потужність бітової послідовності поступово приймала три дискретні значення. В результаті проведення дослідження встановлено що використання синтезованої скремблюючої кодової послідовності дозволяє здійснювати виділення бітів, що передаються, в умовах коли потужність шумового завадового сигналу та внутрішнього шуму каналу перевищує потужність корисного сигналу на величину до 18 дБ. Окреслені обмеження, що виникають при використанні синтезованої кодової послідовності. Зроблено висновок про можливість застосування синтезованої кодової послідовності при практичній побудові телекомунікаційних каналів інформаційних систем.

Ключові слова: телекомунікаційна мережа; примітивний поліном; скремблюючі кодові послідовності; показники якості каналу; комп'ютерне моделювання; інформаційна система.

Pliushch O.G., Vyshnivskiy V.V., Prokopov S.V., Ishcheryakov S.M.

State University of Telecommunications, Kyiv

STUDY OF SCRAMBLING CODING SEQUENCE UTILIZATION IN TELECOMMUNICATION NETWORKS OF INFORMATION SYSTEMS

Abstract: Problems of securing noise immunity and information transmission concealment in telecommunication networks of information systems are considered. In order to improve performance, it is proposed to use scrambling coding sequences, which spread the spectrum of the bits being transmitted. To synthesize new scrambling coding sequences, tenth degree primitive polynomial is used. Autocorrelation properties of the obtained scrambling coding sequence are studied. Limitations caused by those properties are deduced. In order to establish a possibility of synthesized scrambling coding sequence use in the telecommunication networks data transmission channels, it is carried out computer simulation of the transmission process of the bit set, whose spectrum is spread by the obtained sequence. In the process of computer simulation, a mixture of the desired signal in the form of a scrambled bit set, internal noise of information transmission channel and interfering signal was formed. While the powers of the internal noise and interfering signal remained constant, power of the bit sequence gradually assumed three discrete values. As a result of the research, it is established that utilization of the synthesized scrambling sequence permits to perform extraction of the bits being transmitted, under conditions in which the power of the noise interfering signal and the internal noise of the channel surpasses power of the desired channel by up to 18 decibel. The limitations set by the use of the synthesized coding sequence are described. An inference concerning a

© Плющ О. Г., Вишнівський В.В., Прокопов С.В., Іщеряков С.М. 2020

possibility of obtained coding sequence use in practical implementation of telecommunication channels of information networks is made.

Keywords: *telecommunication network; primitive polynomial; scrambling coding sequences; channel quality indicators; computer simulation; information system.*

Плющ А.Г., Вишневский В.В., Прокопов С.В., Ищеряков С.М.

Государственный университет телекоммуникаций, Киев

ИССЛЕДОВАНИЕ ПРИМЕНЕНИЯ СКРЕМБЛИРУЮЩЕЙ КОДОВОЙ ПОСЛЕДОВАТЕЛЬНОСТИ В ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ ИНФОРМАЦИОННЫХ СИСТЕМ

Аннотация: *Рассмотрены вопросы обеспечения помехозащищенности и скрытности передачи информации в телекоммуникационных сетях информационных систем. Предложено использовать для повышения этих характеристик скремблирующие кодовые последовательности, которые расширяют спектр передаваемых битов. С целью синтеза новых скремблирующих кодовых последовательностей используется примитивный полином десятого порядка. Исследованы автокорреляционные характеристики синтезированной скремблирующей кодовой последовательности. Сделан вывод об определенных ограничениях накладываемых этими характеристиками. Для установления возможностей использования синтезированной скремблирующей кодовой последовательности в каналах передачи данных телекоммуникационных сетей, произведено компьютерное моделирование процесса пересылки набора бит, спектр которых расширен полученной последовательностью. В процессе осуществления компьютерного моделирования формировалась смесь полезного сигнала в виде скремблированной битовой последовательности, внутренних шумов канала передачи информации и помехового шумового сигнала. В то время как мощности внутреннего шума и помехового сигналов оставались постоянными, мощность битовой последовательности последовательно принимала три дискретных значения. В результате проведения исследования установлено, что использование синтезированной скремблирующей кодовой последовательности позволяет осуществлять выделение передаваемых битов в условиях, в которых мощность шумового мешающего сигнала и внутреннего шума канала превышает мощность полезного сигнала на величину до 18 дБ. Определены ограничения, которые возникают при использовании синтезированной кодовой последовательности. Сделан вывод о возможности использования синтезированной кодовой последовательности при практической реализации телекоммуникационных каналов информационных систем.*

Ключевые слова: *телекоммуникационная сеть; примитивный полином; скремблирующие кодовые последовательности; показатели качества канала; компьютерное моделирование; информационная система.*

1. Вступ

Скремблюючі кодові послідовності широко використовуються у телекомунікаційних мережах. Вони дозволяють отримати кращу заводо захищеність та скритність бездротових телекомунікаційних мереж за рахунок розширення спектру сигналу що передається.

Автокореляційні характеристики скремблюючих кодових послідовностей в найбільшій мірі визначають якість передачі інформації в телекомунікаційних каналах. Пошук кодових послідовностей з гарними кореляційними показниками є окремою складною задачею.

Добре відомими є кодові послідовності отримані з примітивних поліномів. Такі тривалі кодові послідовності використовуються в системах мобільного зв'язку третього покоління [2,4]. Але використанню коротких кодових послідовностей не приділено достатньо уваги. Кодові послідовності, синтезовані з примітивних поліномів восьмого та дев'ятого порядків мають свої обмеження, тому важливим є дослідження характеристик послідовностей отриманих з поліномів порядку вищого за дев'ятий, наприклад десятій.

Вищесказане обумовлює актуальність і необхідність проведення досліджень в цьому напрямку.

2. Аналіз літературних даних і постановка проблеми

В роботі [6] надано найбільш повну та детальну інформацію про скремблюючі кодові послідовності, що використовуються в телекомунікаційних мережах. Описані шляхи генерування таких послідовностей та переваги які отримуються за рахунок їх використання. Тим не менш, ця робота не приділяє достатньої уваги дослідженню характеристик певних скремблюючих кодових послідовностей у реальному телекомунікаційному каналі. Вона носить більш теоретичний характер і в ній відсутні результати комп'ютерного моделювання.

Найбільша практична складова застосування скремблюючих кодових послідовностей присутня в [4]. В цій книзі наведено багато графічного матеріалу, що пояснює характеристики скремблюючих кодових послідовностей, та представлена довідникова інформація про примітивні поліноми, які можуть використовуватися для їх отримання. Між тим, в цьому джерелі інформації приділена максимальна увага скремблюючим кодовим послідовностям що використовуються в технології CDMA2000, в той час як інші досліджені поверхнево.

В роботах [2,3] розглянуто застосування скремблюючих кодових послідовностей в технології UMTS і перераховано більшість з них. Все ж таки, це джерело є більш загальним і не приділяє достатньої уваги перевірці характеристик скремблюючих кодів методами імітаційного моделювання.

