Форма № Н-9.02

Національний університет «Полтавська політехніка імені Юрія Кондратюка»
(повне найменування закладу вищої освіти)
Навчально-науковий інститут інформаційних технологій і робототехніки
(повне найменування інституту, назва факультету (відділення))
Кафедра автоматики, електроніки та телекомунікацій
(повна назва кафедри (предметної, циклової комісії))

Пояснювальна записка

до кваліфікаційної роботи

магістра
(ступінь вищої освіти)

на тему «**Розроблення алгоритму прихованого інформаційного обміну для бездротових систем передачі даних»**

Виконав: студент 2 курсу, групи 6 дТТ спеціальності 172 «Електронні комунікації та радіотехніка»
(шифр і назва напряму підготовки, спеціальності

Гладкий Є. Д._____
(прізвище та ініціали)
Керівник Фомін О. С.
(прізвище та ініціали)
Рецензент_____
(прізвище та ініціали)

Полтава – 2025 рік

Національний університет «Полтавська політехніка імені Юрія Кондратюка»
Інститут Навчально-науковий інститут інформаційних технологій і робототехніки
Кафедра Автоматики, електроніки та телекомунікацій
Освітній рівень магістр
Спеціальність 172 «Електронні комунікації та радіотехніка»

ЗАТВЕРДЖУЮ
завідувач кафедри автоматики, електроніки та телекомунікацій
_____ д.т.н., проф. О.В. Шефер
“ ” _____ 2024 р.

З А В Д А Н Н Я

НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Гладкому Євгенію Дмитровичу

1. Тема проекту (роботи) **«Розроблення алгоритму прихованого інформаційного обміну для бездротових систем передачі даних»**
керівник проекту (роботи) Фомін Олександр Сергійович, к.т.н.
затверджена наказом вищого навчального закладу від 09.08.2024 року № 818-ф,а

2. Строк подання студентом проекту (роботи) 19.12.2024 р.

3. Вихідні дані до проекту (роботи). Кількісна оцінка прхованості інформаційного обміну, не менше 0,6. Якісна оцінка, не нижче ріня В.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) Вступ. Аналіз принципів роботи бездротових систем передачі в умовах деструктивних впливів. Аналіз альтернативних методів забезпечення прихованого інформаційного обміну. Вибір критерія оцінювання прихованості інформаційного обміну в бездротових системах передачі даних. Комплексний підхід для оцінки прихованості інформаційного обміну. Розроблення моделі процесу забезпечення прихованого інформаційного обміну для бездротових систем передачі. Розроблення алгоритму реалізації моделі процесу забезпечення прихованого інформаційного обміну для бездротових систем передачі. Реалізація обчислювального методу оцінки прихованості інформаційного обміну на основі нечіткої логіки. Оцінка достовірності сигналів. Застосування розроблених моделей обчислювального методу. Висновки.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових плакатів): Актуальність предмет та об’єкт дослідження. Структурна схема системи звязку. Структурна схема системи зв’язку з однократною ретрансляцією. Залежність структурної прихованості від різних типів сигналів. Алгоритм забезпечення прихованості на основі хаотичних сигналів. Модель процесу забезпечення прихованосі інформаційним обміном. Модифікований алгоритм із ускладненою імітаційною вставкою. Графоаналітичне представлення програмної реалізації розробленого обчислювального методу. Модель системи з простими сигналами. Фазові портрети сигналів за різних умов. Графоаналітичне представлення розробленого алгоритму прихованості. Структурна схема пристрою імітозахисту.

Дата видачі завдання 02.09.2024 р.

КАЛЕНДАРНИЙ ПЛАН

Пор №	Назва етапів магістерської роботи	Термін та ообсяги виконання етапів роботи			Примітка (плакати)
1	Вступ. Аналіз принципів роботи бездротових систем передачі в умовах деструктивних впливів. Аналіз альтернативних методів забезпечення прихованого інформаційного обміну.	07.10.24		15%	Пл. 1
2	Вибір критерія оцінювання прихованості інформаційного обміну в бездротових системах передачі даних.	16.10.24	I	25%	Пл. 2, 3
3	Комплексний підхід для оцінки прихованості інформаційного обміну.	05.11.24		40%	Пл.4
4	Розроблення моделі процесу забезпечення прихованого інформаційного обміну для бездротових систем передачі.	12.11.24		50%	Пл.5
5	Розроблення алгоритму реалізації моделі процесу забезпечення прихованого інформаційного обміну для бездротових систем передачі.	19.11.24	II	60%	Пл.6
6	Реалізація обчислювального методу оцінки прихованості інформаційного обміну на основі нечіткої логіки.	26.11.24		70 %	Пл. 7,8
7	Оцінка достовірності сигналів отриманих за розробленим алгоритмом. Застосування розроблених моделей обчислювального методу.	11.12.24		90 %	Пл. 9
8	Висновки. Формування додатків. Оформлення кваліфікаційної роботи та підготовка графічних матеріалів.	19.12.24	III	100%	Пл. 10, 11

Студент _____ Гладкий Є. Д.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Фомін О. С.
(підпис) (прізвище та ініціали)

ЗМІСТ

ВСТУП

Останнім часом спостерігається стрімке зростання бездротових систем передачі, які активно впроваджуються у різні сфери людської діяльності. Однією з таких перспективних сфер є контроль територій різних об'єктів, у яких використовуються системи, що забезпечують збір інформації з розподілених об'єктів за допомогою датчиків з радіоповідомленнями, наприклад системи охоронно-пожежної сигналізації [1].

Перспективною сферою є спеціальна робототехніка, яка застосовується в різних критичних галузях, у яких використання людської праці є небезпечним, наприклад, патрулювання та охорона територій [2].

Ще однією перспективною галуззю є автомобільні системи безпеки, серед областей застосування яких, наприклад, можна виділити ідентифікацію та контроль доступу до транспортних засобів [3].

В даний час відбувається стрімке зростання технічної оснащеності та підготовленості осіб, які здійснюють протиправні дії, що призводить до різко зростання числа спроб здійснення злочинних посягань.

Для забезпечення прихованого інформаційного обміну в системах, що забезпечують збір інформації, найчастіше використовуються прості сигнали, які легко виявляються та перехоплюються.

Серед основних методів порушення працездатності систем, що забезпечують збір інформації, виділяють перешкоду, імітацію сигналу кінцевого обладнання, фіктивну заміну обладнання об’єкту системи зв'язку, а також прийом помилкової інформації від датчиків, які часто підмінюють або блокують [4]. У зв'язку з цим виникає завдання забезпечення прихованого інформаційного обміну в умовах зазначених деструктивних впливів, а також їх комплексної взаємодії.

У даний час для вирішення цього завдання застосовуються методи та алгоритми забезпечення прихованого інформаційного обміну, побудовані на основі криптографічних методів та шумоподібних сигналів [5, 6].

У першому випадку, прихований інформаційний обмін забезпечується в системах зв'язку простими сигналами, які повною мірою не дозволяють забезпечити прихованість інформації, що передається по бездротових каналах від перехоплення і придушення радіосигналу.

У другому випадку, прийнятний рівень прихованості теж не забезпечується, оскільки використовується мала кількість кодових послідовностей (наприклад, m-послідовності) і після прийому 2n реалізацій радіосигналу m-послідовність стає передбачуваною, через що радіосигнали таких систем зв'язку потенційно можна перехопити, підмінити чи придушити.

Разом з тим, в даний час активно почала розвиватися теорія використання в системах зв'язку хаотичних сигналів, які мають наступні характеристики, потенційно придатні для підвищення прихованості інформаційного обміну: велика кількість кодових конструкцій, непередбачуваність на великих інтервалах часу, підвищена прихованість.

Об'єкт дослідження: бездротова передача сигналу.

Предмет дослідження: методи та алгоритми забезпечення потайного інформаційного обміну в бездротових системах передачі даних.

Мета дослідження: підвищення прихованості інформаційного обміну в бездротових системах передачі за рахунок використання хаотичних сигналів за умов комплексних деструктивних впливів.

1 АНАЛІТИЧНА ЧАСТИНА

1.1 Аналіз принципів роботи бездротових систем передачі в умовах деструктивних впливів на процес інформаційного обміну

В останні роки спостерігається стрімке зростання бездротових систем передачі, які активно впроваджуються у різні сфери людської діяльності. Однією з таких перспективних сфер є контроль територій, наприклад системи охоронно-пожежної сигналізації.

Ще однією перспективною галуззю є спеціальна робототехніка. Робототехнічні системи (РТС) застосовуються в різних критичних областях, в яких використання людської праці є небезпечним і важкоздійсненним, наприклад, патрулювання та охорона територій та інші.

Через обмежені можливості провідних ліній бездротові канали зв'язку виглядають найбільш привабливими. Як ще одну перспективну область можна виділити автомобільні системи безпеки (АСБ). Серед областей їх застосування можливо виділити, наприклад, ідентифікацію та контроль доступу до транспортних систем на об'єкти, що охороняються та інші. В АСБ бездротові канали зв'язку також активно впроваджуються, оскільки дозволяють робити необхідні дії, наприклад ідентифікацію та контроль доступу транспортних засобів на віддаленій відстані.

В [7] показано на прикладі армії США, що в період з 2017 по 2023 кількість віддалено керованих безпілотних літальних апаратів зросла в 15 разів, а зростання віддалено керованих наземних РТС виявилося ще більшим, збільшившись в 60 разів (рис. 1.1). На ри. 1.1 введено такі позначення: а – безпілотні літальні апарати, б – наземні робототехнічні системи, 1 – 2017 рік, 2 – 2019 рік, 3 – 2021 рік, 4 – 2023 рік.

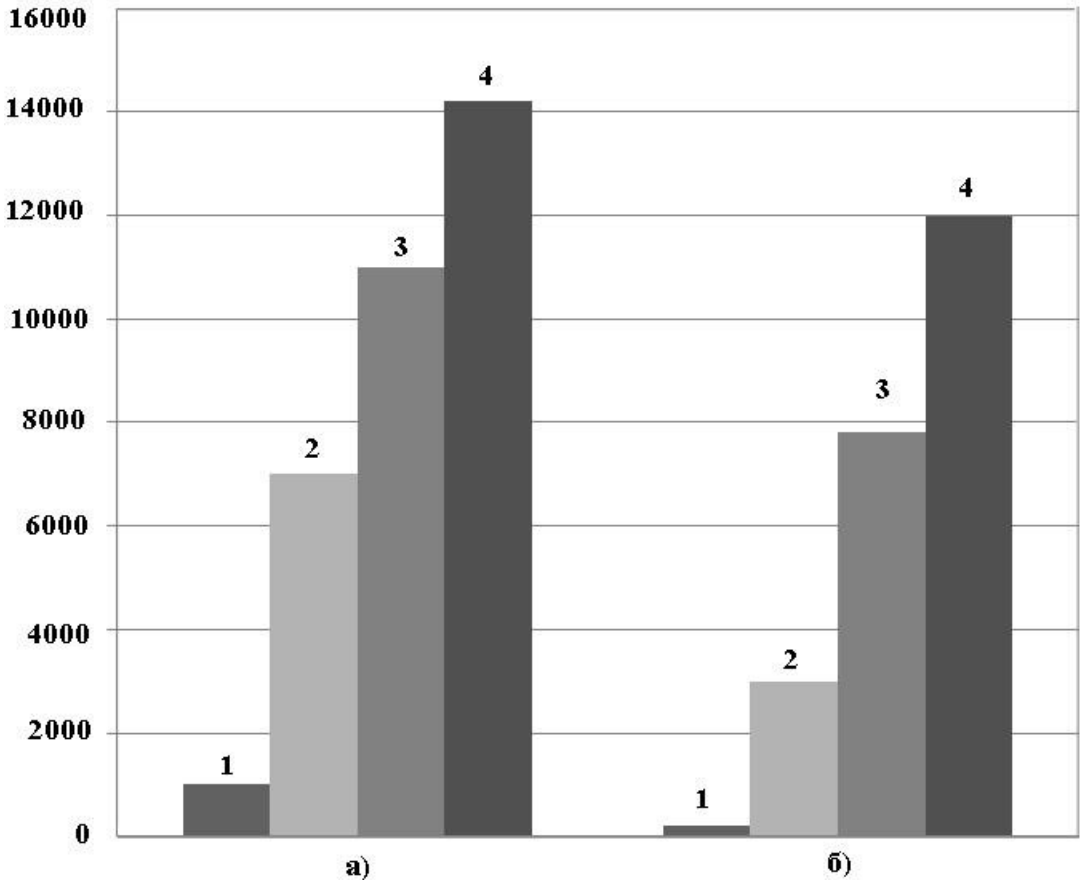


Рисунок 1.1 – Кількість віддалено керованих безпілотних літальних апаратів та віддалено керованих наземних РТС в США

На ри. 1.2 введено такі позначення: а – безпілотні літальні апарати, б – наземні робототехнічні системи, 1 – 2017 рік, 2 – 2019 рік, 3 – 2021 рік, 4 – 2023 рік.

Бездротові системи передачі даних у порівнянні з дротовими системами передачі даних мають наступні переваги [8]: простота організації, менші витрати на побудову та експлуатацію, можливість застосування за відсутності проводових ліній зв'язку та у надзвичайних ситуаціях, можливість оперативної зміни структури та параметрів систем, велика зона покриття та деякі інші.

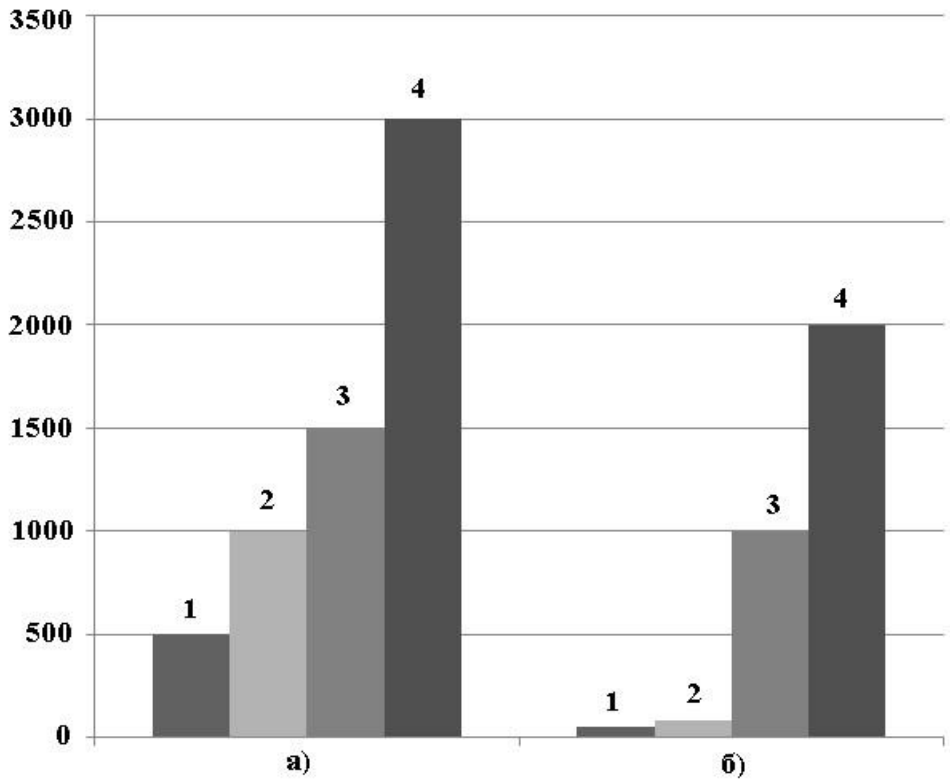


Рисунок 1.2 – Кількість віддалено керованих безпілотних літальних апаратів та віддалено керованих наземних РТС в Україні

Проаналізуємо відомі методи реалізації деструктивних впливів на радіоканал систем передачі. До основних видів деструктивних впливів віднесено такі фактори, що дестабілізують: перехоплення, перегляд, підміна, радіоелектронне придушення.

Слід зазначити, що дані фактори, що дестабілізують, можуть застосовуватися не тільки окремо, але й в комплексі. Комплексні деструктивні впливи, що впливають на бездротову систему передачі даних одночасно, можуть дестабілізувати її роботу достатньою мірою і для їх реалізації в даний час відомо багато методів і технологій [9].

Розглянемо практичну реалізацію описаних вище деструктивних впливів (перехоплення, перегляд, заміна, радіоелектронне придушення) на радіоканал для того, щоб показати, що рівень потенційного деструктивного впливу на нього завжди є досить високим. Так відомі методи часткового розкриття зашифрованої за допомогою криптографічних методів захисту

(КМЗ) інформації, наприклад, алгебраїчні та статистичні методи криптоаналізу [10], а також диференціальні та лінійні методи. Так само відомо багато технологій спрямованих на придушення радіосигналів, які досить успішно можуть порушити роботу як радіоканалу на основі простих сигналів, в якому інформація прихована за допомогою КМЗ, так і радіоканалу, заснованого на використанні шумоподібних сигналів (ШПС). Також досить поширеним є перехоплення радіосигналу за допомогою оптимального приймача [11].

Сучасні способи деструктивного впливу по відношенню до різних поширених технологій зв'язку з ШПС [12]: технологія на основі випадкового вибору частотно-часових позицій (ЧЧП), технологія на основі псевдовипадковою перебудовою робочої частоти (ППРЧ), технологія на основі використання фазозміни.

Загороджувальні перешкоди можна подати за допомогою наступного виразу:

$$P = U_{mш}(t)\cos[\omega_{p1}t + \phi_{p1}(t)], \tag{1.1}$$

де $U_{mш}(t)$ – закон зміни огинаючої перешкоди, $\omega_{p1}(t)$ – закон зміни фази перешкоди, φp_1 – середня частота перешкоди.

Виявлення здійснюється за рахунок використання сигналу, що приймається в якості опорного гармонійного коливання.