Джерело [1] тільки поверхнево нагадує, що скремблюючі кодові послідовності можуть бути використані в телекомунікаційних каналах управління безпілотними летальними апаратами або дронами. При цьому, аналіз можливих кодів та дослідження їх характеристик не виконуються.

Робота [5] виглядає як така, що робить загальний огляд різних технологій, що використовуються в бездротових телекомунікаційних мережах; в ній скремблювання є тільки одним з багатьох підходів. Увага до синтезу та перевірці характеристик скремблюючих кодових послідовностей не приділяється.

У даній роботі зроблено спробу розв'язання вищеназваних проблем.

3. Мета і задачі дослідження

Метою роботи є пошук примітивного поліному десятого ступеня з наступним синтезом на його основі скремблюючої кодової послідовності і вивчення її характеристик при використанні у телекомунікаційних мережах.

Для досягнення поставленої мети розв'язуються наступні наукові задачі:

- отримання примітивного поліному десятого порядку для виконання синтезу відповідної псевдовипадкової кодової послідовності;
- синтез псевдовипадкової кодової послідовності на основі примітивного поліному десятого порядку;
- дослідження характеристик синтезованої кодової послідовності при використанні у телекомунікаційному каналі с завадами.

4. Результати дослідження

4.1 Вибір скремблюючої кодової послідовності та дослідження її характеристик

Для забезпечення відповідних характеристик телекомунікаційного каналу, скремблюючі кодові послідовності повинні демонструвати дуже гарні автокореляційні властивості. Такі властивості можуть бути створені у таких послідовностях, що синтезуються з використанням примітивних поліномів певного порядку. Скремблююча кодова послідовність з використанням примітивного поліному дев'ятого порядку згідно з порядком поліному складається з 511 чипів. Для подолання цих обмежень, пропонується дослідити телекомунікаційний канал, в якому використовується скремблююча кодова послідовність протяжністю 1023 чипи і яка є створеною з використанням примітивного поліному десятого порядку. Примітивні поліноми можливо отримувати за рахунок поліноміального ділення повного поліному певного порядку, але в джерелах інформації вже є приклади виведених

примітивних поліномів певного порядку, які можливо використовувати для синтезу кодових послідовностей [4].

Примітивний поліном десятого порядку над полем Галуа GF(2), який представлений в [4], виглядає наступним чином:

$$F(x)=x^{10}+x^3+1. \quad (1)$$

На рис.1. представлена псевдовипадкова скремблююча кодова послідовність синтезована згідно з (1). Ця кодова послідовність сформована в логіці «1» та «-1»; така логіка є більш зручною при роботі в телекомунікаційному каналі.

Кореляційні властивості скремблюючої кодової послідовності зображеної на рис.1 висвітлюються кривими представленими на рис.2. Цей рисунок показує результат обробки узгодженим стискаючим фільтром послідовності з п'яти біт (1,1,-1,-1,1); кожний з цих бітів є скремблований кодовою послідовністю наведеною на рис.1.

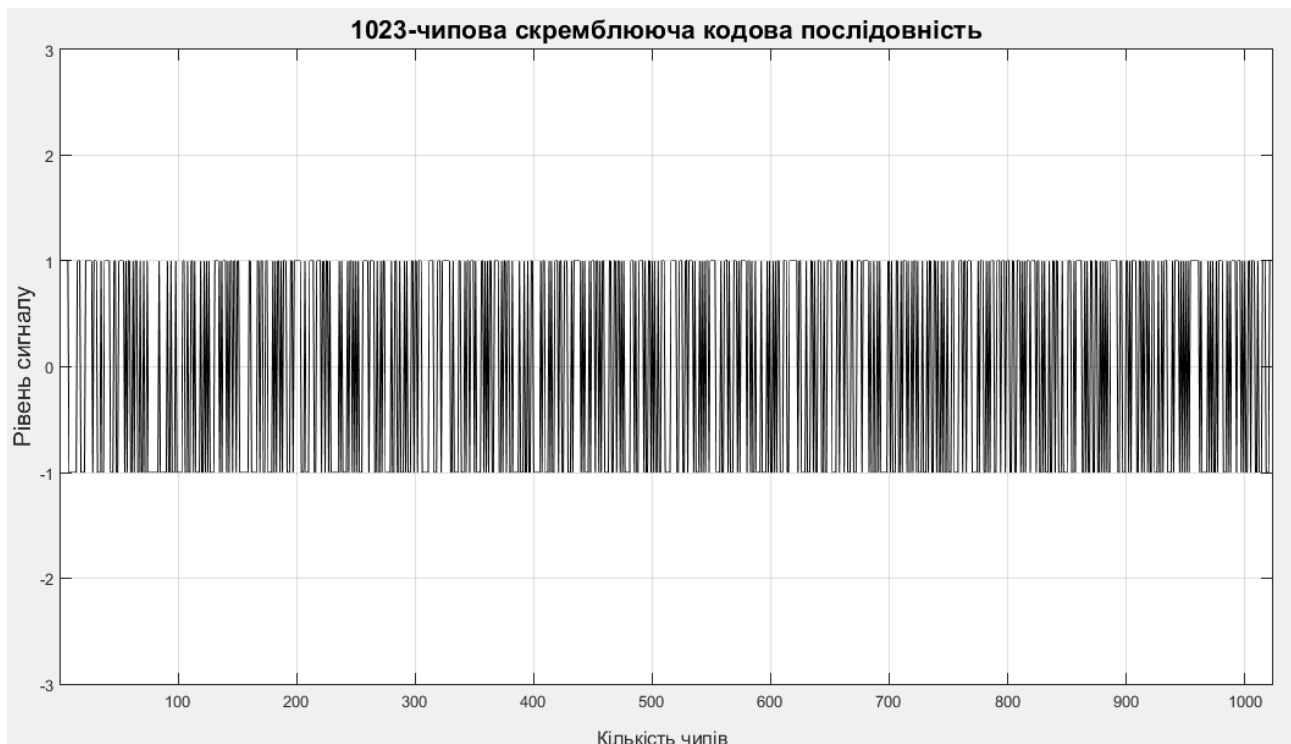


Рис. 1. Скремблююча кодова послідовність з 1023-чипів створена за рахунок використання (1)

Крива на рис.2 наочно демонструє унікальні властивості псевдовипадкових кодових послідовностей отриманих з примітивних поліномів. Ці властивості полягають в тому, що при нульовому зсуві значення автокореляційної функції дорівнює кількості чипів в послідовності, тобто 1023, в той час як при будь-якому зсуві значення автокореляційної функції дорівнює -1.

Але, у випадку коли біти змінюють свій знак, ця унікальна кореляційна властивість втрачається і виникають побічні пелюстки автокореляційної функції, як це показує рис. 2. Можливо зробити припущення, що ці бокові пелюстки будуть знижувати характеристики телекомунікаційного каналу, який використовує таку кодову послідовність.

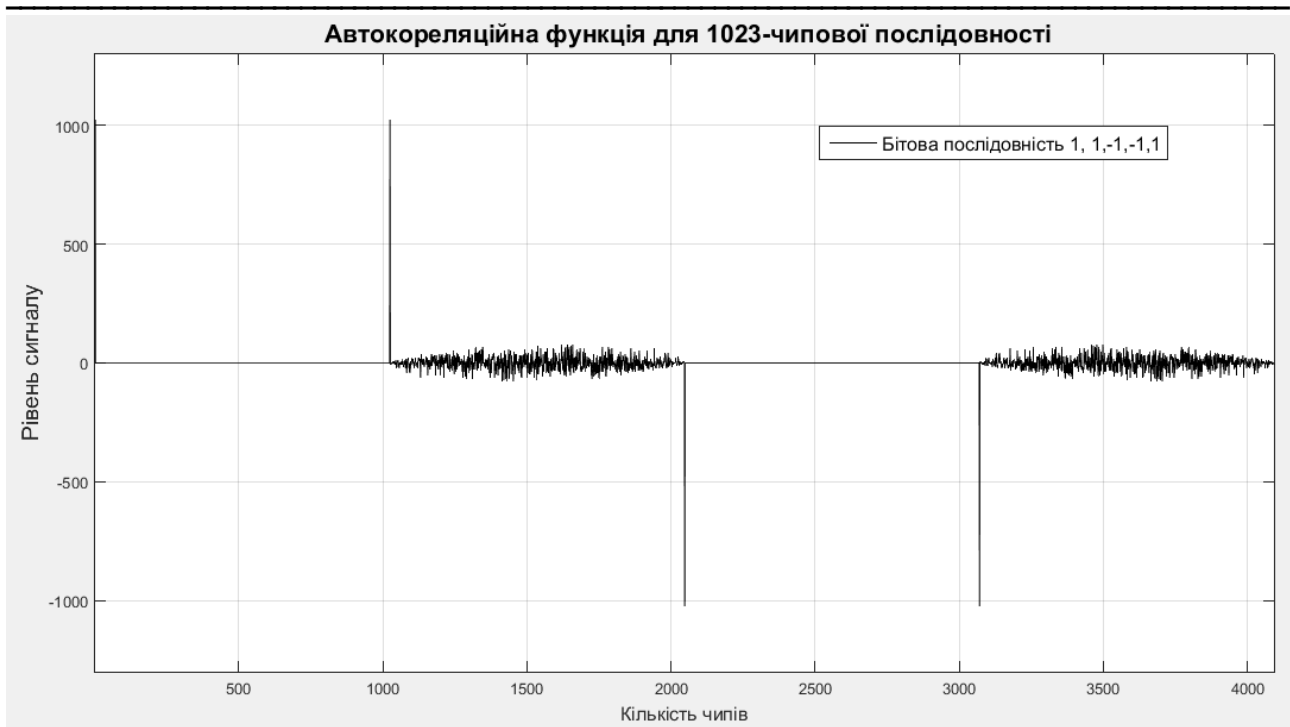


Рис. 2. Автокореляційна функція послідовності з п'яти різних бітів скрембльованих кодовою послідовністю, зображеною на рис.1

4.2 Дослідження характеристик телекомунікаційного каналу з внутрішніми шумами та зовнішньою завадою що використовує синтезовану кодову послідовність

Для дослідження характеристик телекомунікаційного каналу, в якому використовується бітова послідовність скрембльована синтезованою кодовою послідовністю з 1023 чипів, використовувалося комп'ютерне імітаційне моделювання. Моделювання проводилося для наступних умов:

- імітувалася комплексна адитивна суміш з 5 біт, що включає в себе корисний сигнал зі змінною потужністю, внутрішній шум каналу та завадовий сигнал;
- корисний сигнал представляється у вигляді комплексних відліків скремблюючої послідовності з урахуванням знаку певного біту інформації з, відповідно, фазами або 0 або π ;
- внутрішній шум каналу представлений як комплексні відліки з нормальним розподіленням ймовірності;
- завадовий сигнал так само представлений як комплексні відліки з нормальним розподіленням ймовірності;
- потужність внутрішнього шуму встановлена одиниця;
- потужність завадового сигналу встановлена три одиниці відносно рівня внутрішніх шумів;
- потужність корисного сигналу приймає відповідно значення 0.0625, 0.125 та 0.25 відносних одиниць;
- бітова послідовність складається з п'яти наступних біт: 1,1,-1,-1,1;
- створена сигнальна суміш пропускається через фільтр який є узгоджений зі скремблюючою кодовою послідовністю і, таким чином, виконує стиснення бітової послідовності.

Імітаційне моделювання здійснювалося за допомогою середовища Matlab.

Результати комп'ютерного імітаційного моделювання при дотриманні наведених вище умов та відносної потужності корисного сигналу 0.25 представлені на рис.3, рис.4, рис.5, рис.6, рис.7 та рис.8.

На рис.3, рис.4 та рис.5 зображені дійсна, уявна та модульна складові адитивної суміші сигналів на вході стискаючого фільтру. В цьому випадку сумарна потужність внутрішніх шумів каналу та завадового сигналу перевищує потужність корисного сигналу в 16 разів або на 12 дБ.

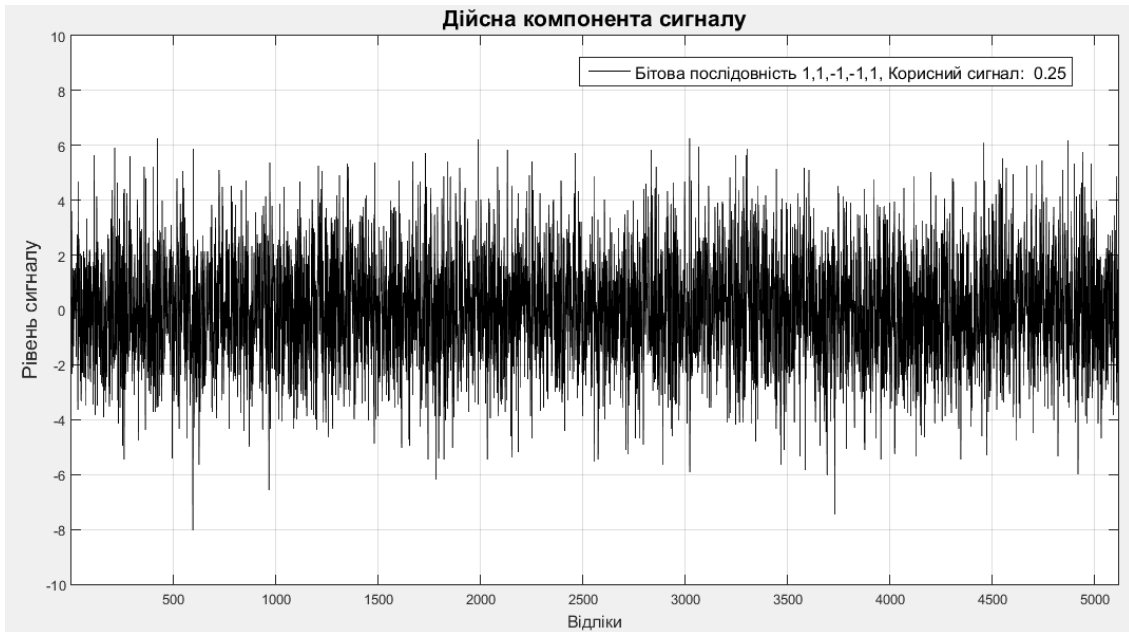


Рис.3. Дійсна компонента адитивної суміші корисного сигналу, внутрішнього шуму та завадового сигналу для відносної потужності корисного сигналу 0.25