Для систем зв'язку з ШПС небезпечними перешкодами є імітуючи загороджувальні перешкоди, які описуються наступним виразом:

$$P(t) = \sum_{i=1}^{n} K_i U_m Q_i(t - t_d - \tau_i)\sin[2\pi(L \pm \Delta f)(t - t_d - \tau_i) + \phi], \tag{1.2}$$

де K_i – коефіцієнт, що враховує рівень загороджувальної перешкоди, що імітує, U_m – амплітуда сигналу, Q_i – тип модуляції і кодова послідовність, L – несуча частота.

Отже, можна зробити такі проміжні висновки:

- в даний час проблемі застосування комплексних деструктивних впливів (перехоплення, перегляд, заміна, радіоелектронне придушення) приділяється недостатньо уваги;

- часто наголошується, що проблема забезпечення прихованості радіоканалу є актуальною і вимагає нових рішень через те, що існуючі підходи не завжди можуть впоратися із завданням щодо забезпечення прихованості радіоканалу від деструктивних впливів.

Загальна структура радіоканальної системи зв’язку представлена рис. 1.3.

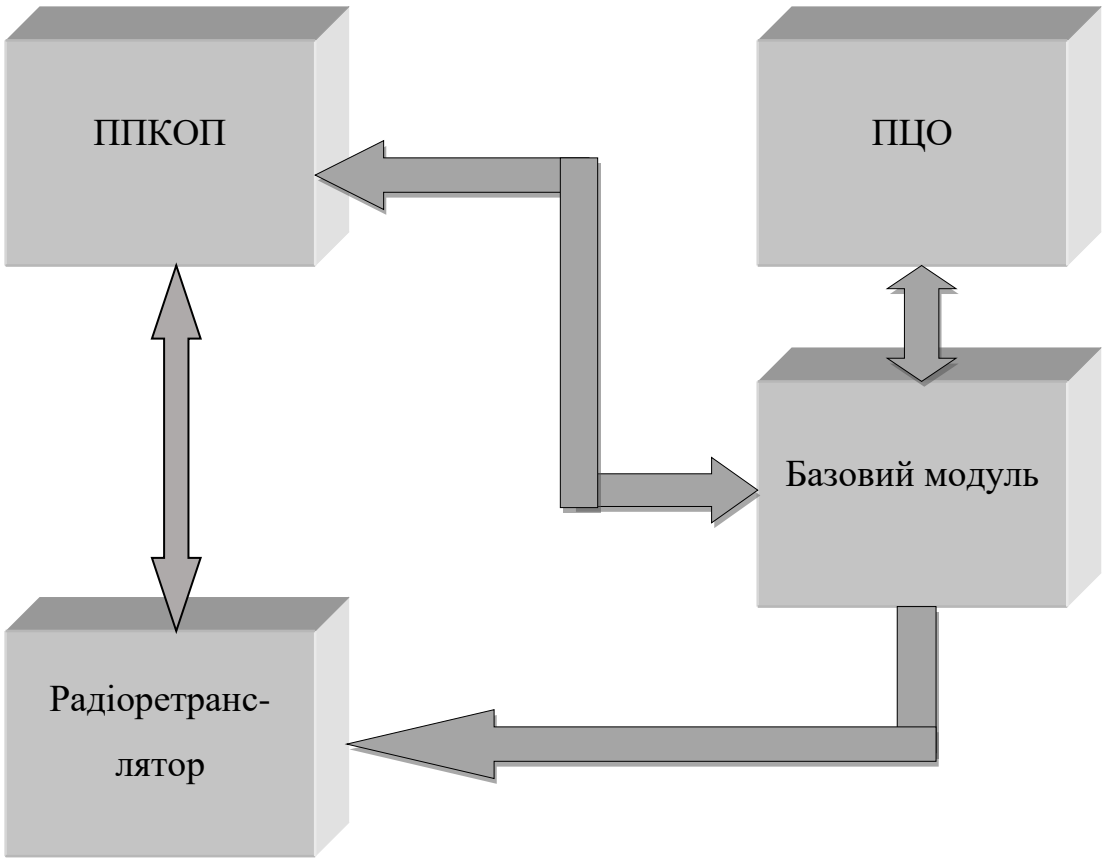


Рисунок 1.3 – Спрощена структурна схема системи зв’язку

До складу системи входять: ППКОП – прилад приймально-контрольний охоронно-пожежний, ПЦО – пульт централізованої охорони.

Для забезпечення потайного інформаційного обміну реалізовані способи криптографічного захисту інформації та захисту об'єктового обладнання від заміни, шляхом передачі за командою з ПЦО унікального номера об'єкта, які забезпечують прихованість від перегляду та заміну даних, що передаються. Разом з тим, дані способи не забезпечують прихованість від перехоплення і радіоелектронного придушення даних, що передаються, так як в даному випадку передача в каналі зв'язку здійснюється за допомогою гармонійних сигналів, представлених частотною модуляцією.

Як відомо, з розширенням смуги частот радіосигналу, з'являються труднощі у його виявленні з допомогою систем радіотехнічної розвідки, тобто канал зв'язку стає більш потайним. На рис. 1.4 наведено спектри системи зв'язку із простими сигналами (а) та системи зв'язку з шумоподібними сигналами (б) на фоні спектру шумів.

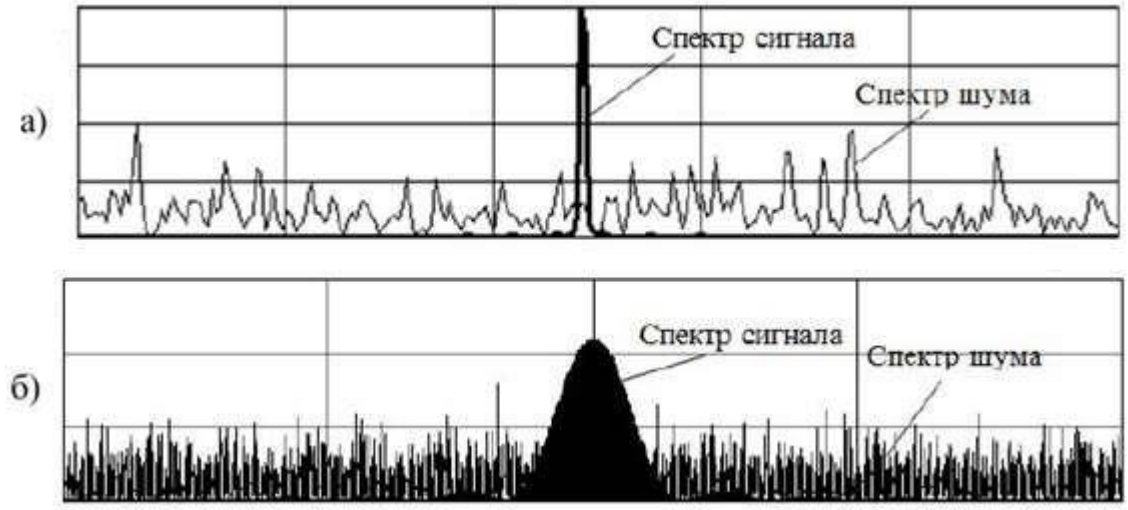


Рисунок 1.4 – Спектри сигналів на фоні спектра шумів:
а) простий сигнал, б) шумоподібний сигнал

Як видно з рис. 1.4, маємо якісну оцінку прихованості системи зв'язку, яка заснована на використанні простих сигналів, що легко виявляються. Таким чином, системи зв'язку засновані на використанні простих сигналів,

досить легко перехоплюються і пригнічуються, що свідчить про їх низьку як енергетичну, так і структурну прихованість.

Прихованість даної системи, як бездротової системи передачі на основі простих сигналів, дорівнює $P_{прих}$=0,2.

На рис. 1.5 наведено найпростішу структурну схему системи зв’язку з одноразовою ретрансляцією.

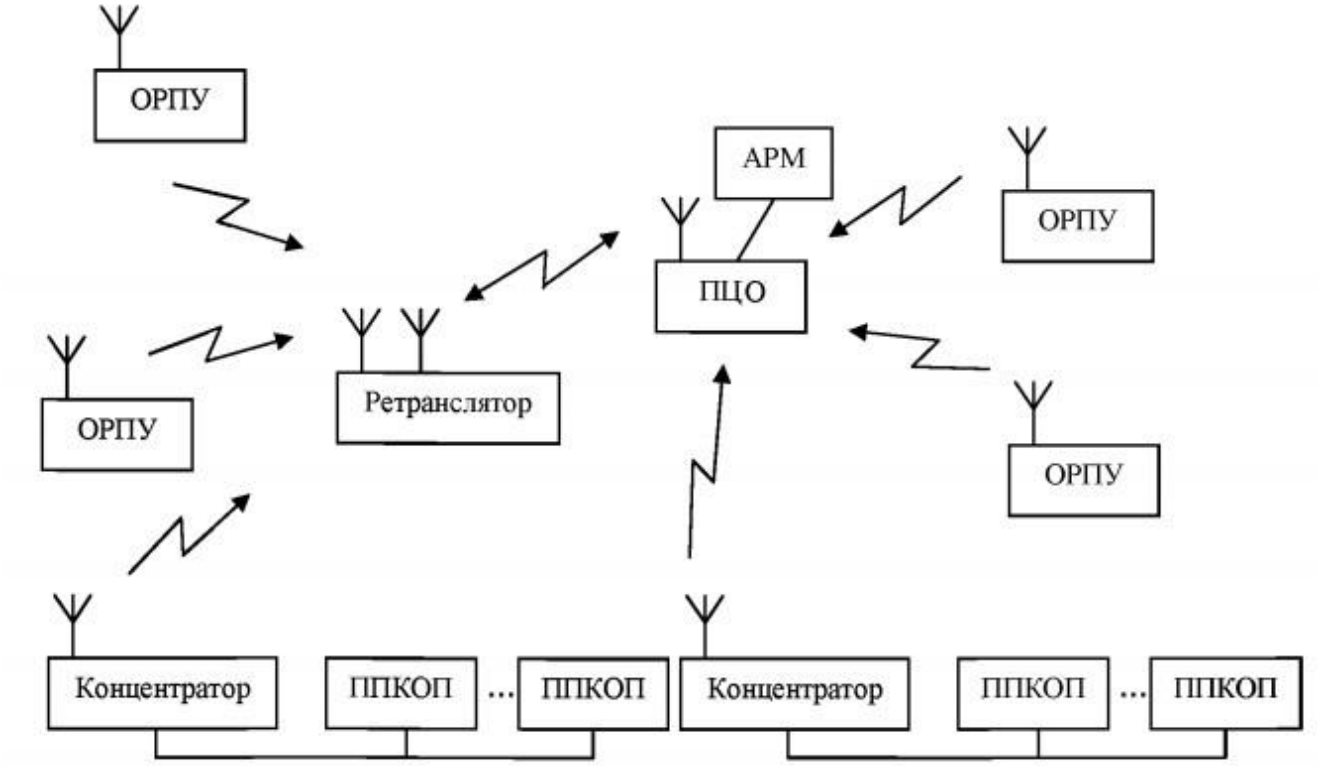


Рисунок 1.5 – Найпростіша структурна схема системи зв’язку з однократною ретрансляцією

До складу системи входять: ОРПУ – об'єктовий радіопередавальний пристрій, АРМ – автоматизоване робоче місце, ППКОП – прилад приймально-контрольний охоронно-пожежний, ПЦО – пульт централізованої охорони.

Відмінною особливістю даної системи ОПС є використання для забезпечення прихованості, крім елементів криптографічного захисту інформації, передача бітової інформації за допомогою коду Баркера за таким

правилом: кожен біт передається прямим (якщо біт дорівнює «1») або інверсним (якщо біт дорівнює «0 ») з кодом Баркера завдовжки рівним 7 біт. Отже, реалізується пряме розширення спектра. Описані технології в даному прикладі забезпечують прихованість від перегляду та підміни, однак вони не забезпечують прихованість від перехоплення і радіоелектронного придушення даних, що передаються, так як в даному випадку передача в каналі зв'язку здійснюється за допомогою гармонійних сигналів, представлених частотною модуляцією. Прихованість даної системи, як бездротової системи передачі на основі шумоподібних сигналів (ШПС) і частотної модуляції, дорівнює $P_{прих}$=0,4.

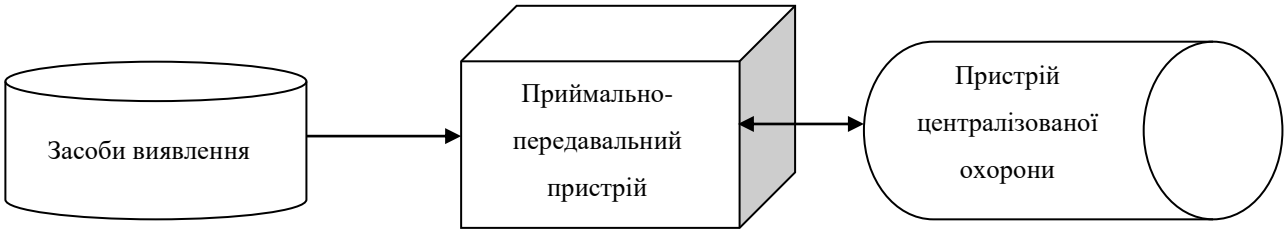


Рисунок 1.6 – Спрощена структурна схема системи зв’язку

Відмінною особливістю даної системи (рис.1.6) є використання для забезпечення скритності ППРЧ, при якій робоча частота сигналу перебудовується в широких межах виділеного частотного діапазону відповідно до псевдовипадкового коду, відомого на приймальній стороні і невідомого для можливого постановника перешкод.

Разом з тим, даний підхід не забезпечує прихованість від перехоплення і радіоелектронного придушення даних, оскільки в даному випадку передача в каналі зв'язку здійснюється за допомогою гармонічних сигналів, представлених частотною модуляцією. Прихованість даної системи, як бездротової системи передачі на основі ШПС і частотної модуляції, дорівнює $P_{прих}$=0,4.

Як видно з рис. 1.4, системи зв'язку з урахуванням шумоподібних сигналів виявити важче, ніж системи зв'язку з урахуванням простих сигналів.

Разом з тим відомо, що системи зв'язку на основі шумоподібних сигналів зазвичай використовують лінійні та нелінійні псевдовипадкові послідовності (ПВП) для розширення спектра (наприклад, m-послідовності), які належать до категорії послідовностей з малим обсягом послідовностей та складністю зміни алгоритму своєї роботи. Зокрема, структура генератора ПВП буде відома при обробці 2n символів ПВП, де n - це розрядність генератора. Так само те, що ПВП, що знімаються з різних елементів пам'яті, циклічно зрушені один відносно одного. Крім того, у цих системах використовується частотна модуляція. Ц свідчить про недостатню прихованість даних систем зв'язку.

Важливим питанням є визначення кількісного показника прихованості, яке є прийнятним за умов впливу різних деструктивних чинників.

Необхідним рівнем прихованості систем зв'язку вважається рівень близький, до значення 0,87 [13]. У [13] необхідним рівнем прихованості систем зв'язку вважається рівень близький до значення 0,8.

З наведеного аналізу можна зробити висновок, що округлене кількісне значення умовного необхідного показника прихованості лежить в інтервалі:

$$P_{прих} = [0{,}60 - 0{,}80]. \qquad (1.3)$$

Прийнято, що інтервал, поданий виразом (1.3), є умовним, тобто його можна застосовувати до кількісних оцінок прихованості різної природи (як імовірнісним, так і не імовірнісним).

Отже, в результаті проведених досліджень встановлено, що відомі бездротові системи передачі даних на основі простих сигналів, що, не дозволяють протистояти перехопленню і радіоелектронному придушенню сигналів, що передаються, а бездротові системи передачі даних на основі ШПС використовують у своєму складі широко поширені генератори ПВП (наприклад, m-послідовності) володіють обмеженою кількістю шумоподібних сигналів через обмеженість періоду генерації ПВП.

Крім того, використання одного і того ж методу модуляції (у даному випадку – частотної модуляції) різними виробниками систем є неприйнятним. Сказане підтверджують тим фактом, що всі наведені оцінки прихованості знаходяться нижче значень інтервалу [0,60÷0,80], визначеного виразом (1.3), що вказує на їхню низьку прихованість від деструктивних впливів.

На основі проведених досліджень визначено суперечність на практиці, яка полягає в тому, що існуючі способи забезпечення потайного інформаційного обміну в бездротових системах передачі даних досягли своїх граничних значень і не можуть надалі підвищувати прихованість.

Отже, необхідно шукати нові підходи для підвищення прихованості інформаційного обміну бездротових системах передачі даних.

1.2 Аналіз альтернативних методів забезпечення прихованого інформаційного обміну для бездротових систем передачі

Останнім часом великий розвиток набувають ідеї використання для забезпечення прихованості радіоканалу бездротових систем передачі даних, методи та алгоритми забезпечення прихованості інформаційного обміну на основі використання шумоподібних сигналів (ШПС). Аналіз методів та алгоритмів забезпечення прихованого інформаційного обміну в бездротових системах передачі даних на основі ШПС показав, що їх умовно можливо розділити на наступні групи [12, 13]:

− методи та алгоритми забезпечення прихованого інформаційного обміну на основі передачі сигналів на частотно-часових позиціях;

− методи та алгоритми забезпечення прихованого інформаційного обміну на основі псевдовипадкової перебудови робочої частоти;

− методи та алгоритми забезпечення прихованого інформаційного обміну на основі фазоманіпульсних сигналів;

– методи та алгоритми забезпечення прихованого інформаційного обміну на основі частотно-модульованих сигналів.

У системах з ПВП часто для забезпечення непередбачуваності випадкових позицій використовуються генератори випадкових чисел (ГВЧ) та псевдовипадкових послідовностей, за допомогою чого забезпечується прихованість від перегляду, заміни, перехоплення та радіоелектронного придушення. Сигнали, що передаються за допомогою ПВП, у загальному випадку описуються таким виразом:

$$S(t) = \sqrt{2P}b(t)\cos\{2\pi(f_c + f_h(t))t\}w(l_t T_s), \tag{1.4}$$

де P – потужність сигналу, $b(t)$ – прямокутні імпульси, f_c – несуча частота, $f_h(t)$ – збільшення частоти «стрибка», $w(l_t T_s)$ – випадковий часовий інтервал, протягом якого може бути переданий сигнал.