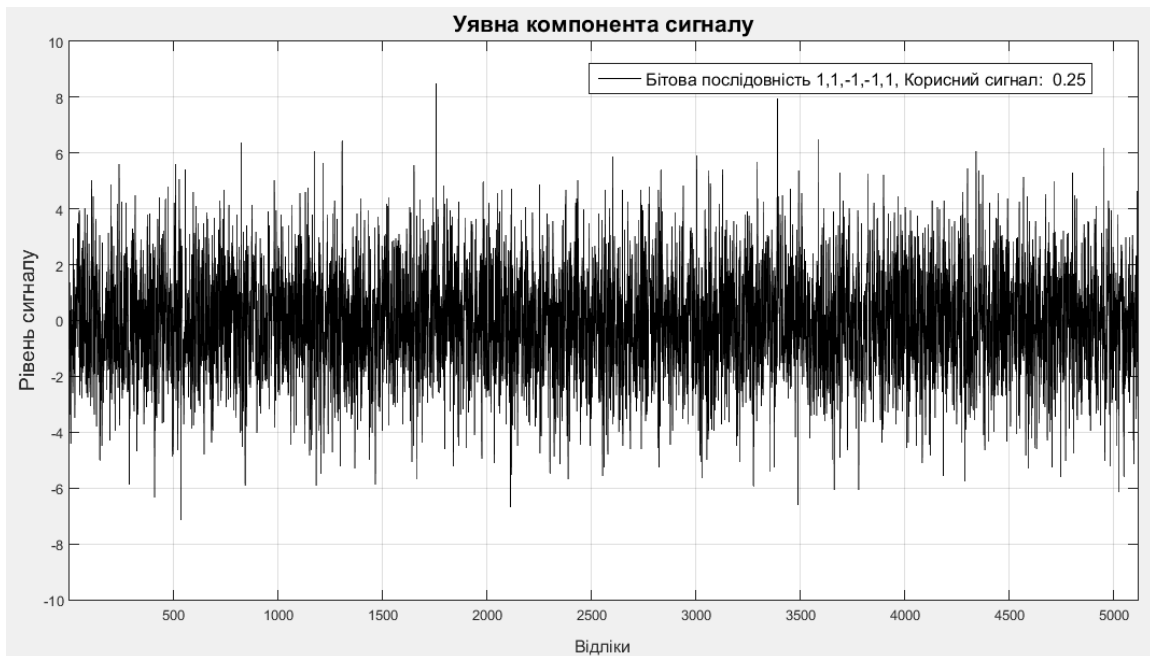


Рис.4. Уявна компонента адитивної суміші корисного сигналу, внутрішнього шуму та завадового сигналу для відносної потужності корисного сигналу 0.25

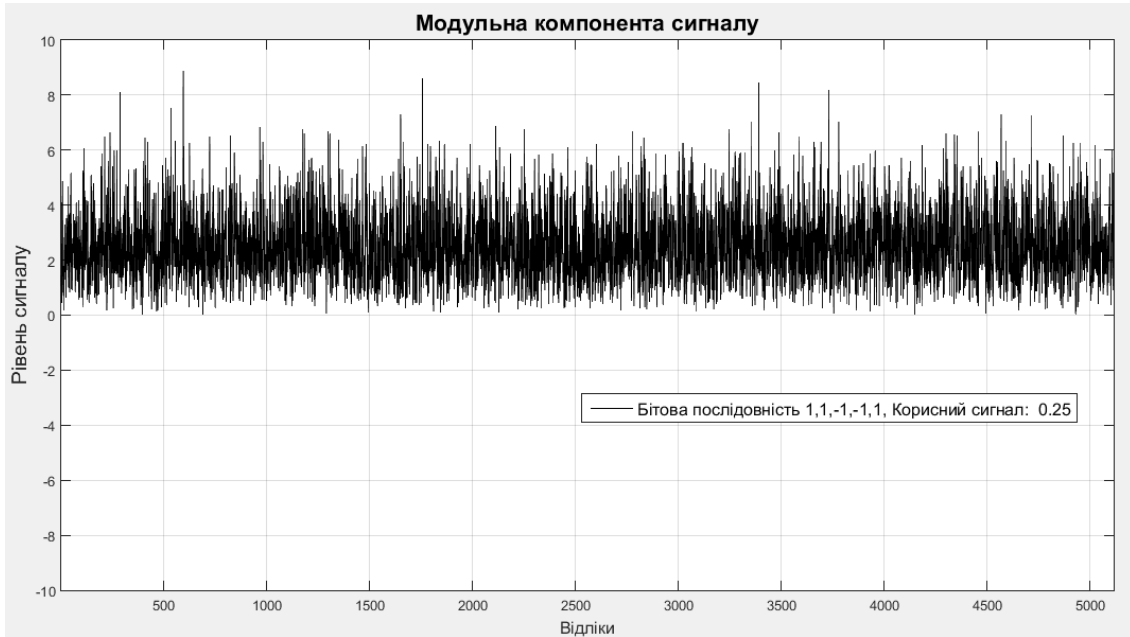


Рис. 5. Модульна компонента адитивної суміші корисного сигналу, внутрішнього шуму та завадового сигналу для відносної потужності корисного сигналу 0.25

Аналіз результатів наведених на цих рисунках дозволяє зробити висновок, що корисний сигнал є повністю захований у внутрішніх шумах каналу та заваді і не може бути виділений без знання його структури.

Рис.6, рис.7 та рис.8 показують дійсну, уявну та модульну складові сигналу на виході стискаючого фільтра. Вивчення результатів показує, що за рахунок стискання корисний сигнал впевнено виділяється на фоні шумових сигналів і може бути відновлена початкова скрембльована бітова послідовність.

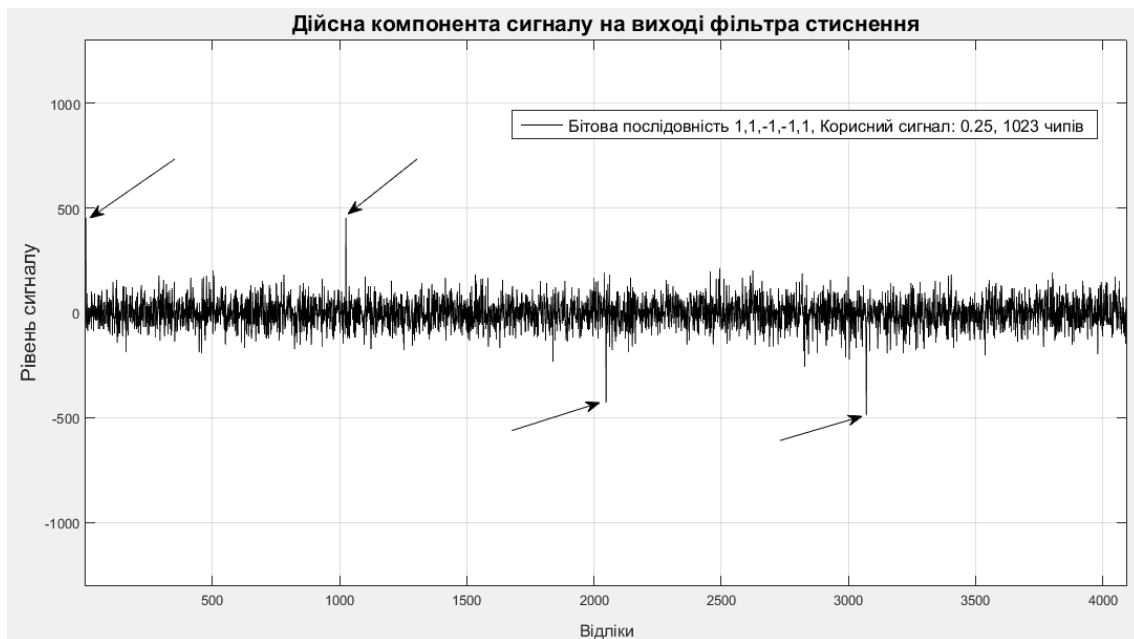


Рис.6. Дійсна компонента сигнальної суміші на виході фільтра стиснення для відносної потужності корисного сигналу 0.25

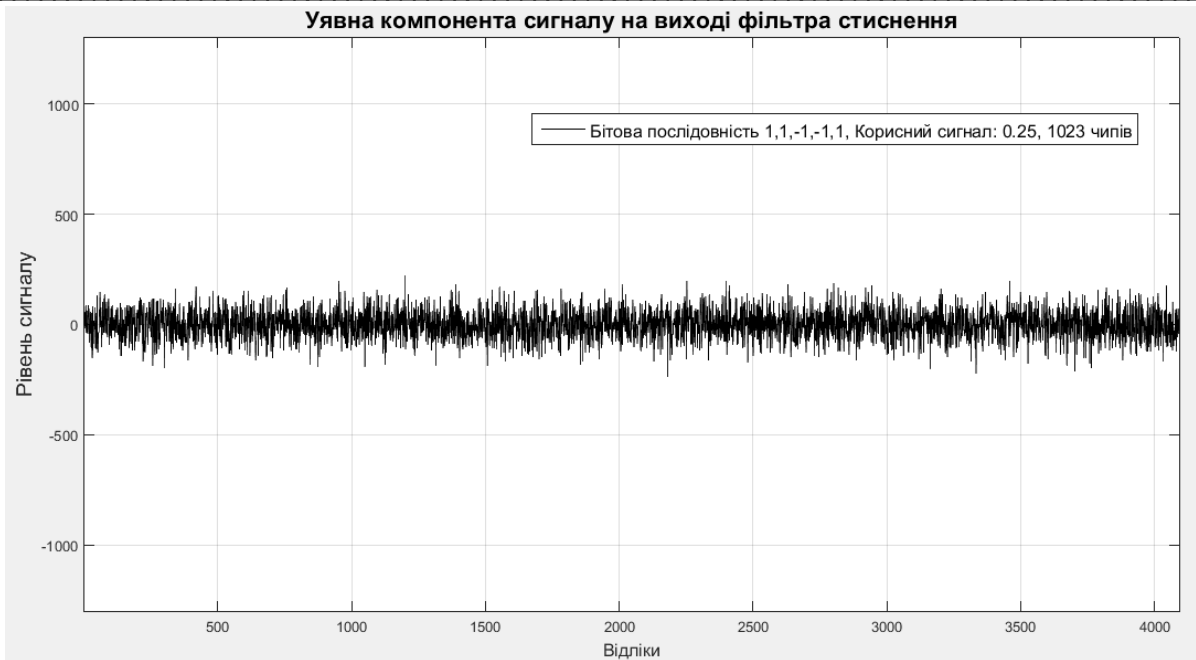


Рис.7. Уявна компонента сигнальної суміші на виході фільтра стиснення для відносної потужності корисного сигналу 0.25

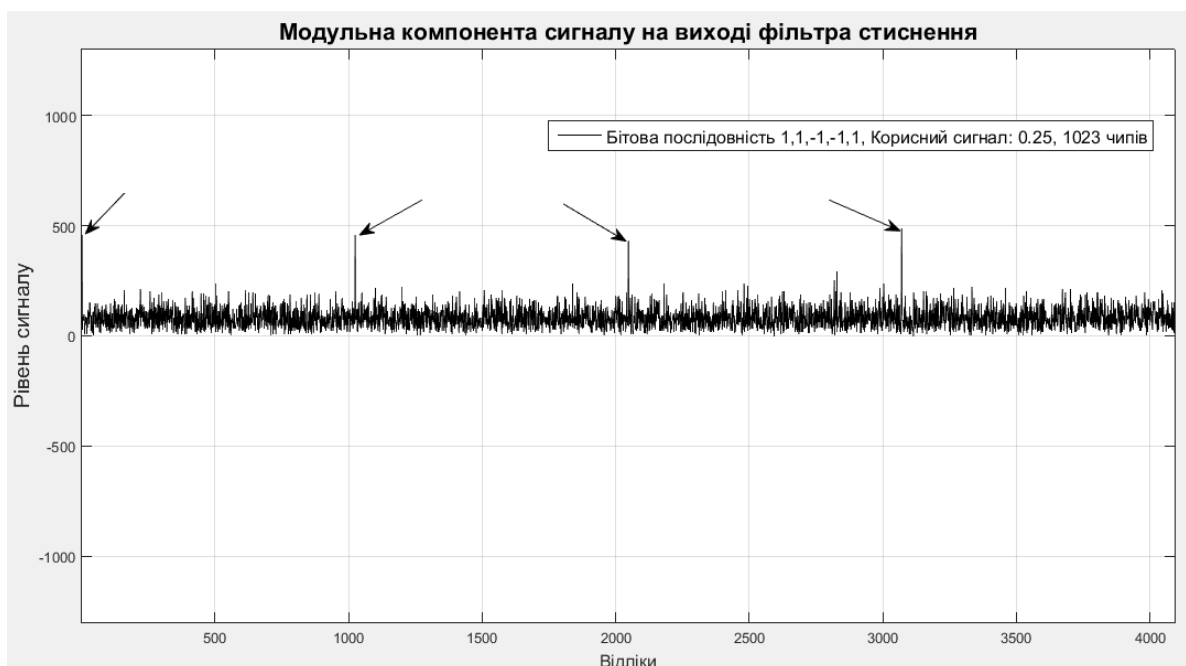


Рис. 8. Модульна компонента сигнальної суміші на виході фільтра стиснення для відносної потужності корисного сигналу 0.25

Стрілочки на рис.6 та рис.8 позначають біти корисного сигналу виділені при стисканні з суміші внутрішнього шуму та шумової завади.