Зазвичай, ПВП в якому вибираються за допомогою індивідуального унікального ключа, який присвоєний кожному об'єкту, що охороняється. Сигнали, що передаються за допомогою випадкових ПВП, можна в загальному випадку описати виразом (1.4).

В якості недоліку даного підходу можна виділити складність зміни унікального ключа у разі компрометації об'єкта. Також часто використовують алгоритм забезпечення потайного інформаційного обміну, покладений в основу системи, за допомогою якої повідомлення передаються через стрибкоподібну передачу частоти на центральний приймальний пристрій, який зберігає покажчики на майбутні частоти і час для кожного динамічно оновлювального датчика, а також ID кожного із датчиків. Недоліком даного підходу є мала допустима кількість частотно-часових позицій сигналів, що передаються.

Отже, методи та алгоритми забезпечення прихованого інформаційного обміну на основі ШПС забезпечують скритність від основних видів

деструктивних впливів (перегляд, підміна, перехоплення та придушення перешкодами). До їх загальних недоліків можна віднести недостатню прихованість до деструктивних впливів через використання у своєму складі широко поширених генераторів ПВП (наприклад, m-послідовності), так як після прийому 2n реалізацій радіосигналу, m-послідовність стає передбачуваною і сигнали, що передаються, можна легко перехопити, підмінити або придушити перешкодами. Так само можна відзначити, що практичні реалізації розглянутих методів та алгоритмів забезпечення скритності на основі ШПС відрізняються складністю приймально-передавальної апаратури.

З наведених результатів можна зробити висновок, що необхідно шукати нові шляхи підвищення прихованості інформаційного обміну в бездротових системах передачі даних, оскільки проведений аналіз показав, що відомі методи та алгоритми забезпечення прихованості інформаційного обміну не дозволяють підвищити прихованість інформаційного обміну.

Вирішити завдання підвищення прихованості інформаційного обміну в бездротових системах передачі в умовах комплексних деструктивних впливів потенційно можна шляхом використання методів і алгоритмів забезпечення прихованості інформаційного обміну з урахуванням хаотичних сигналів. Для підтвердження цього висновку проаналізуємо переваги хаотичних сигналів порівняно з відомими методами та алгоритмами забезпечення прихованості інформаційного обміну на основі ШПС.

Одним із найбільш перспективних забезпечення прихованого інформаційного обміну на основі ШПС є використання хаотичних сигналів (ХС), зі схожим за своїми властивостями з шумом.

Шумовим сигналом називається сукупність одночасно існуючих електричних коливань, частоти та амплітуди яких мають випадковий характер. Спектр шумових сигналів займає широку смугу частот. Якщо цей спектр рівномірний на всіх частотах від 0 до ∞, такий сигнал називається «білим». «Білий» шум є ідеальним шумовим сигналом, що має нескінченний

спектр і функцію кореляції у вигляді дельта-функції. Реалізувати практично «білий» шум неможливо, оскільки для його генерації і обробки потрібна апаратура з необмеженою смугою пропускання, у реальних системах використовується шум з обмеженою смугою [14]. У зв'язку з цим, важливим питанням є використання замість реальних, сигналів шуму, що мають властивості близькі до білого шуму. Такі властивості мають хаотичні сигнали. Хаотичні сигнали є по своїй суті шумоподібними сигналами, тому що мають властивості випадкових шумових сигналів (з великим числом кодових конструкцій, суцільним спектром потужності, непередбачуваністю на великих інтервалах часу, підвищеною прихованістю і т.д.) і має головну особливість, яка відрізняє їх від звичайних шумів: вони реалізуються з використанням існуючого математичного алгоритму, тобто мають властивість повторюваності або відтворюваності [15]. Реалізувати хаотичні сигнали можна як апаратними, і програмними генераторами. Причому, невеликі зміни параметрів або початкових значень генератора призводять до істотної зміни форми коливання, що генерується, яка дає можливість формування і вибору різних реалізацій хаотичних сигналів. Дані властивості хаотичного сигналу, що використовується як переносник інформації, дозволяють забезпечувати прихованість передачі. Використання програмного або апаратного «генератора хаосу» забезпечує можливість вибору реалізацій сигналу з необхідними показниками та багаторазового відтворення тих самих реалізацій.

Одним з таких показників хаотичних сигналів є BDS-статистика, яка базується на статистичних властивостях кореляційної розмірності досліджуваного процесу у фазовому просторі, яка в свою чергу визначається кореляційним інтегралом. Ці дані в окремих випадках дають більше інформації про клас процесу (випадкові, хаотичні, регулярні), ніж енергетичні показники.

BDS-статистика описується виразом:

$$w_{m,N}(\varepsilon) = \sqrt{N-m+1}\frac{C_{m,N}(\varepsilon) - C_{1,N-m}(\varepsilon)^m}{\sigma_{m,N}(\varepsilon)}, \quad (1.5)$$

де $C_{m,N}(\varepsilon)$ та $C_{1,N}$ $-m(\varepsilon)^m$ – кореляційні інтеграли, а $\sigma_{m,N}(\varepsilon)$ – середньоквадратичне відхилення.

Завдання аналізу переданого сигналу розглядається як непараметрична перевірка однієї з гіпотез: H0 – дані x =(x x1, 2,...,xn), що спостерігаються, незалежні і однаково розподілені (білий шум) і H1 – дані не відносяться до білого шуму, що можливо у випадку, коли вони є сумішшю шуму та сигналу.

Серед потенційних недоліків використання генераторів хаотичних сигналів слід відзначити збільшене значення пік-фактора сигналів, що передаються, і складності синхронізації приймально-передавальної частини. Зокрема, відомо, що збільшене значення пік-фактора обмежує реалізовані значення енергетичної ефективності радіопередавального пристрою, знижує перешкодостійкість прийому, демаскує факт передачі інформації на тлі шуму, ускладнює та здорожує застосовувану апаратуру.

Значення пік-фактора сигналу обчислюється за допомогою наступного виразу:

$$C_{rest} = U_{max}/\sigma \quad (1.6)$$

де Umax – максимальне значення сигналу, σ – середньоквадратичне значення сигналу.

Для сучасних систем зв'язку значення пік-фактора сигналів, що передаються, обчислене за допомогою виразу (1.6), повинно знаходитися приблизно в діапазоні Crest [1-4]. Пік-фактор Crest може обчислюватись різними програмами, наприклад ScicosLab та деякими іншими.

Важливою перевагою систем зв'язку на основі хаотичних сигналів є більша структурна прихованість, ніж у відомих систем зв'язку на основі ШПС. На основі розрахунків потенційної структурної прихованості Sp

показано (рис. 1.7), що потенційна структурна прихованість хаотичного сигналу Sхск істотно вище в порівнянні з потенційною структурною прихованістю ПВП Sпсп і для бази B=16 перевищує її приблизно в 2 рази, бази B=32 перевищує її приблизно 2,5 разу, а бази B=64 – перевищує 3 рази.

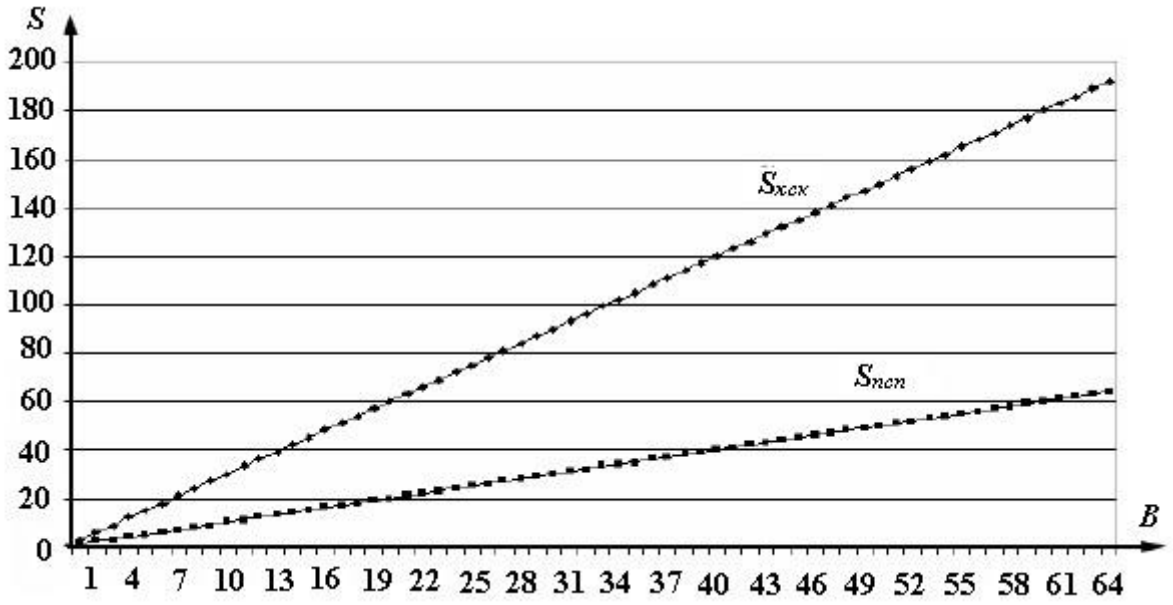


Рисунок 1.7 – Залежність потенційної структурної прихованості S від бази сигналу B для різних типів сигналів

В якості міри структурної прихованості може виступати показник лінійної складності, що обчислюється за допомогою алгоритму Берлекемпа-Мессі. Встановлено, що хаотичні сигнали мають більш високу прихованість, ніж відомі генератори кодових послідовностей (наприклад, m-послідовності). Так нормоване на довжину коду число розрядів еквівалентного регістру зсуву з лінійними зворотними зв'язками (РЗЛЗЗ) генератора хаотичних сигналів на основі кубічної параболи перевищує приблизно в 5 разів нормоване на довжину коду число розрядів еквівалентного РСЛЗЗ генератора m-послідовностей. На рис. 1.8 введено такі позначення: L/N – нормований на довжину коду обсяг ансамблю сигналів; rlin/N – нормована на довжину коду кількість розрядів еквівалентного РСЛЗЗ; 1 – m-послідовності; 2 – генератор хаотичних сигналів на основі кубічної параболи.

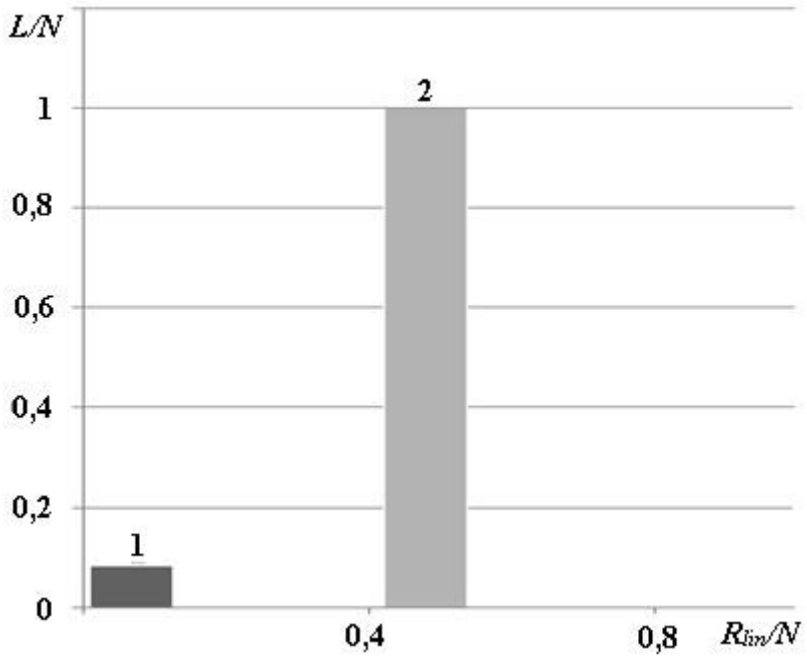


Рисунок 1.8 – Відношення нормованого обсягу ансамблю сигналів до нормованого на довжину коду числа розрядів еквівалентного реєстру зсуву з лінійними зворотними зв'язками

На основі проведеного аналізу, з відомою ймовірнісною оцінкою прихованості та її адаптацією для відомих шумоподібних сигналів та хаотичних сигналів, наведено графіки залежності оцінки с прихованості Рприх від бази сигналу В при різних відношеннях сигнал/шум q для систем зв'язку на основі шумоподібних сигналів (рис. 1.9) та для систем зв'язку з урахуванням хаотичних сигналів (рис. 1.10).

Як видно з наведених рисунків, для систем зв'язку на основі шумоподібних сигналів (рис. 1.9) у міру збільшення бази сигналу прихованість спочатку збільшується (приблизно до Рприх = 0,4 ... 0,5), а потім починає зменшуватися. Ця властивість пов'язана з різною (конкуруючою) поведінкою ймовірностей виявлення та розкриття структури сигналу. Разом з тим для систем зв'язку на основі хаотичних сигналів (рис. 1.10) явно помітно, що прихованість зі збільшенням бази різко зростає (приблизно до Рприх=0,7..1) і перевищує прихованість систем зв'язку на основі шумоподібних сигналів приблизно 1,5 рази.

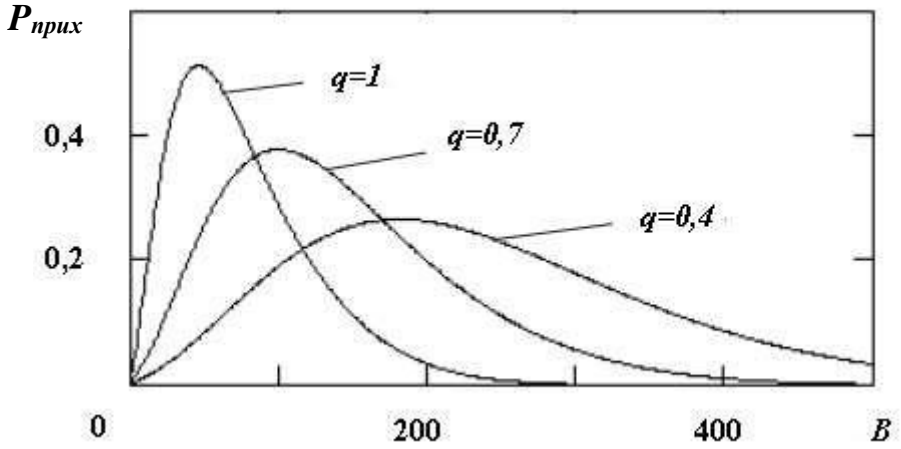


Рисунок 1.9 – Залежність прихованості $P_{прих}$ від бази сигналу B за різного відношення сигнал/шум q для систем зв'язку на основі шумоподібного сигналу

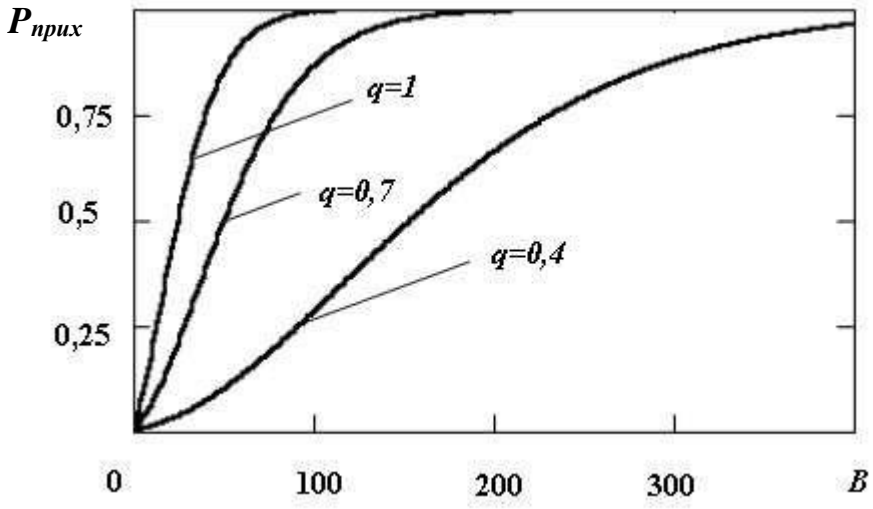


Рисунок 1.10 – – Залежність прихованості $P_{прих}$ від бази сигналу B за різного відношення сигнал/шум q для систем зв'язку на основі хаотичного сигналу

Ще однією перевагою систем зв'язку на основі хаотичних сигналів над відомими системами зв'язку на основі шумоподібних сигналів є перевага за кількістю кодових послідовностей, що використовуються. У таблиці 1.1 як приклад наведено кількісні значення деяких відомих генераторів кодових послідовностей.

Таблиця 1.1

Кількість кодових послідовностей відомих генераторів, що використовуються в системах зв'язку

Назва	Кількість кодових послідовностей, N
m-послідовності	$\approx 10^5$
Коди Голда	$\approx 10^5$
Коди Касамі	$\approx 10^8$
Генератор хаотичних сигналів на основі кубічної параболи	$\approx 10^{17}$

Як видно з табл. 1.1, хаотичні послідовності за кількістю кодових послідовностей значно (приблизно в 109 разів) перевершують поширені генератори кодових послідовностей, наприклад, m-послідовності.

1.3 Висновки за розділом та постановка завдань

Підтверджено актуальність використання бездротових систем передачі в різних галузях. Показано переваги бездротових систем передачі даних над традиційними системами.

Проведено аналіз деструктивних впливів на інформаційний обмін у бездротових системах передачі даних та методів їх реалізації, в результаті якого встановлено, що основними деструктивними впливами на інформаційний обмін є перехоплення, перегляд, заміна та радіоелектронне придушення, які можуть застосовуватися одночасно.

Здійснено аналіз відомих методів та алгоритмів забезпечення прихованості інформаційного обміну у бездротових системах передачі даних в умовах зазначених деструктивних впливів.