Результати моделювання для наведених вище умов та відносної потужності корисного сигналу, що дорівнює 0.125, зображені на рис.9, рис.10 та рис.11. В цьому випадку сумарна потужність внутрішнього шуму та завади перевищує потужність корисного сигналу в 32 рази або на 15 дБ.

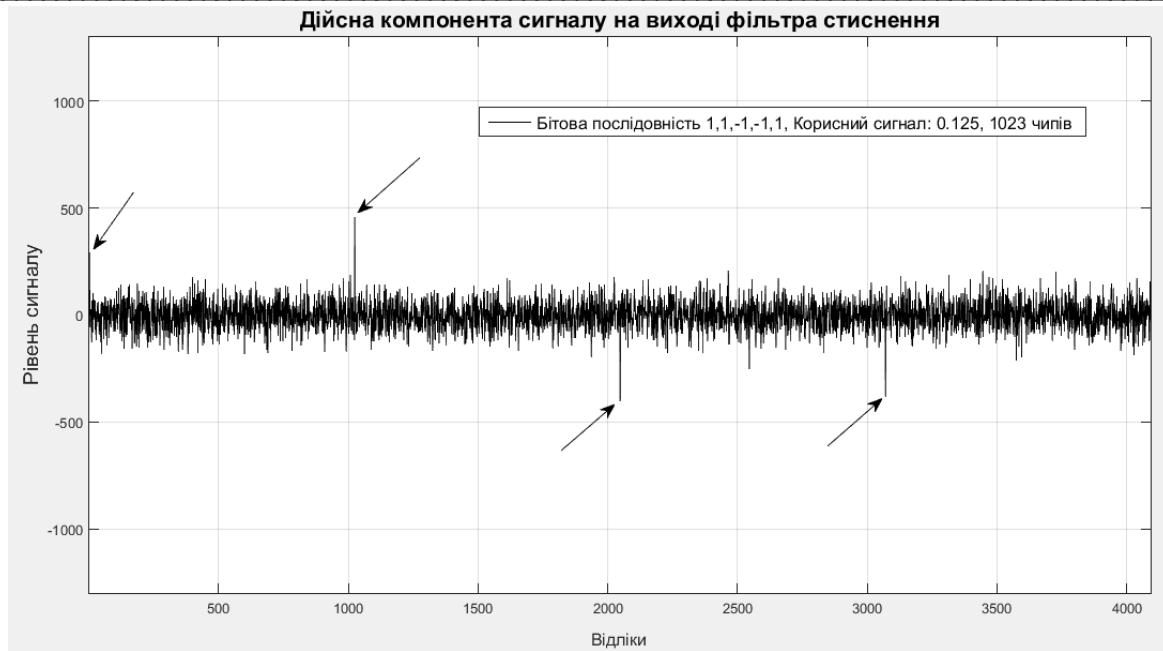


Рис.9. Дійсна компонента сигнальної суміші на виході фільтра стиснення для відносної потужності корисного сигналу 0.125

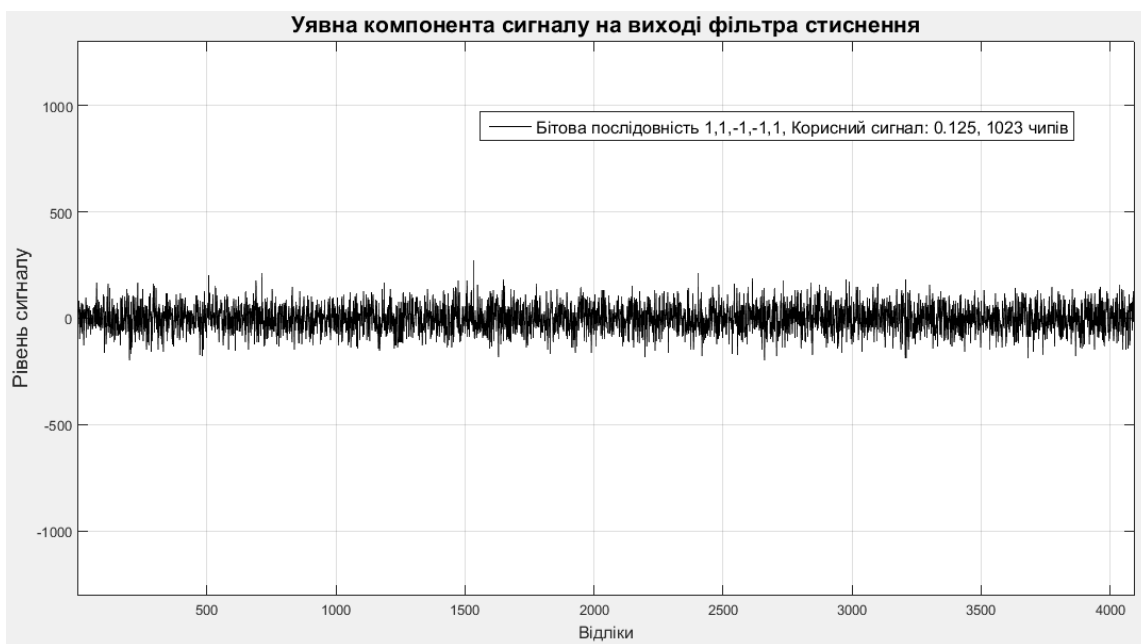


Рис. 10. Уявна компонента сигнальної суміші на виході фільтра стиснення для відносної потужності корисного сигналу 0.125

Стрілочки на рис.9 та рис.11, як і раніше, позначають біти корисного сигналу виділені при стисканні з суміші внутрішнього шуму та шумової завади.

Аналіз показує, що відношення корисний сигнал завада на виході фільтра стиснення погіршилося у порівнянні з попереднім випадком, але все одно є достатнім для відновлення бітової послідовності, що передається.