Здійснено вибір критерію оцінювання прихованості та методів його реалізації для оцінки прихованості інформаційного обміну у бездротових системах передачі даних.

Отже, необхідно за допомогою проведеного аналізу вирішити такі задачі:

1) розробити обчислювальний метод оцінки прихованості на основі нечіткої логіки для бездротових систем передачі в умовах комплексних деструктивних впливів;

2) розробити математичну модель процесу забезпечення прихованого інформаційного обміну в бездротових системах передачі даних та алгоритм її реалізації на основі хаотичних сигналів в умовах комплексних деструктивних впливів;

3) розробити комплекс програм, який забезпечить прихований інформаційний обмін даних в бездротових системах передачі, в умовах комплексного деструктивного впливу на систему передачі.

2 КОНСТРУКТОРСЬКА ЧАСТИНА

2.1 Вибір критерія оцінювання прихованості інформаційного обміну в бездротових системах передачі даних

Для оцінки ефективності методів та алгоритмів забезпечення прихованості необхідна оцінка, що дозволяє визначити рівень прихованості на основі кількісної та якісної оцінки. В даний час відомо безліч різних обчислювальних методів та моделей оцінки прихованості. Загалом їх можна розділити на великі групи: аналітичні методи і статистичні методи.

Аналітичні методи дозволяють одержати характеристики системи як деяку функцію параметрів її функціонування. Зазвичай аналітична модель представляє собою сукупність математичних символів і відношень, під час вирішення яких отримують параметри та необхідні оцінки системи, що досліджується. Часто такими параметрами виступають імовірнісні чи інші характеристики.

Статистичні методи засновані на комп'ютерному моделюванні моделей, що імітують поведінку реальних об'єктів, процесів і систем у часі, протягом заданого періоду та багаторазово повторюються для подальшої статистичної обробки отриманих даних з метою підтвердження їх адекватності.

Поєднання аналітичних і статистичних методів є дуже корисним, оскільки дозволяє не тільки ефективно досліджувати різні об'єкти, але й розуміти і пояснювати фізичну суть процесів і явищ, що відбуваються в досліджуваній системі.

Відповідно до оцінки прихованості виділяється 4 рівні (S1, S2, S3, S4). У найпотаємніших рівнях S3 та S4 передбачено обов'язкове використання кодування сигналу певною кількістю оригінальних кодів (таблиця 2.1).

Таблиця 2.1

Рівні прихованості систем передачі

Рівень прихованості систем передачі	Опис
S1	прихованість відсутня
S2	Прихованість відсутня, проте є діагностика функціонування окремих елементів
S3	Діагностика функціонування окремих елементів (S2) та кодування сигналу (не менше 250 оригінальних кодів) у лінії (каналі) зв'язку
S4	Діагностика функціонування окремих елементів (S2) з кодуванням сигналу в лінії (каналі) зв'язку, що використовує спеціальний алгоритм, який повинен бути таким, щоб у синхронізованих системах передачі сповіщень набір даних 100 біт у будь-якій послідовності не повторювався серед 10000000 біт однієї послідовності, а в несинхронізованих системах набір даних 100 байт у будь-який послідовності не повторювався серед 1000000 байт однієї послідовності

Аналіз таблиці 2.1 показує, що до недоліків цього методу оцінки можна віднести:

a) відсутність кількісних показників;

b) у методі не приділяється увага конкретним підходам деструктивного впливу на радіоканал і конкретним методам забезпечення прихованості радіоканалу.

Внаслідок чого, наприклад, використання методів та алгоритмів забезпечення потайного інформаційного обміну на основі криптографічного методу захисту та шумоподібного сигналу з однаковою кількістю

оригінальних кодових послідовностей ставиться в один клас, хоча загальновідомо, що методи та алгоритми забезпечення потайного інформаційного обміну на основі шумоподібного сигналу забезпечують більший рівень прихованості від комплексних деструктивних впливів (перегляд, підміна, перехоплення, радіоелектронне придушення), у той час як методи та алгоритми забезпечення потайного інформаційного обміну на основі криптографічного методу захисту не здатні протистояти перехопленню та придушенню перешкод [16].

Виходячи з цього, важливим є питання кількісної оцінки прихованості інформаційного обміну в бездротових системах передачі даних, основою яких покладено проаналізовані методи та алгоритми забезпечення потайного інформаційного обміну. В даний час однією з найвідоміших кількісних моделей оцінки прихованості бездротових систем передачі даних є ймовірнісна оцінка прихованості [17]. Під прихованістю розуміється здатність системи зв'язку протистояти виявленню противником її робочого стану за допомогою радіорозвідки. Як відомо [18], радіорозвідка систем зв'язку складається з наступних кроків: виявлення сигналу, визначення структури сигналу і розкриття інформації, що передається. Переліченим завданням радіотехнічної розвідки можна протиставити три види прихованості сигналів: енергетичну, структурну та інформаційну.

Енергетична прихованості характеризує здатність протистояти заходам, спрямованим виявленню сигналу розвідувальними приймальними пристроями, а структурна прихованість – ступінь ускладнення визначення структури сигналу. Інформаційна прихованість визначається стійкістю криптографічного ключа. Кількісним заходом енергетичної прихованості є можливість правильного виявлення Рвияв. Кількісною мірою структурної прихованості є можливість розкриття структури сигналу Рстр, за умови, що сигнал виявлений. Кількісним заходом інформаційної прихованості є можливість розкриття змісту переданої інформації Рінф , за умови, що сигнал виявлено і розкрито його структура.

Отже, ймовірність розвідки Рр визначається наступним виразом:

$$Р_р = Р_{вияв} * Р_{стр} * Р_{інф}. \quad (2.1)$$

Часто завдання оцінки інформаційної прихованості не ставиться, оскільки виявлення сигналу, що передається, і визначення його структури дозволить зловмиснику поставити перешкоду, від якої інформаційна прихованість не захищає. Тому, ефективне вирішення проблеми забезпечення прихованості переданих даних у системах зв'язку, у тому числі і при компрометації ключа дешифрування, повинна лежати в галузі забезпечення високої енергетичної та структурної прихованості переданих сигналів. Звідси вираз (2.1) перетворюється на такий вид:

$$Р_р = Р_{вияв} * Р_{стр}. \quad (2.2)$$

На основі виразу (2.2) обчислюється загальна оцінка прихованості $Р_{прих}$:

$$Р_{прих} = 1 - Р_р = 1 - Р_{вияв} * Р_{стр}. \quad (2.3)$$

Для оцінки прихованості, що описується виразом (2.3), важливим є той факт, що для обчислення енергетичної Рвияв і структурної Рстр прихованості пропонуються різні математичні вирази. Наприклад, для оцінки структурної прихованості для відомих шумоподібних сигналів:

$$P_{стршпс} = P\{|\varepsilon| < \varepsilon_0 = \Phi(\frac{3\varepsilon_0}{2})qFT(1-\rho^2)\}, \quad (2.4)$$

де Ф(z) – інтеграл імовірності, ε_0 – межі довірчого інтервалу, ρ – коефіцієнт частотно-часового зв'язку.

Для оцінки структурної скритності для хаотичних сигналів:

$$P_{стрхс} = P\,|\,\varepsilon\,| < \varepsilon_0 = \Phi(\frac{3\varepsilon_0}{2}\frac{1}{\sigma_\lambda}). \quad (2.5)$$

Потенційну структурну прихованість Sp можна обчислювати за допомогою наступного виразу:

$$S_p = \log_2 A, \quad (2.6)$$

де А – ансамбль реалізацій, який визначається кількістю всіх можливих значень будь-яких параметрів.

2.2 Комплексний підхід для оцінки прихованості інформаційного обміну в бездротових системах передачі

Для оцінки прихованості необхідний комплексний підхід - умови роботи радіотехнічних систем повинні оцінюватися з урахуванням як технічних можливостей розвідки, так і з урахуванням технічних можливостей самих радіотехнічних систем, однак це є досить трудомістким процесом через необхідність обчислення оцінки прихованості в різних умовах, у тому числі в умовах комплексних деструктивних впливів для радіотехнічних систем різного призначення.

При ймовірності оцінки прихованості зазвичай не враховується оцінка інформаційної прихованості, що спотворює загальну оцінку прихованості.

Як перспективний напрямок для розвитку обчислювальних методів і моделей оцінки прихованості в даний час виділяється апарат нечіткої логіки, який в умовах неповноти та слабоструктурованості вихідних даних дозволяє отримати як кількісну оцінку прихованості, так і якісну.

Визначення формули важливості інциденту порушення прихованості:

$$I_{лм} = k(m)\ At\ P. \quad (2.7)$$

Визначення формули чисельної оцінки прихованості систем передачі в локальній мережі (ЛМ):

$$P_{прср} = 1 - I_{лм}. \quad (2.8)$$

Вычисление оценки скрытности систем передачи данных в ЛМ:

$$P_{прср} = 1 - k(m)\ At_i As_i\ P_{лмі}\ T_i, \quad (2.9)$$

де k(m) – нормуючий коефіцієнт, що дозволяє уявити отриманий результат в діапазоні [0,1]; Ati – рівень деструктивного впливу на і-у локальну обчислювальну мережу; Asi - критичність активів і-ої локальної обчислювальної мережі; Рлмі - рівень забезпечення прихованості і-ої локальної мережі; Ti – рівень довіри пристрою і-ї локальної мережі.

Отже, згідно з цим обчислювальним методом, прихованість обчислюється за допомогою виразу (2.9), що дозволяє в умовах неповноти та слабоструктурованості вихідних даних обчислити оцінку прихованості інформаційного обміну в бездротових системах передачі даних.

Таблиця 2.1

Переведення нечіткого параметра At у чисельне значення

Нечіткий параметр	Чисельне значення
Дуже низький	1
Низький	2
Средній	3
Високий	4
Дуже високий	5

Таблица 2.2

Переведення нечіткого параметра Р у чисельне значення

Нечіткий параметр	Чисельне значення
Дуже низький	5
Низький	4
Средній	3
Високий	2
Дуже високий	1

Отже, знаючи числові значення, можна отримати чисельну (кількісну) оцінку прихованості інформаційного обміну бездротових системах передачі даних від деструктивних впливів в цілому [19]:

$$Р_{прих} = 1\text{-}І_{прих}. \quad (2.10)$$

Для обчислення оцінки прихованості інформаційного обміну бездротових системах передачі від деструктивних впливів:

$$Р_{прих}=1\text{-}k(m)\ At\ P. \quad (2.11)$$

Вираз (2.11) не враховує різноманіття деструктивних впливів, тому пропонується для більш точного визначення кількісної та якісної оцінки прихованості інформаційного обміну враховувати основні деструктивні впливи для радіоканалу бездротових систем передачі даних та всі методи забезпечення прихованості від них. Далі кожному методу слід привласнити чисельне значення і провести підсумовування, що є узагальненими показниками рівня забезпечення прихованості P_O та рівня деструктивного впливу At_O:

$$At_O = \Sigma At_i, \quad (2.12)$$

Вираз (2.12) дозволяє отримати коефіцієнт нормування k(m) (2.13), при цьому P_O та At_O обчислюються при максимальних значеннях:

$$k(m)=1/At_O\ Pc. \qquad (2.13)$$

Для переводу кількісної оцінки якісну складемо таблицю зпівставлення (таблиця 2.3).

Таблиця 2.3

Зпівставлення кількісних та якісних оцінок прихованості

Значення кількісної оцінки прихованості	Значення якісної оцінки прихованості
$0 < P_{прср} < 0,2$	Дуже низька
$0,2 < P_{прср} < 0,4$	Низька
$0,4 < P_{прср} < 0,6$	Средня
$0,6 < P_{прср} < 0,8$	Висока
$0,8 < P_{прср} < 1$	Дуже висока

2.3 Висновки за розділом

Розроблений обчислювальний метод оцінки прихованості на основі нечіткої логіки включає наступні етапи:

1) завдання прихованості бездротових систем передачі даних;

2) перетворення нечітких значень змінних «дуже низький», «низький», «середній», «високий», «дуже високий» у числові значення;

3) визначення формули важливості інциденту порушення прихованості, що описується виразом (2.7);

4) визначення формули чисельної оцінки прихованості інформаційного обміну в бездротових системах передачі даних від деструктивних впливів загалом, що описується виразом (2.10);

5) обчислення узагальнених показників рівня деструктивного впливу та рівня забезпечення прихованості;

6) обчислення коефіцієнта нормування, що описується виразом (2.13);

7) обчислення оцінки прихованості інформаційного обміну в бездротових системах передачі даних, що описується виразом (2.9);

8) переведення кількісної оцінки на якісну оцінку за табличним методом.

3 ДОСЛІДНИЦЬКА ЧАСТИНА

3.1 Розроблення моделі процесу забезпечення прихованого інформаційного обміну для бездротових систем передачі

Як було встановлено раніше в першому розділі, в даний час у бездротових системах передачі даних основними методами та алгоритмами забезпечення прихованого інформаційного обміну є методи та алгоритми, засновані на криптографічних системах передачі та на основі шумоподібних сигналів.

Встановлено, що бездротові системи передачі даних, в основу яких покладено проаналізовані методи та алгоритми забезпечення прихованого інформаційного обміну, не забезпечують достатньої прихованості від комплексних деструктивних впливів.

На рис. 3.1 представлена узагальнена схема розробленого підходу забезпечення прихованості інформаційного обміну в бездротових системах передачі даних, заснована на використанні хаотичних сигналів [21]. Вона складається з блоку контролю, що включає генератор ПСП-1, генератор ПСП-2, накопичувач хаотичної послідовності (НХП), накопичувач копії хаотичної послідовності (НКХП), пристрій порівняння (ПП); ненавмисних і навмисних деструктивних впливів і контрольованого об'єкта (датчика), що включає генератор ПСП-2, НХП, НКХП.

Схема на рис. 3.1, функціонує в такий спосіб. Для запуску блоку контролю на вхід ПСП-1 генератора подається стартова команда. Після цього генератор ПСП-1 виробляє перше псевдовипадкове число. Отримане значення відправляється на генератор ПСП-2 блоку контролю та одночасно з цим перемножується з хаотичною послідовністю і через лінію зв'язку передається на контрольований об'єкт (датчик).

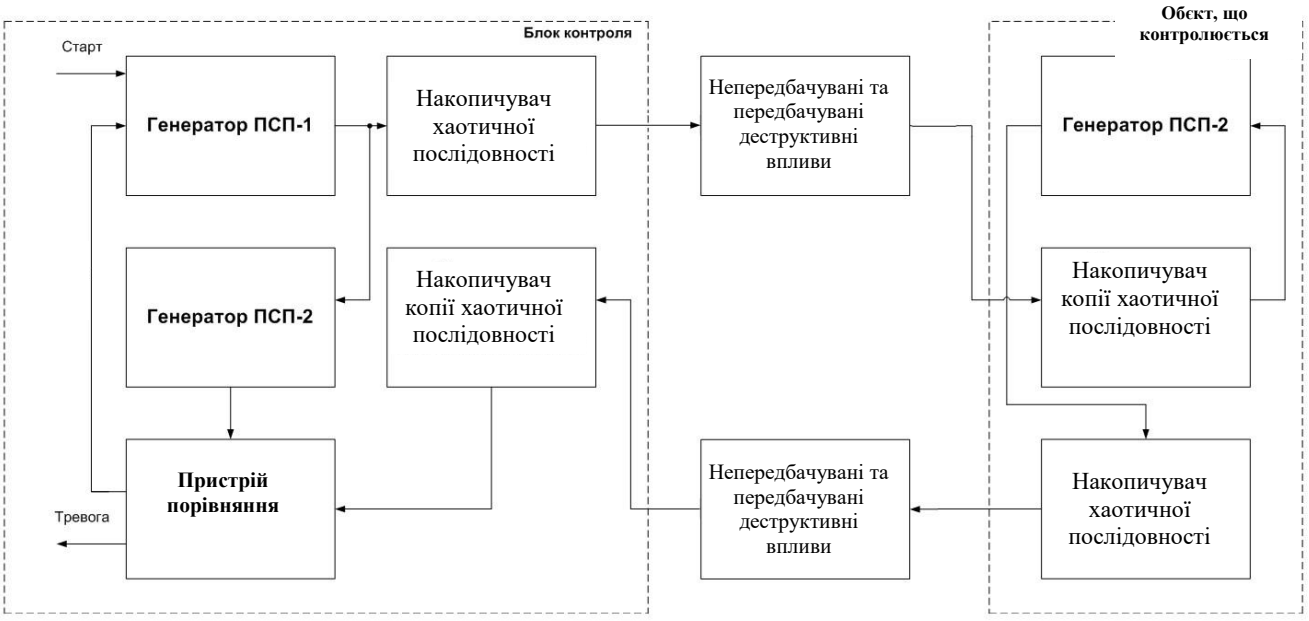


Рисунок 3.1 – Узагальнена схема розробленого підходу забезпечення прихованості інформаційного обміну в бездротових системах передачі на основі застосування хаотичних сигналів

У лінії зв'язку на сигнали, що передаються, впливають різні ненавмисні і навмисні деструктивні впливи (наприклад, нав'язування хибних даних або придушення перешкодами).

Після цього відбувається декодування отриманого сигналу за допомогою копії хаотичного сигналу, ідентичної хаотичної послідовності в блоці контролю, і далі декодований сигнал у вигляді послідовності надходить до генератора ПСП-2, функція генерації послідовності якого ідентична функції генератора ПСП-2 блоку контролю. Потім відбувається перемноження послідовності ПСП-2 контрольованого об'єкта (датчика) з хаотичною послідовністю через лінію зв'язку передається на блок контролю.

У лінії зв'язку на сигнали, що передаються, впливають різні ненавмисні і навмисні деструктивні впливи (наприклад, нав'язування хибних даних або придушення перешкодами). Після цього відбувається декодування отриманого сигналу за допомогою копії хаотичної послідовності, ідентичної хаотичної послідовності в контрольованому об'єкті (датчику), і далі

декодований сигнал у вигляді послідовності надходить на пристрій порівняння, в якому перевіряється відгук раніше прийшов значення генератора ПСП-2 блоку контролю і відгук генератора ПСП-2 контрольованого об'єкта (датчика). У разі збігу значень, які від контрольованого об'єкта (датчика) і блоку контролю, виробляється сигнал «Норма», який служить генерацією наступного псевдовипадкового числа генератором ПСП-1. При розбіжності значень пристрій порівняння видає команду «Тривога».