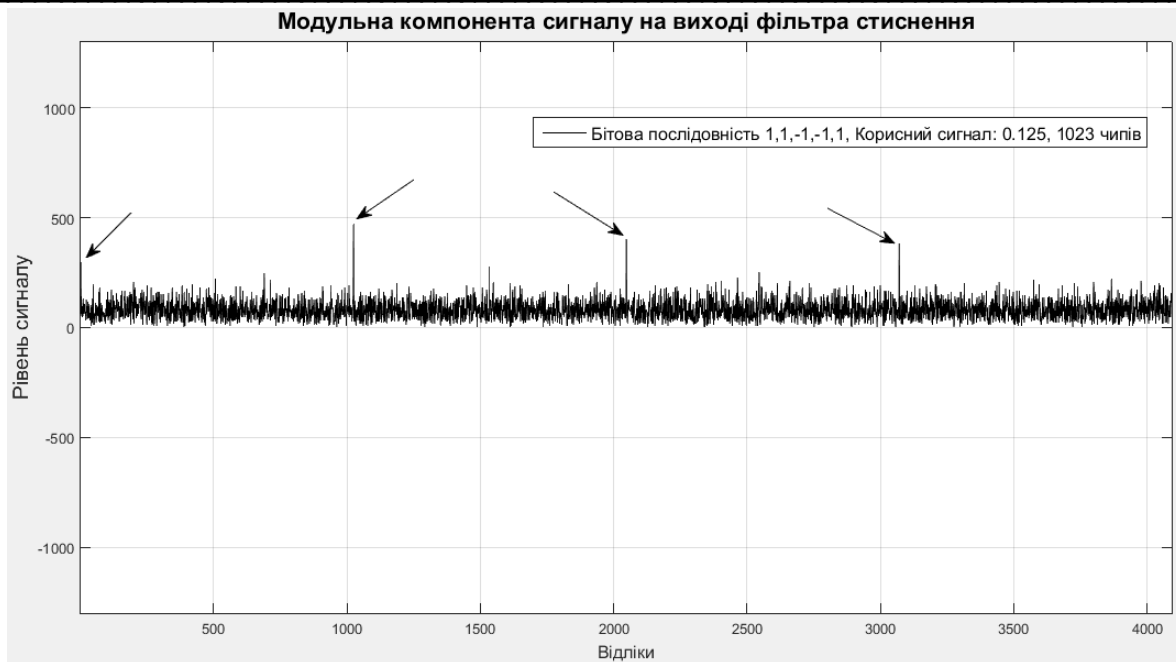


Рис. 11. Модульна компонента сигнальної суміші на виході фільтра стиснення для відносної потужності корисного сигналу 0.125

Результати моделювання для наведених вище умов та відносної потужності корисного сигналу що дорівнює 0.0625, зображені на рис.12, рис.13 та рис.14. В цьому випадку сумарна потужність внутрішнього шуму та завади перевищує потужність корисного сигналу в 64 рази або на 18 дБ.

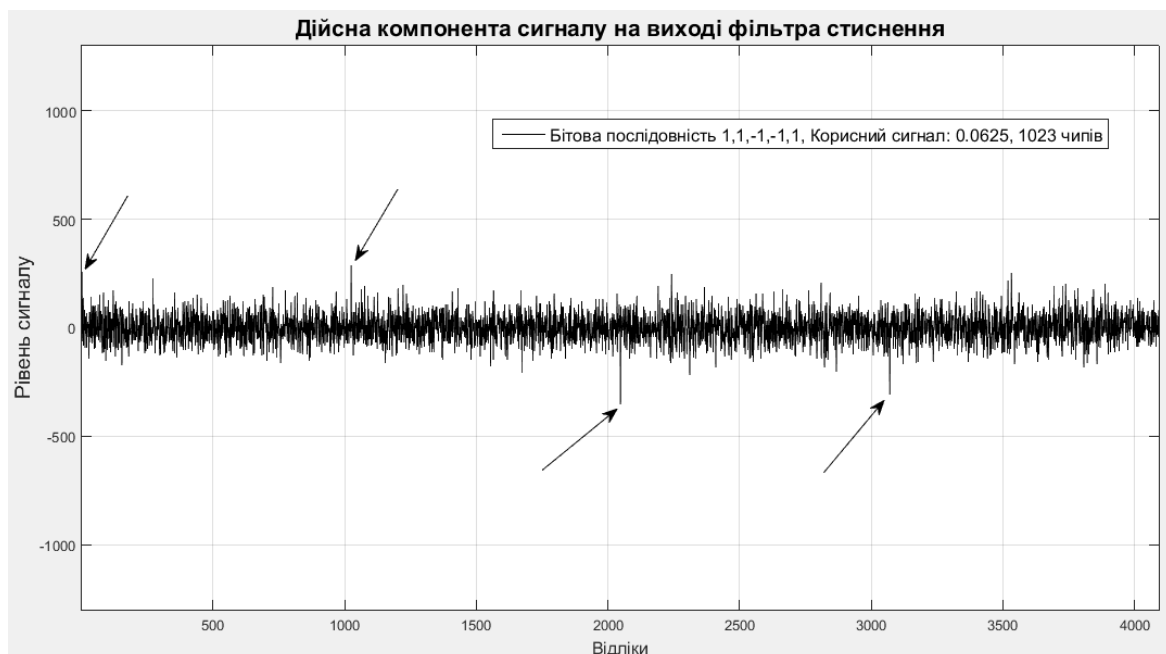


Рис. 12. Дійсна компонента сигнальної суміші на виході фільтра стиснення для відносної потужності корисного сигналу 0.0625

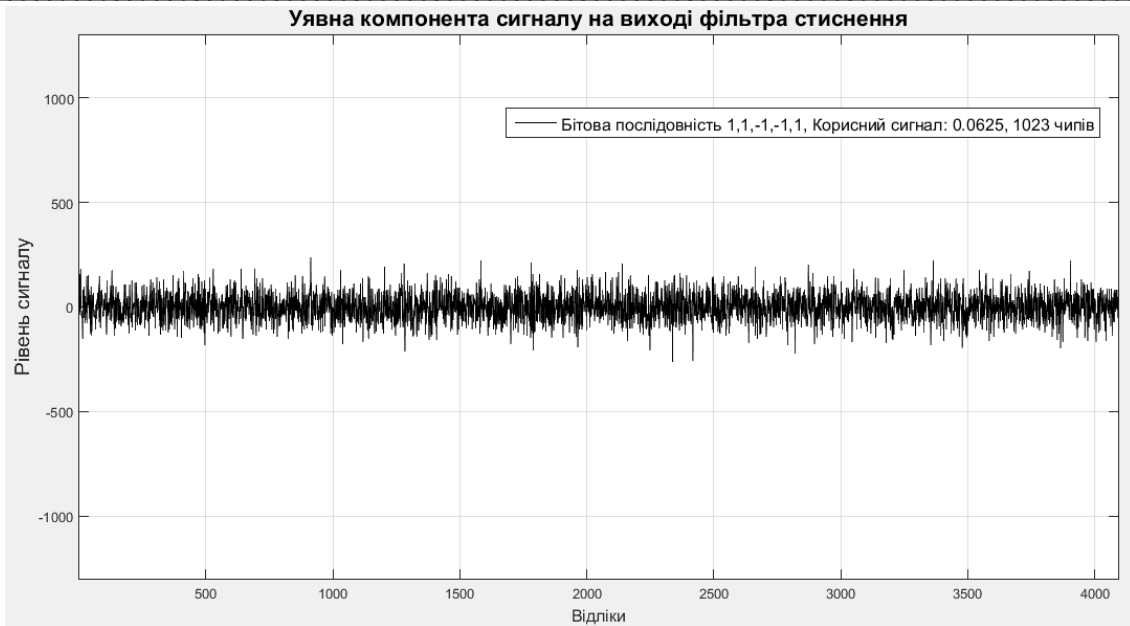


Рис. 13. Уявна компонента сигнальної суміші на виході фільтра стиснення для відносної потужності корисного сигналу 0.0625