3.2 Розроблення алгоритму реалізації моделі процесу забезпечення прихованого інформаційного обміну для бездротових систем передачі

На основі описової моделі пропонується алгоритм реалізації процесу забезпечення потайного інформаційного обміну, що складається з наступних кроків:

1. Ініціалізація генератора ПСП-1 блоку контролю.

2. Вироблення першого псевдовипадкового числа генератором ПСП-1 блоку контролю.

3. Відправлення отриманого значення одночасно на генератор ПСП-2 блоку контролю та НХП.

4. Передача твору ПСП-1 та ХС із НХП на контрольований об'єкт.

5. Декодування у контрольованому об'єкті отриманого сигналу за допомогою НКХП, ідентичного НХП у блоці контролю.

6. Надходження декодованого сигналу у вигляді послідовності в генератор ПСП-2 контрольованого об'єкта, функція генерації послідовності якого ідентична функції генератора ПСП-2 блоку контролю.

7. Передача виробленої послідовності ПСП-2 контрольованого об'єкта з НХП на блок контролю.

8. Декодування у блоці контролю отриманого сигналу за допомогою НКХП, ідентичного НХП у об'єкті, що контролюється.

9. Надходження декодованого сигналу як ПСП-2 контрольованого об'єкта в ПП.

10. Вироблення ПСП-2 блоку контролю та її надходження до ПП.

11. Порівняння ПСП-2 блоку контролю та ПСП-2 контрольованого об'єкта.

12. Якщо порівняння правильне, відображення сигналу «Норма» і перехід до п. 1 алгоритму.

13. Якщо порівняння неправильне, то відображення сигналу «Тривога» та перехід до п. 14 алгоритму.

14. Формування сигналу «Прихованість даних, що передаються, порушена».

На рис. 3.2 описаний алгоритм наведено як блок-схеми.

Як видно з рис. 3.2 наведено узагальнений вид алгоритму, тобто його можна використовувати в різних бездротових системах передачі даних, де існує необхідність забезпечення потайного інформаційного обміну між кількома об'єктами. Використання в блоці контролю і контрольованому об'єкті однакових накопичувачів хаотичних послідовностей, а також однакових генераторів ПСП-2, ініціалізація яких здійснюється псевдовипадковим числом, що періодично змінюється, виробляється генератором ПСП-1 блоку контролю, дозволяє підвищити прихованість від деструктивних впливів переданих керуючих і службових.

На підставі описаних вище моделей процесу забезпечення потайного інформаційного обміну та алгоритму її реалізації розроблено модифікований алгоритм.

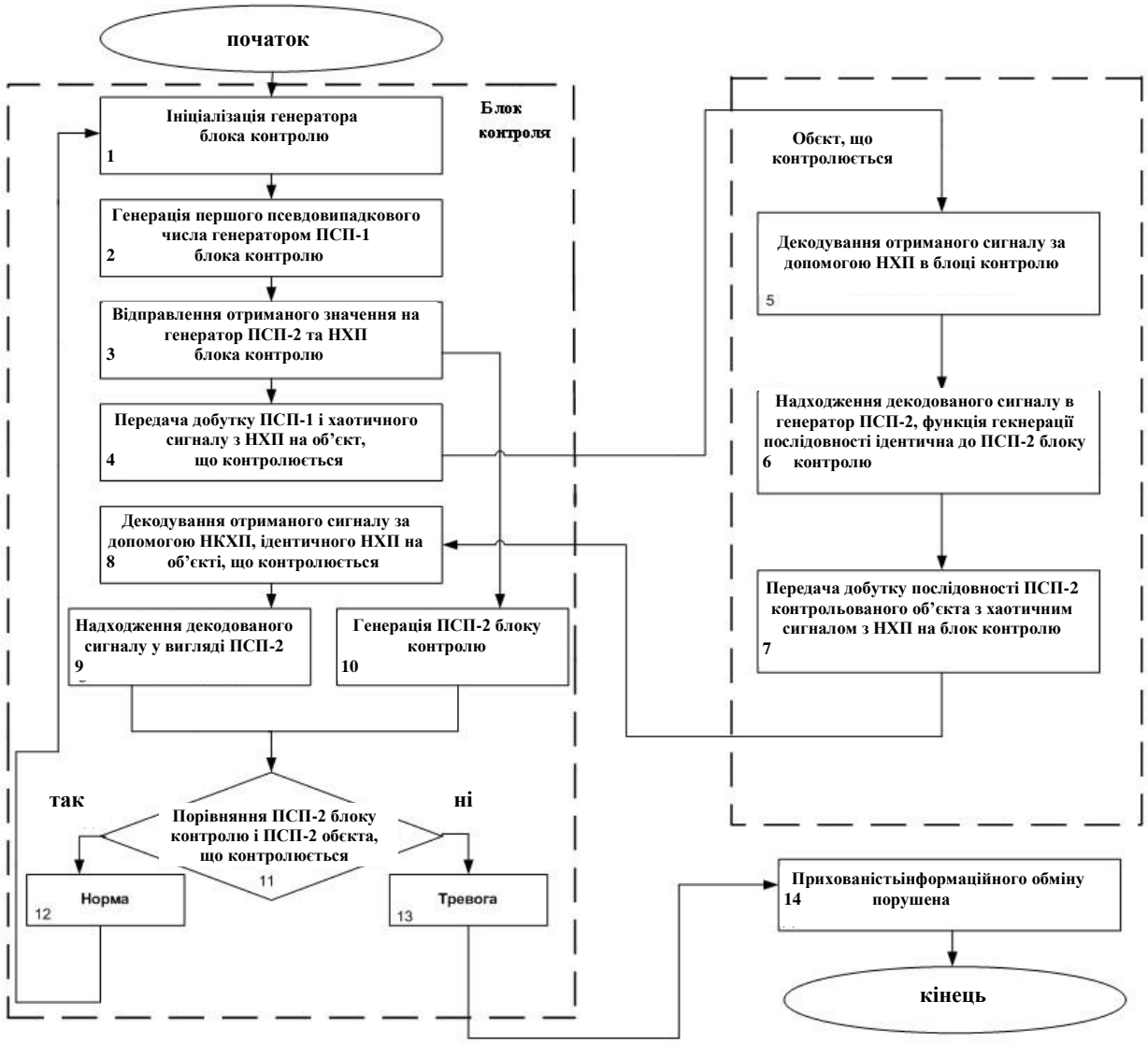


Рисунок 3.2 – Розроблений алгоритм реалізації моделі процесу забезпечення прихованого інформаційного обміну

Алгоритм складається з наступних кроків:

1. Ініціалізація генератора ПСП-1 блоку контролю.

2. Вироблення першого псевдовипадкового числа генератором ПСП-1 блоку контролю, та його відправлення на генератор ПСП-2 блоку контролю та блок логічної операції XOR.

3. Вибір ПЗП унікальних ідентифікаційних даних датчиків з таблиці одного унікального значення, присвоєного кожному контрольованому об'єкту.

4. Додавання за правилом XOR значень першої ПСП-1 блоку контролю та обраного контрольованого об'єкта.

5. Відправлення отриманого значення НХП, де воно перемножується з ХС, і передача отриманої послідовності на контрольований об'єкт.

6. Декодування у контрольованому об'єкті отриманого сигналу за допомогою НКХП, ідентичного НХП у блоці контролю.

7. Надходження декодованого сигналу в блок логічної операції XOR контрольованого об'єкта, який одночасно з цим приходить індивідуальне значення контрольованого об'єкта.

8. Отримання в блоці логічної операції XOR контрольованого об'єкта значення ПСП-1 блоку контролю та його надходження у вигляді послідовності у генератор ПСП-2 контрольованого об'єкта, функція генерації послідовності якого ідентична функції генератора ПСП-2 блоку контролю.

9. Вироблення у генераторі ПСП-2 контрольованого об'єкта, функція генерації послідовності якого ідентична функції генератора ПСП-2 блоку контролю, послідовності ПСП-2.

10. Передача виробленої послідовності ПСП-2 контрольованого об'єкта з НХП на блок контролю.

11. Декодування у блоці контролю отриманого сигналу за допомогою НКХП, ідентичного НХП у контрольованому об'єкті.

12. Надходження декодованого сигналу як ПСП-2 контрольованого об'єкта в ПП.

13. Вироблення ПСП-2 блоку контролю та її надходження до ПП.

14. Порівняння ПСП-2 блоку контролю та ПСП-2 контрольованого об'єкта.

15. Якщо порівняння правильне, відображення сигналу «Норма» і перехід до п. 1 алгоритму.

16. Якщо порівняння неправильне, то відображення сигналу «Тривога» та перехід до п. 17 алгоритму.

17. Формування сигналу «Прихованість даних, що передаються, порушена».

На рис. 3.3 розроблений модифікований алгоритм наведено як блок-схеми.

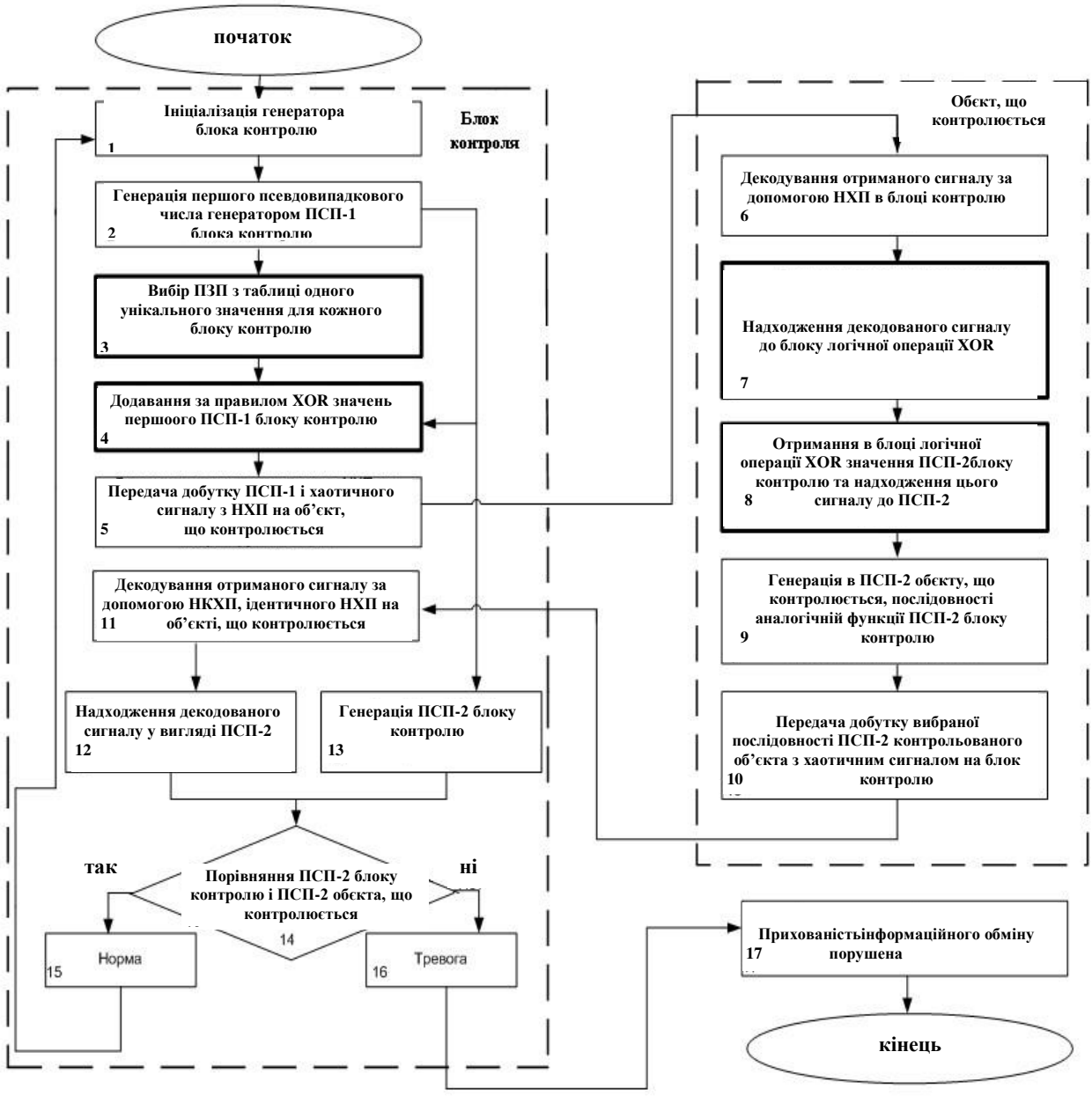


Рисунок 3.3 – Розроблений модифікований алгоритм реалізації моделі процесу забезпечення потайного інформаційного обміну з ускладненою імітаційною вставкою

Як видно, розроблений модифікований алгоритм має узагальнений вигляд - його застосування на практиці може бути різноманітним.

Відмінною рисою модифікованого алгоритму, на відміну від наведеного вище, є ускладнена імітаційна вставка для команд, що передаються за рахунок додавання за правилом XOR вихідного значення ПСП-1 і контрольованого об'єкта. Цю суму можна використовувати як імітаційну вставку, що ускладнює сторонньому спостерігачеві процес вивчення алгоритму генерації ПСП, так і заміну службових і тривожних команд, що передаються, при передачі від блоку контролю на контрольовані об'єкти, а також для перевірки справжності контрольованих об'єктів.

Крім того, надалі, можна передбачити, що при передачі службових і тривожних повідомлень від контрольованого об'єкта на блок контролю (у зворотному напрямку), можна використовувати, як імітаційну вставку, не значення ПСП-2, що виробляється на контрольованому об'єкті, а також суму за правилом XOR значення ПСП-2 контрольованого об'єкта (відновлення вихідної ПСП-2 контрольованого об'єкта буде здійснюватися додаванням за правилом XOR у блоці контролю отриманої суми з контрольованого об'єкта, що перевіряється).

Прихованість від перегляду, перехоплення і придушення перешкодами забезпечується, як і в наведеному раніше алгоритмі, накопичувачем хаотичних сигналів, що перезаписуються, в якій можливо записати потенційно нескінченну кількість різних хаотичних реалізацій (для відновлення вихідної ПСП, а також службової та тривожної інформації необхідно мати точну копію хаотичного сигналу).

3.3 Висновки за розділом

Розроблено модель процесу забезпечення прихованості інформаційного обміну. Її перевагами є облік у своєму складі оператора формування хаотичних сигналів і оператора взаємодії сигналів, що передаються, з навмисними і ненавмисними деструктивними впливами в каналі зв'язку.

Розроблено алгоритм реалізації моделі процесу забезпечення потайного інформаційного обміну, який дозволяє підвищити приховання від деструктивних впливів переданих керуючих та службових команд за рахунок використання в блоці контролю та контрольованому об'єкті однакових накопичувачів хаотичних послідовностей, а також однакових генераторів ПСП -2, ініціалізація яких здійснюється псевдовипадковим числом, що періодично змінюється, генератором, що виробляється ПСП-1 блоку контролю.

Розроблено модифікований алгоритм реалізації моделі процесу забезпечення потайного інформаційного обміну, який заснований на алгоритмі забезпечення потайного інформаційного обміну, який дозволяє підвищити приховання від деструктивних впливів переданих керуючих та службових команд за рахунок використання ускладненої імітаційної вставки для команд, що передаються, заснованої на додаванні за правилом XOR вихідного значення ПСП-1 та контрольованого об'єкта.

4 РОЗРОБЛЕННЯ ПРАКТИЧНИХ РЕКОМЕНДАЦІЙ

4.1 Реалізація обчислювального методу оцінки прихованості інформаційного обміну на основі нечіткої логіки

На рис. 4.1 запропоновано графоаналітичне представлення розробленої програмної реалізації обчислювального методу оцінки прихованості інформаційного обміну бездротових систем передачі на основі нечіткої логіки. Представлена алгоритмічна реалізація відповідає розробленому в другому розділі обчислювальному методу оцінки прихованості на основі нечіткої логіки, що описується виразами (2.1)-(2.8).

На рис. 4.2 зображено графоаналітичне представлення розробленої програми, що реалізує запропоновану модель процесу забезпечення потайного інформаційного обміну.

На рис. 4.2 введені такі позначення:

1 – модуль, що реалізує функції джерела інформації (блок контролю, контрольований об'єкт);

2 – модуль, що реалізує функції накопичувача хаотичного сигналу;

3 – модуль, що реалізує функції модулятора-передавача; фільтра;

5 - модуль, що реалізує функції підсилювача;

6 - модуль, що реалізує функції першого помножувача;

7 - модуль, що реалізує функції другого помножувача;

8 - модуль, що реалізує функції першого інвертора;

11 - модуль, що реалізує функції другого інтегратора;

12 - модуль, що реалізує функції пристрою віднімання;

13 - модуль, що реалізує функції пристрою прийняття рішення;

14 - модуль, що реалізує функції одержувача інформації (блок контролю, контрольований об'єкт).

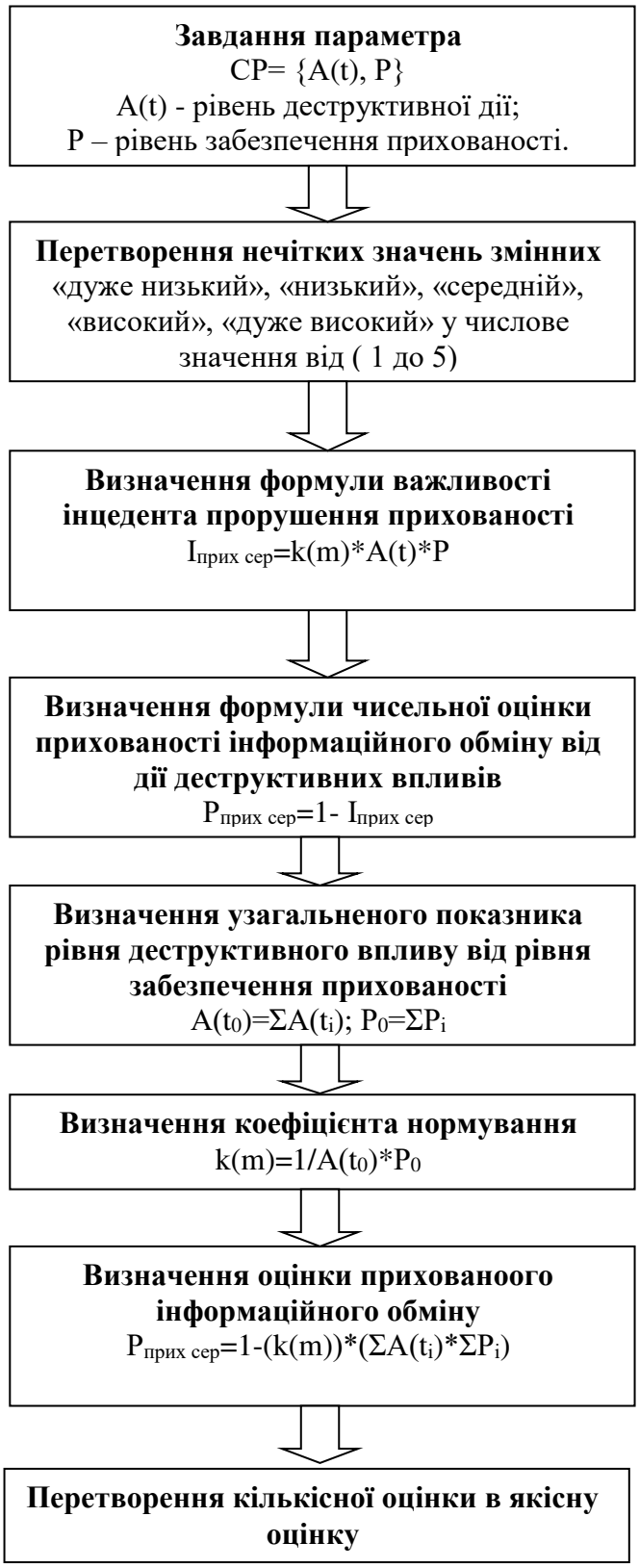


Рисунок 4.1 – Графоаналітичне представлення програмної реалізації розробленого обчислювального методу оцінки прихованості

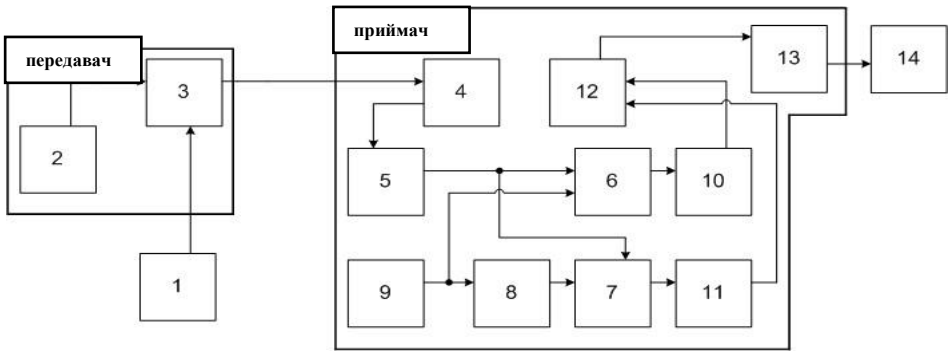


Рисунок 4.2 – Графоаналітичне представлення програмної реалізації запропонованої моделі процесу забезпечення прихованого інформаційного обміну

Вихідними даними для опису графоаналітичного представлення програмної реалізації запропонованої моделі процесу забезпечення потайного інформаційного обміну є:

Sx(t) – хаотичний сигнал;

Sінф(t) – вихідний інформаційний сигнал (ПСП-1 та ПСП-2);

U (t) - сигнал, що передається в каналі зв'язку;

Sвих інф(t) – відновлений інформаційний сигнал (ПСП-1 та ПСП-2).

Інформаційний сигнал Sінф(t) може приймати два значення -1 і 1. При цьому вихідний сигнал модуля, що реалізує функції модулятора-передавача, являє собою сигнал U(t), створений за допомогою перемноження в ньому вихідного інформаційного сигналу Sінф(t) з хаотичним сигналом Sx(t).

У каналі зв'язку на переданий сигнал U(t) діє адитивна гауссівська перешкода, тому на вхід модуля, що реалізує функції приймального пристрою, надходить суміш сигналу і перешкоди, що передається, R(t)=U(t)+N(t).

Після входження в режим синхронізації, з модуля, що реалізує функції смугового фільтра, виходить сигнал Y(t)=U(t)+N(t), який потім підсилюється. Після цього підсилений сигнал Yпідс(t) одночасно множиться на копію хаотичного сигналу Sx(t), аналогічну хаотичному сигналу на передавальній стороні, а також множиться на її інвертоване значення Sx(t). У результаті

виходять сигнали $S_{П1}(t)$=-Yпідс(t) Sx(t) і $S_{П2}(t)$=Yпідс(t) Sx(t), які потім проходять через модулі, що реалізують функції інтегратора, і приймають наступні значення $G_1(t)$-$G_2(t)$. Причому після виходу сигналу з модуля, що реалізує функції інтегратора, можливі наступні випадки:

– G(t) max, при G(t)+Sп(t)>max;

– G(t)=G(t)+$S_П(t)$, при min < G(t)+$S_П(t)$< max;

– G(t) =min, при G(t)+$S_П(t)$< min.

Тут min і max - постійні, що характеризують поріг обмеження вихідного сигналу модуля, що реалізує функції інтегратора. Далі сигнали G(t1) і G2(t) надходять у модуль, що реалізує функції пристрою, який вираховує де обчислюється їх різниця. З виходу модуля пристрою віднімання, різницевий сигнал $Z_{раз}(t)$ надходить в модуль, що реалізує функції вирішального пристрою, де відбувається порівняння прийнятих рівнів з пороговим значенням:

- Sвих інф.(t) =1 при Z разів (t) > 0,

- Sвих інф.(t) = -1 при Z разів (t) < 0.

Після цього відновлений інформаційний сигнал Sвих інф.(t) надходить у модуль, що реалізує функції одержувача, при цьому в ідеальному випадку Sінф(t) =Sвих інф.(t).

Вхідними параметрами розробленого алгоритму є хаотичний сигнал Sx(t) і вихідний інформаційний сигнал Sінф(t). Після їх перемноження утворюється сигнал U(t). У каналі зв'язку на переданий сигнал U(t)діє адитивна гауссовская перешкода, тому сигнал перетворюється до виду R(t)= U(t)+N(t). Після входження в режим синхронізації, з модуля, що реалізує функції смугового фільтра, виходить сигнал Y(t)=U(t)+N(t), який потім підсилюється. Після цього підсилений сигнал одночасно множиться на копію хаотичного сигналу Sx(t), аналогічну хаотичному сигналу на стороні, що передає, а також множиться на її інвертоване значення -Sx(t).

На рис. 4.3 наведено спрощений алгоритм роботи розробленої програми.

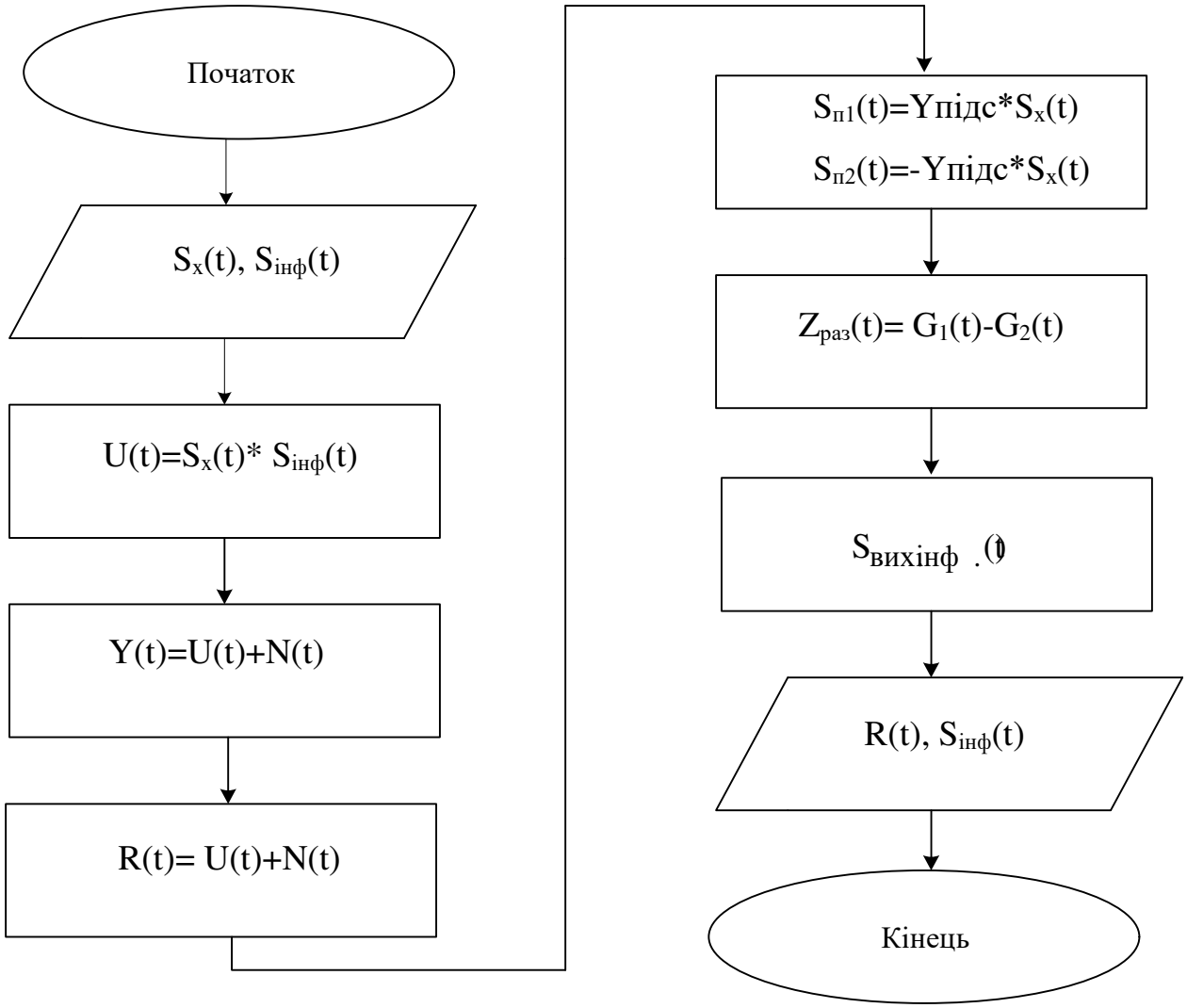


Рисунок 4.3 – Спрощений алгоритм работи системи

У результаті виходять сигнали $S_{П1}(t)$ і $S_{П2}(t)$ які потім проходять через модулі, що реалізують функції інтеграторів, і приймають наступні значення $G_1(t)$ і $G_2(t)$. Далі сигнали $G_1(t)$ і $G_2(t)$ надходять у модуль різниці. З виходу модуля різницевий сигнал Zріз(t) надходить у модуль, де він перетворюється на відновлений інформаційний сигнал. Вихідними параметрами для розробленої програми є сигнал R(t), що передається в каналі зв'язку, і інформаційний сигнал $S_{інф}(t)$.

На рис. 4.4 наведено графоаналітичну послідовність розробленого алгоритму, що реалізує модель системи зв'язку із простими сигналами

Рисунок 4.4 – графоаналітична послідовність розробленого алгоритму, що реалізує модель системи зв'язку із простими сигналами

Відповідно до рис. 4.4 вихідний сигнал b(t) надходить у модуль, що реалізує функції передавального пристрою, де він перетворюється на сигнал u(t), придатний для передачі каналом зв'язку. При передачі каналами зв'язку сигнал u(t) може спотворюватися, тому він перетворюється на сигнал z(t). Модуль, що реалізує функції приймального пристрою, обробляє прийнятий сигнал z(t) і відновлює вихідний сигнал.

4.2 Оцінка достовірності сигналів отриманих за розробленим алгоритмом

Проведемо оцінку достовірності сигналів, що генеруються програмною реалізацією моделі системи зв'язку із простими сигналами.

Було отримано близько 50 різних часових реалізацій сигналів, що передаються в каналі зв'язку. Отриманих даних достатньо для коректного аналізу процесів, що відбуваються в системі зв'язку з простими сигналами.

Проведемо їх візуальний (якісний) та кількісний аналіз на основі методів нелінійної динаміки [22]. Проаналізуємо отримані дані системи зв'язку з урахуванням простих сигналів. Щоб коректно застосувати методи нелінійної динаміки до отриманим даним, спочатку необхідно визначити мінімальну розмірність атрактора (псевдоаттрактора). Розмірність атрактора (псевдоаттрактора) сигналів, що передаються, дорівнює 1.

Перш за все розглянемо отримані візуальні (якісні) показники переданих в каналі зв'язку сигналів (фазові портрети).

На рис.4.5 наведено приклад фазового портрета сигналів системи зв'язку з простими сигналами, що передаються в каналі зв'язку.

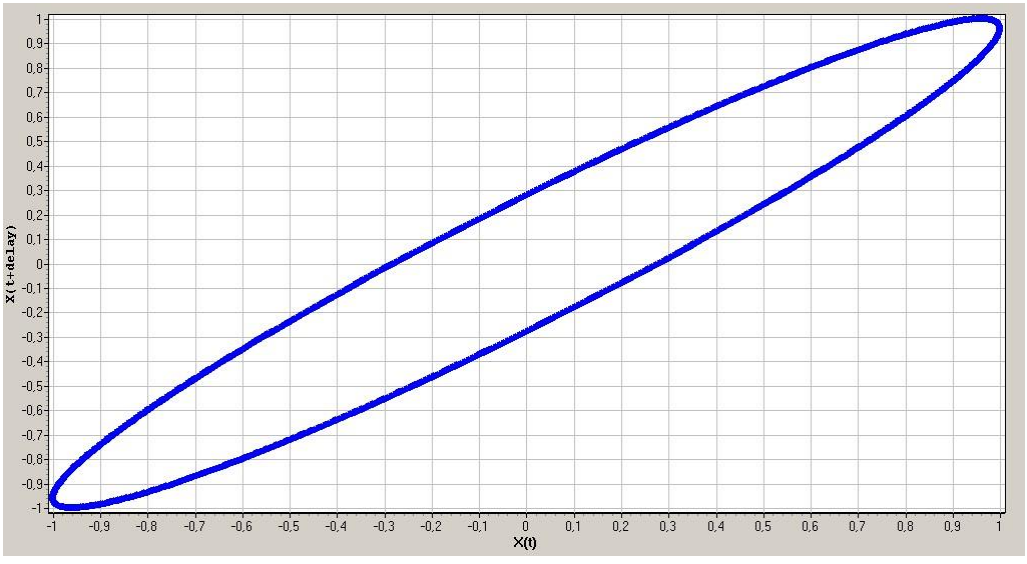


Рисунок 4.5 – Фазовий портрет сигналу, що передається у каналі зв'язку

Розглянемо отримані кількісні показники сигналів системи зв'язку з простими сигналами (максимальний показник Ляпунова, BDS-статистику), що передаються в каналі зв'язку. У таблиці 4.1 наведено отримані значення BDS-статистики й значення максимального показника Ляпунова.

Таблиця 4.1

Значення кількісних показників, одержаних для моделі системи зв'язку з простими сигналами

Показник	Значення
BDS-статистика	>1000
Максимальний показник Ляпунова	≤0

Як очевидно з візуальних (якісних) показників, досліджувані сигнали є регулярними. Отримані фазові портрети показують явну структурованість, оскільки за формою являють собою еліпс.

Далі розглянемо отримані кількісні показники системи зв'язку з простими сигналами. Значення максимального показника Ляпунова досліджуваних сигналів приймаємо або негативними, або нульовими, що вказує на регулярність процесу.

Отже, встановлено, що системи зв'язку на основі простих сигналів є регулярними та досить легко виявляються відомими підходами [23]. Також зауважимо, що отримані якісно-кількісні показники можна поширити і інші типи простих сигналів, наприклад прямокутні імпульси, оскільки вони у подібному випадку мають схожі характеристики.

З цього можна зробити висновок про те, що системи зв'язку на основі простих сигналів, навіть у разі використання криптографічних методів захисту, вразливі до таких деструктивних впливів, як перехоплення і радіоелектронне придушення трафіку, цей факт вказує на їх низьку прихованість.

Зауважимо, що однією з областей використання систем зв'язку на основі простих сигналів є різноманітні бездротові системи передачі даних,

зокрема системи охоронно-пожежної сигналізації, системи автомобільної безпеки, робототехнічні комплекси та інші. Тобто дані бездротові системи передачі даних так само вразливі від перехоплення і радіоелектронного придушення трафіку, що також вказує на їх низьку прихованість.

Проведемо оцінку достовірності сигналів.

В якості джерела інформації виберемо генератор рівномірних прямокутних імпульсів, що працює в діапазоні [-1; 1].

За код розширення візьмемо m-послідовності, які знаходять активне застосування в сучасних системах зв'язку (за своїми характеристиками вони близькі до інших подібних послідовностей, наприклад кодів Баркера; так само на їх основі будуються інші послідовності) [24]. Вони є лінійними рекурентними послідовностями максимального періоду, що формуються k-розрядними генераторами на основі регістрів зсуву.

Для цілей аналізу хаотичності моделюваної системи зв'язку змінюватимемо параметри блоку m-послідовностей (PN Sequence generator). Задамо такі параметри: vector of length of register - 20; vector of initial condition register — від 3 до 46.