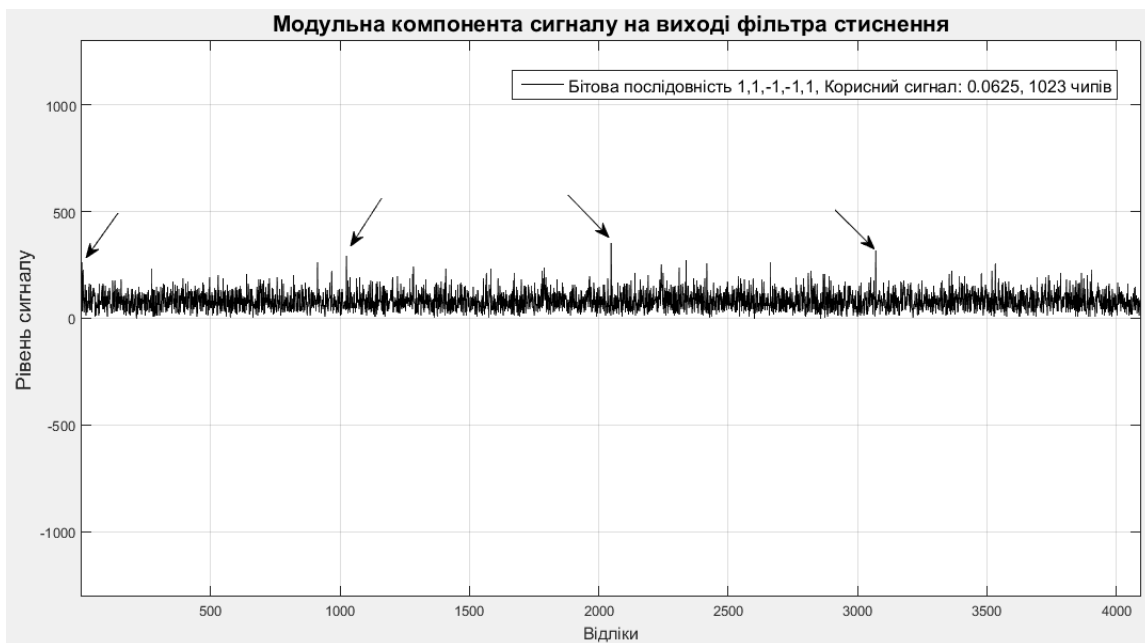


Рис.14. Модульна компонента сигнальної суміші на виході фільтра стиснення для відносної потужності корисного сигналу 0.0625

Аналіз показує, що відношення корисний сигнал завада на виході фільтра стиснення погіршилося, але все ще дозволяє відновити бітову послідовність, що передається. Треба зазначити, що, судячи з рис.12 та рис.14., можливості відновлення бітової послідовності дійшли своєї межі для коду що використовується. Стрілочки на рис.12 та рис.14 також позначають корисний сигнал після стиснення.

5. Обговорення результатів дослідження характеристик телекомунікаційного каналу з внутрішніми шумами та зовнішньою завадою що використовує синтезовану кодову послідовність

Скремблююча псевдовипадкова кодова послідовність має гарні автокореляційні властивості. Коли бітова послідовність, що передається, є незмінною, то ці автокореляційні

властивості є ідеальними. Якщо бітова послідовність, що передається, змінює знак, то ці властивості погіршуються.

Попереднє розширення спектру бітової послідовності синтезованою псевдовипадковою кодовою послідовністю з наступним стисканням цієї бітової послідовності у стискаючому фільтрі дозволяє виділити біти що передаються в телекомунікаційній мережі. Синтезована скремблююча кодова послідовність дозволяє відновити бітову послідовність, що передається, в ситуаціях коли сумарний рівень внутрішнього шуму та завади перевищує корисний сигнал на величину до 18 дБ. По результатам дослідження, це виглядає як найбільший виграш що може бути отриманий. Для отримання кращого результату треба збільшувати кількість бітів у скремблюючій кодовій послідовності.

Використання скремблюючої кодової послідовності отриманої з примітивного поліному десятого порядку дозволяє на 3 дБ покращити якість передачі бітів в телекомунікаційному каналі у порівнянні з тим, що дозволяє використання примітивного поліному дев'ятого порядку. Можливо припустити, що з кожним збільшенням в два рази кількості бітів у скремблюючій кодовій послідовності виграш у відношенні корисний сигнал завада буде зростати на 3 дБ.

6. Висновки

Скремблюючі кодові послідовності є потужним інструментом для покращення завадостійкості та скритності телекомунікаційних мереж інформаційних систем. Авторами синтезована 1023-чипова скремблююча кодова послідовність на основі примітивного поліному десятого порядку. Створена кодова послідовність продемонструвала гарні автокореляційні властивості. Було проведено комп'ютерне імітаційне моделювання обробки стискаючим фільтром суміші бітової послідовності, скрембленою синтезованою послідовністю, та внутрішніх шумів і завадового сигналу при різних рівнях корисного сигналу. Це дозволило дослідити потенціал використання цієї послідовності у телекомунікаційних каналах передачі даних. Виходячи з результатів моделювання можливо дійти висновків, що бітова послідовність може відновлюватися з адитивної суміші навіть у ситуаціях, коли сумарна потужність завадових сигналів перевищує потужність корисного сигналу на 18 дБ.

Порівняльна оцінка характеристик кодової послідовності синтезованої з примітивного поліному десятого порядку з тією, що синтезована з примітивного поліному дев'ятого порядку дозволяє стверджувати що виграш у якості передачі інформації склав 2 рази або три децибелі. Але це досягнуто за рахунок збільшення кількості чипів в послідовності в два рази і за рахунок збільшення ширини спектру що використовується, при збереженні швидкості передачі даних.

Синтезована скремблююча кодова послідовність може бути використана в перспективних телекомунікаційних мережах інформаційних систем для покращення їх завадозахищеності та скритності.

References

1. Edited by Kamesh Namuduri, Serge Chaumette, Jae H. Kim, James P. G. Sterbenz. UAV Networks and Communications. UK: Cambridge University Press, 2017. 242 p.
2. Andreas Springer, Robert Weigel. UMTS: The Physical Layer of the Universal Mobile Telecommunications System. USA: Springer Science & Business Media, 2013. 298 p.
3. Evgenii Krouk, Sergei Semenov. Modulation and Coding Techniques in Wireless Communications. USA: John Wiley & Sons, 2011. 680 p.
4. Lee, Jhong S., Miller, Leonard E. CDMA systems engineering handbook. Boston, London: Artech House, 1998. 1228 p.
5. Clint Smith, Daniel Collins. Wireless Networks. USA: McGraw Hill Professional, 2013. 752p.
6. Byeong G. Lee, Seok C. Kim. Scrambling Techniques for Digital Transmission. USA: Springer Science & Business Media, 2012. 448 p.