Серед особливостей процесу моделювання відзначимо той факт, що в каналі зв'язку на сигнали, що передаються, діє адитивна гауссівська перешкода.

В процесі моделювання вважаємо, що передавальна та приймальна сторони синхронізовані у часі між собою.

Також припустимо, що вихідний інформаційний сигнал вже пройшов процедуру завадостійкого кодування.

В результаті процесу моделювання отримані фазові портрети мають схожий вигляд із рис. 4.6.

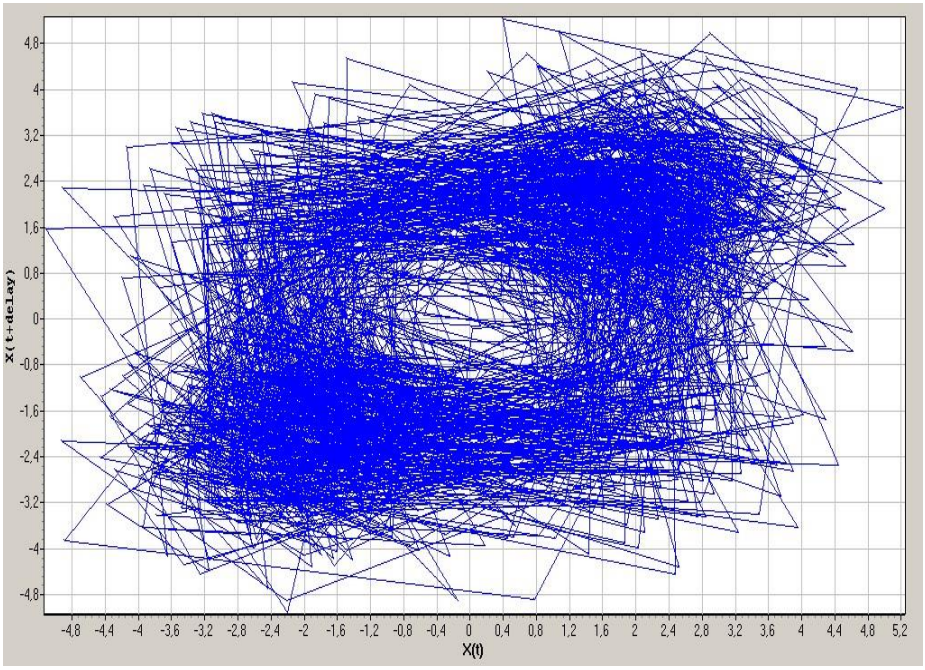


Рисунок 4.6 – Фазовий портрет сигналу, щопередається в каналі зв’язку

Далі розглянемо отримані кількісні показники сигналів системи зв'язку, що передаються з прямим розширенням спектра (максимальний показник Ляпунова.

На рис. 4.7 наведені отримані значення максимального показника Ляпунова, причому по осі ординат розташовані значення максимального показника Ляпунова, а по осі абсцис - значення vector of init condition register.

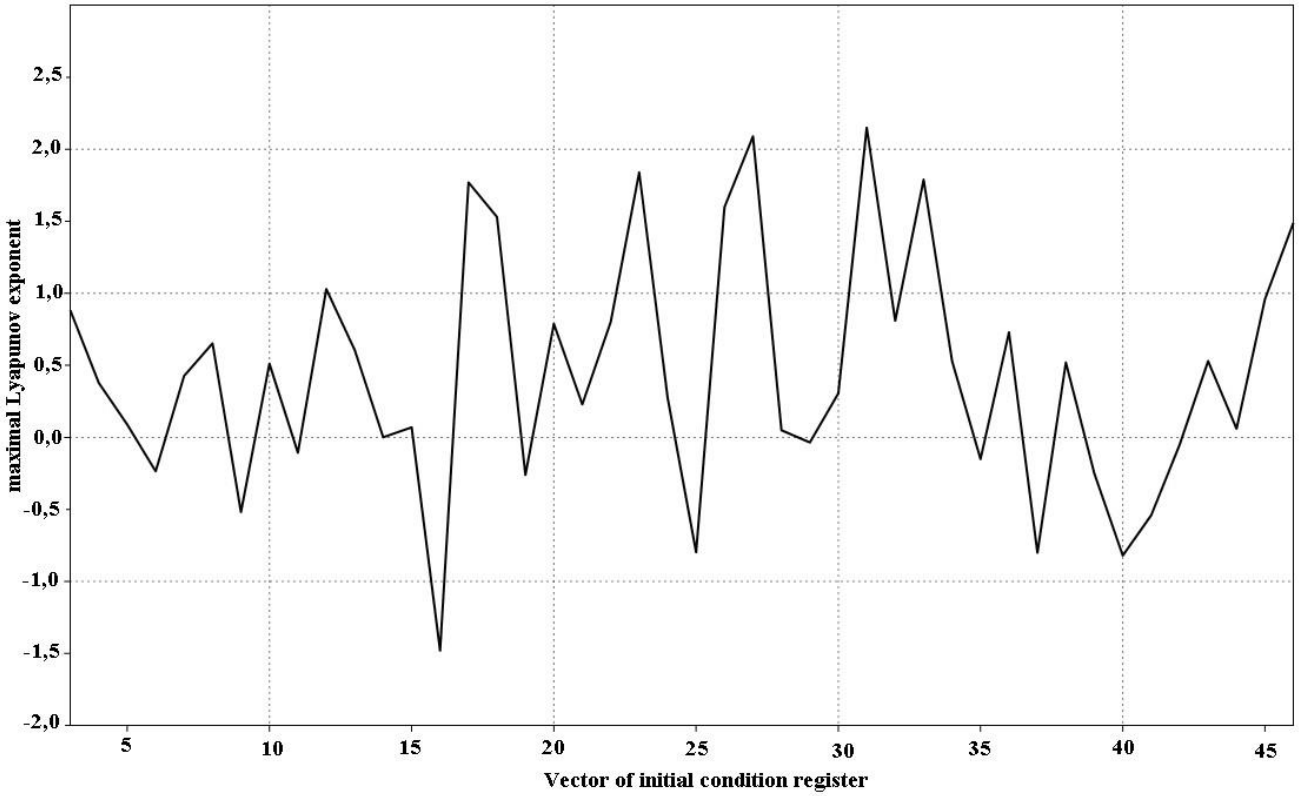


Рисунок 4.7 – Значення максимального показника Ляпунова сигналів зв’язку, що передаються, з прямим розширенням спектра з допомогою m-послідовностей

Отримані кількісні показники моделі системи зв'язку з прямим розширенням спектра з допомогою m-послідовностей наведені у таблиці 4.2.

Таблиця 4.2

Значення кількісних показників, одержаних для моделі системи зв'язку з прямим розширенням спектру

Показник	Значення
Максимальний показник Ляпунова	[-0,7÷1,65]

Як видно з візуальних (якісних) показників для сигналів, отриманих за допомогою m-послідовностей, сигнали, що досліджуються, є шумоподібними. Отримані фазові портрети показують деяку близькість

досліджуваного процесу до поняття «білого шуму», проте явно видно його структурованість. Далі розглянемо отримані кількісні показники системи зв'язку з прямим розширенням спектра з допомогою m-послідовностей. Значення максимального показника Ляпунова досліджуваних сигналів у середньому не перевищують 1,65. Також серед отриманих значень є значення 0, що вказує на регулярність процесу.

Відомо, що максимальний показник Ляпунова для відомих підходів формування шумоподібних сигналів та їх похідних, наприклад, квазішумові сигнали знаходиться приблизно в діапазоні [0...1,5].

Проведемо оцінку достовірності сигналів, що генеруються програмною реалізацією розробленої моделі процесу забезпечення потайного інформаційного обміну. Проведемо їх візуальний (якісний) та кількісний аналіз на основі відомих методів нелінійної динаміки. Зауважимо, інші отримані фазові портрети мають схожий вигляд із рис. 4.8.

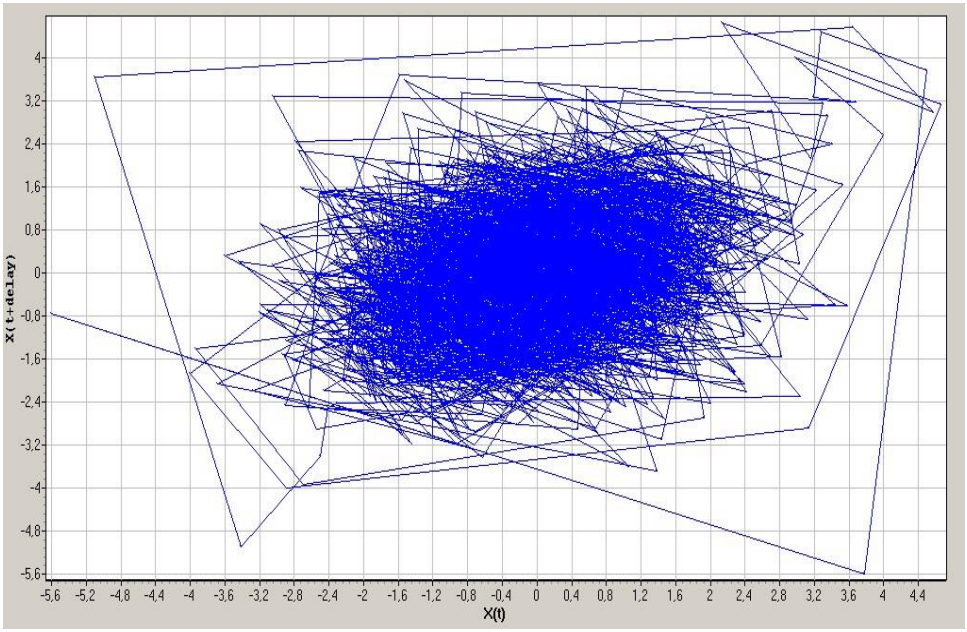


Рисунок 4.8 – Фазовий портрет сигналу, що передається в каналі зв’язку з осцилятором Ван дер Поля

Далі розглянемо отримані кількісні показники сигналів, що передаються в каналі зв'язку, заснованих на використанні в якості генератора

хаотичних сигналів взято осцилятор Ван дер Поля (максимальний показник) [25]. Значення максимального показника Ляпунова наведено рис. 4.9, причому по осі ординат розташовані значення максимального показника Ляпунова, а осі абсцис — значення змінної А.

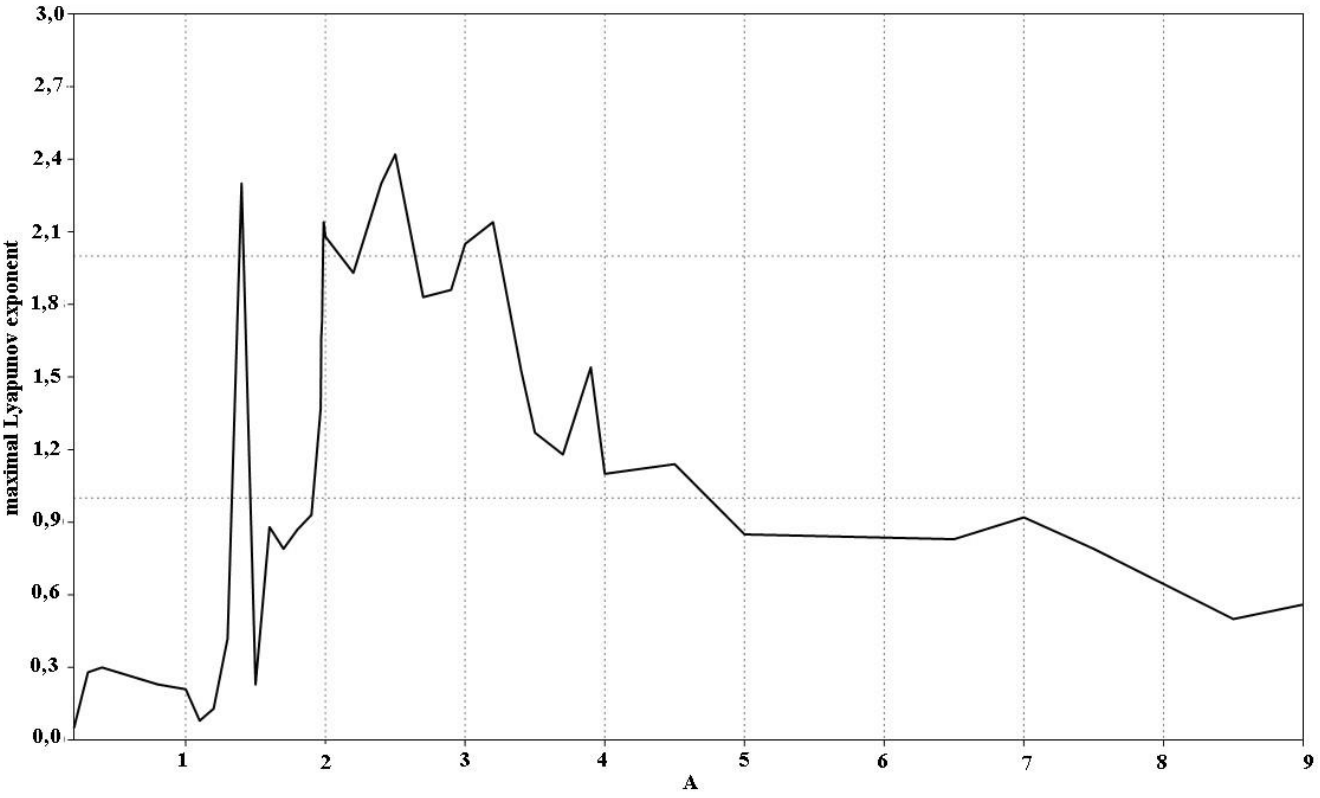


Рисунок 4.9 – Значення максимального показника Ляпунова сигналів, що передаються в каналі зв'язку з осцилятором Ван дер Поля

Отримані кількісні показники при використанні як генератора хаотичних сигналів збуреного осцилятора Ван дер Поля наведені в таблиці 4.3.

Таблиця 4.3

Значення кількісних показників

Показник	Значення
Максимальний показник Ляпунова	[0÷2,3]

Як видно з наведених візуальних (якісних) показників для сигналів, отриманих за допомогою збуреного осцилятора Ван дер Поля, сигнали, що досліджуються, є шумоподібними. Фазові портрети показують їхню нелінійність і близькість до поняття «білого шуму». Тепер розглянемо одержані кількісні показники. Значення максимального показника Ляпунова [0 … 2,3], вказують на те, що сигнали, отримані за допомогою збуреного осцилятора Ван дер Поля, мають позитивні значення максимального показника Ляпунова та, відповідно, є хаотичними.

Далі розглянемо кількісні та якісні показники сигналів, отриманих за допомогою атрактора Ресслера. Спочатку розглянемо візуальні (якісні) показники сигналів, що передаються в каналі зв'язку (фазові портрети) [26]. На рис. 4.9 наведено приклад фазового портрета сигналів, що передаються в каналі зв'язку, отриманого за допомогою атрактор Ресслера.

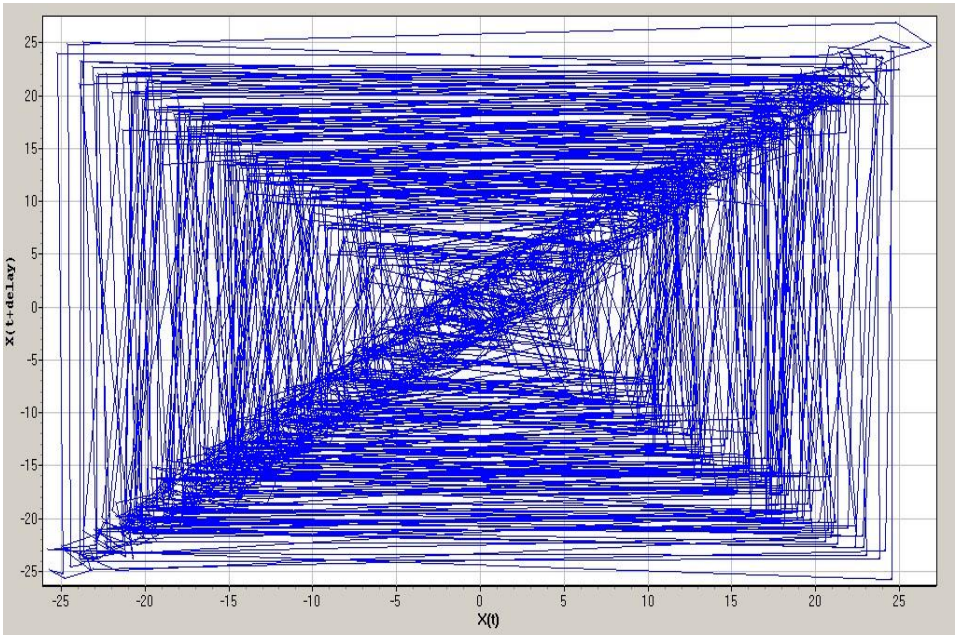


Рисунок 4.9 – Фазовий портрет сигналу, що передається у каналі зв'язку з атрактором Ресслера

Значення максимального показника Ляпунова наведено рис. 4.10, причому по осі ординат розташовані значення самого показника Ляпунова, а осі абсцис — значення змінної c.

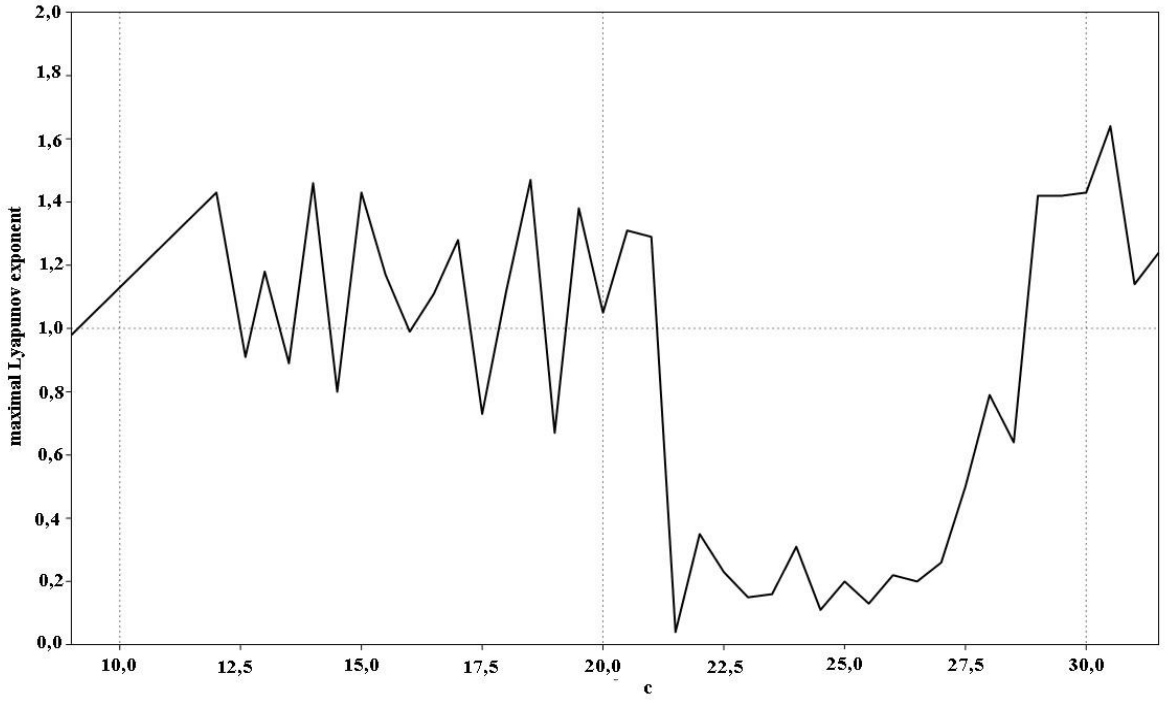


Рисунок 4.10 – Значення максимального показника Ляпунова для даного спектру сигналів з атрактором Ресслера

Другою з додаткових програм, що входять до розробленого комплексу є програмна реалізація моделі системи зв'язку на основі прямого розширення спектру – «MoDiSeSS», створена за допомогою системи математичного моделювання та інженерних обчислень ScicosLab. Програма «MoDiSeSS» призначена для обґрунтування можливості практичного використання системи зв'язку на основі прямого розширення спектра при змінах параметрів послідовностей. Програма дозволяє отримати часові реалізації сигналів, що передаються в каналі зв'язку і сигналів, відновлених на приймальній стороні. Мова програмування: C++.

На сьогодні, пряме розширення спектра для бездротових систем передачі, зокрема систем охоронно-пожежних систем, є перспективним напрямом розвитку. За рахунок використання прямого розширення спектра можна досягти високої прихованості передачі інформації. На рис 4.11 наведено графоаналітичне представлення розробленої програми, що реалізує модель системи зв'язку на основі прямого розширення спектра.

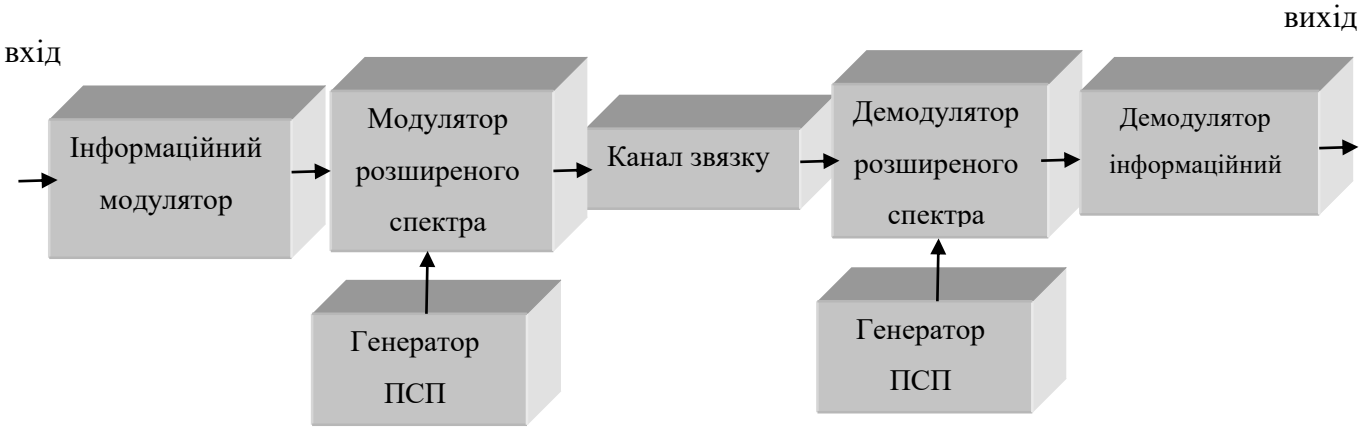


Рисунок 4.11 – Графоаналітичне представлення розробленої програми, що реалізує модель системи зв'язку на основі прямого розширення спектра

Алгоритм роботи системи зв'язку на основі прямого розширення полягає в наступному: на стороні передачі інформаційна послідовність d(t) модулюється за допомогою ПСП p(t), і отриманий корисний сигнал m(t) випромінюється в канал зв'язку. При передачі лініями зв'язку корисний сигнал m(t) підсумовується з перешкодами n(t), після чого змішаний сигнал r(t) надходить на вхід модуля, що реалізує функції приймача. На приймальній стороні сигнал r(t) демодулюється за допомогою точної копії ПСП p(t), яка використовується в модулі, що реалізує функції передавача. В результаті подальшої демодуляції сигналу z(t) виходить інформаційна послідовність d(t).

На рис. 4.12 наведено спрощений алгоритм роботи розробленої програми. Вхідними параметрами для розробленої програми є інформаційна послідовність d(t) та ПСП p(t). Інформаційна послідовність d(t) за допомогою ПСП p(t) перетворюється на корисний сигнал m(t). При передачі лініями зв'язку корисний сигнал m(t) підсумовується з перешкодами n(t), після чого виходить сигнал r(t). Далі сигнал r(t) демодулюється за допомогою точної копії ПСП p(t), що використовується на приймальній стороні. В результаті подальшої демодуляції сигналу z(t) виходить інформаційна послідовність

d(t). Вихідними параметрами для розробленої програми є сигнал r(t) і інформаційний сигнал d(t), що передається в каналі зв'язку.

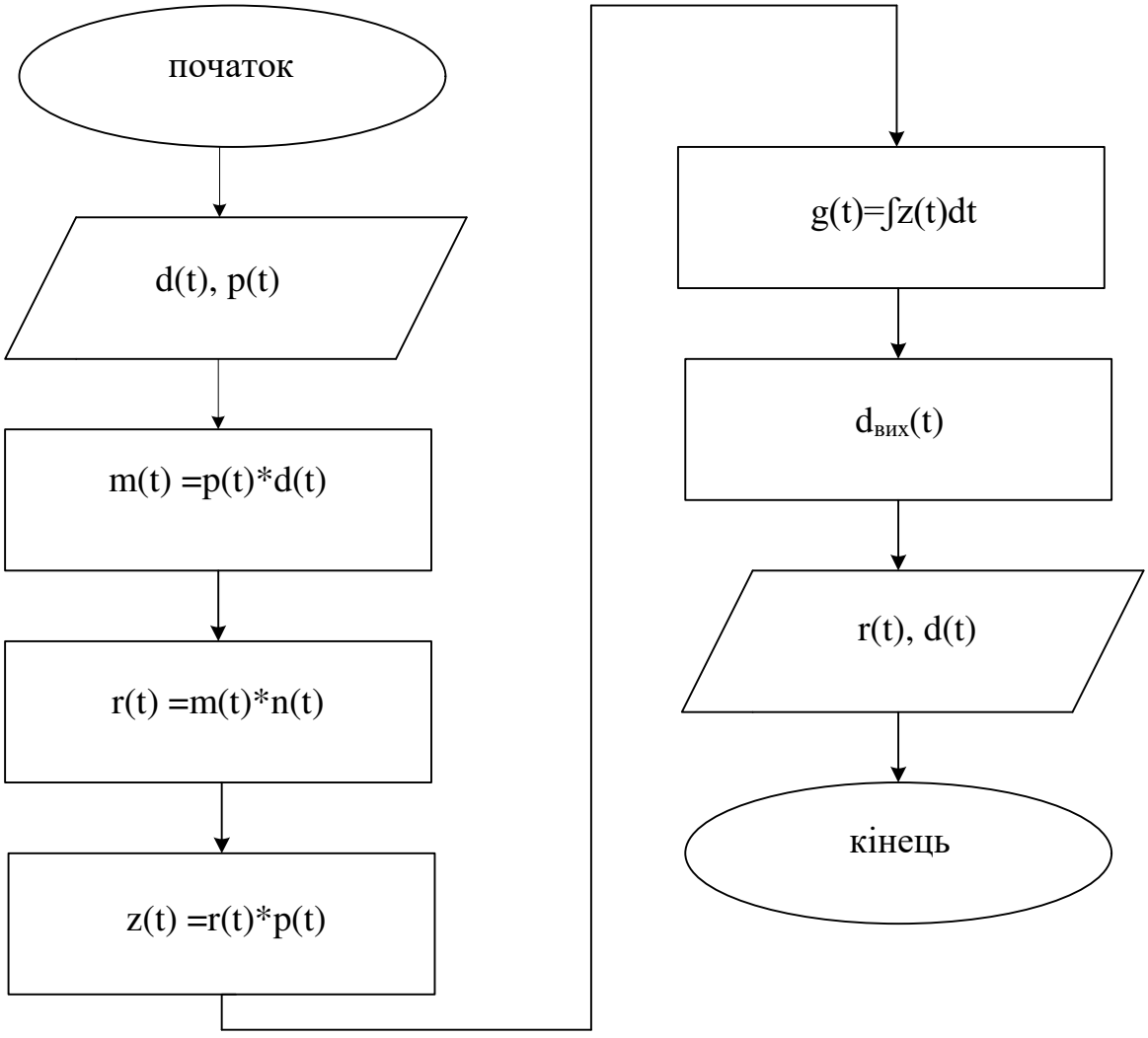


Рисунок 4.12 – Спрощений алгоритм роботи розробленої програми «MoDiSeSS»

4.3 Застосування розроблених моделей обчислювального методу

На рис. 4.13 наведена часова діаграма сигналу моделі системи зв'язку з прямим розширенням спектра, що передається в каналі зв'язку. Вона отримана за допомогою програми «MoDiSeSS». Як легко помітити, вона має шумоподібний вигляд і з неї візуально важко виділити вихідний інформаційний сигнал.

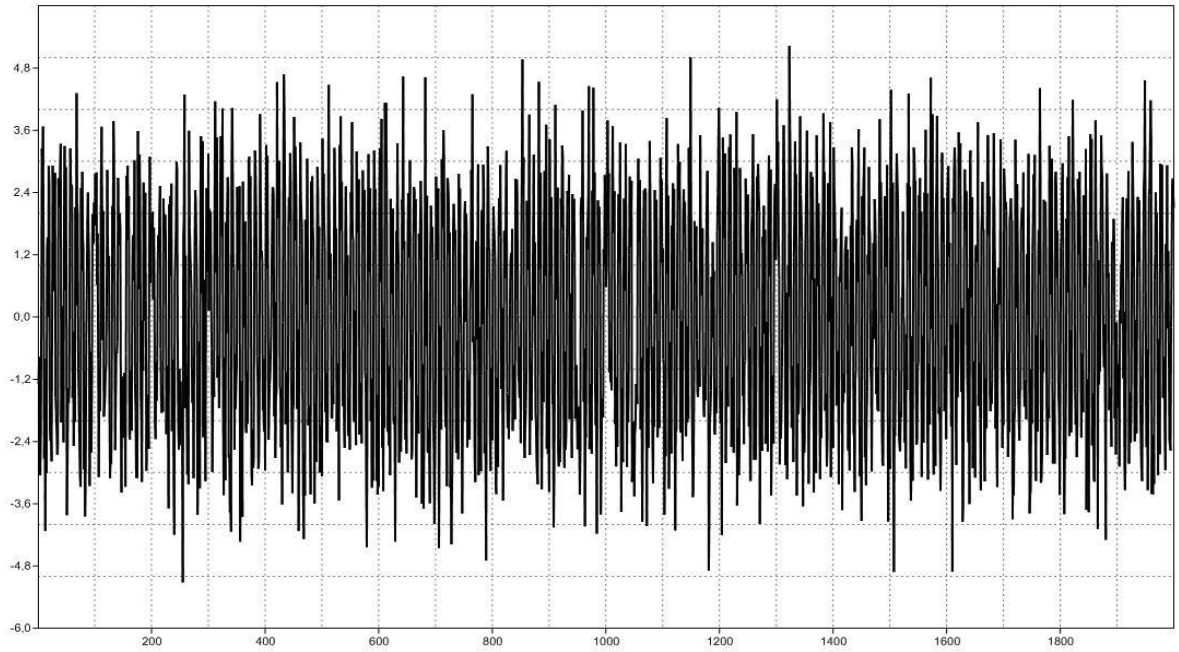


Рисунок 4.13 – Часова діаграма переданого сигналу в каналі звязку з прямим розширенням спектра

Як видно з першого розділу, важливим показником, як для хаотичних, так і для шумоподібних сигналів, є значення BDS статистики сигналів, що передаються. Для того, щоб коректно застосувати методи нелінійної динаміки до отриманих у програмі «MoDiSeSS» даних, спочатку необхідно визначити мінімальну розмірність атрактора (псевдоаттрактора).

На рис. 4.14 наведено розрахункові значення BDS-статистики сигналів, отриманих для моделі системи зв'язку з прямим розширенням спектра, причому по осі ординат розташовані значення BDS-статистики, а по осі абсцис - значення vector of initial condition register.

Отримані значення BDS-статистики показують, що сигнали системи зв'язку з прямим розширенням спектра знаходяться в діапазоні значень BDS-статистики. Значення BDS-статистики для відомих підходів формування шумоподібних сигналів та їх похідних, наприклад, азоманіпульовані сигнали, знаходяться також біля значень 0…40. Значенню BDS-статистики 40 відповідає авторегресійний процес.

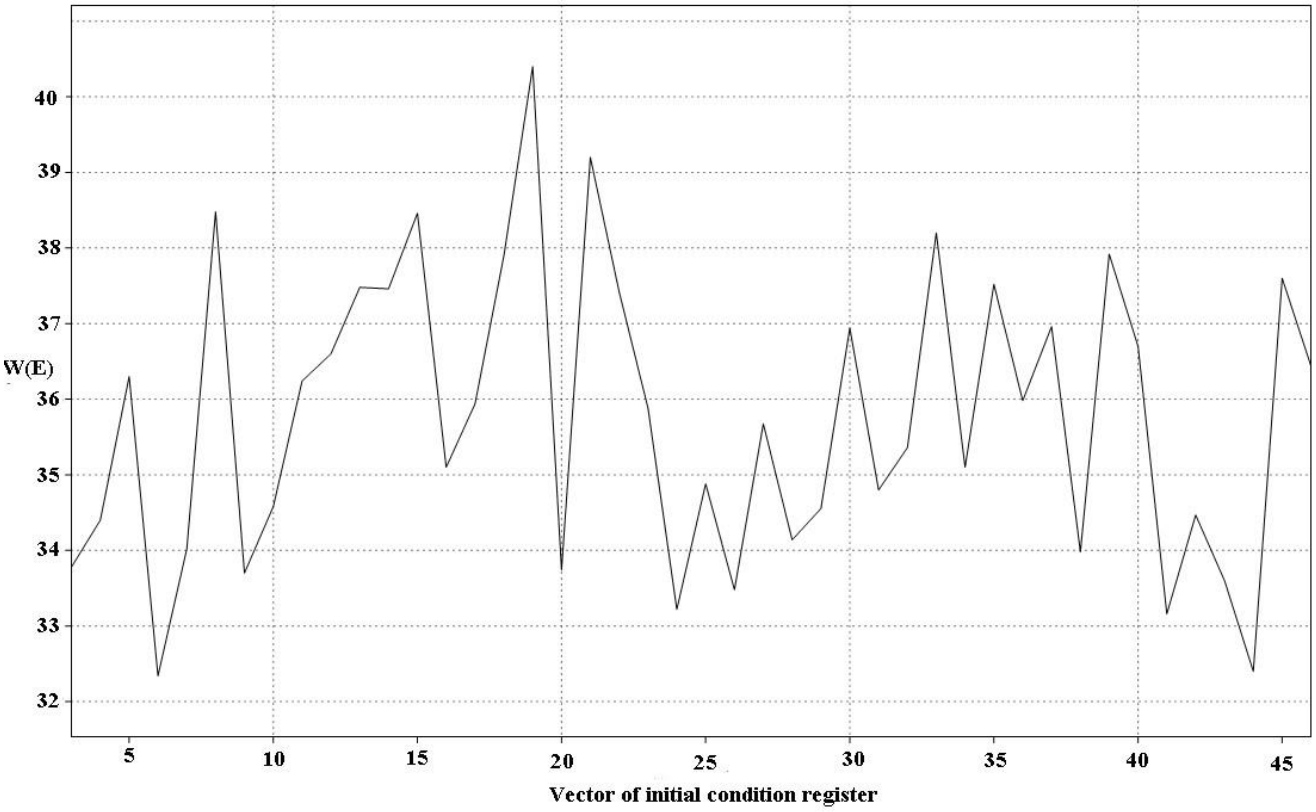


Рисунок 4.14 – Значення BDS-статистики сигналів, що передаються в каналі зв'язку з BDS-статистикою

Отже, системи зв'язку на основі відомих підходів формування шумоподібних сигналів та їх похідних, у тому числі система зв'язку на основі прямого розширення спектру, потенційно класифікуються за допомогою BDS-статистики, і це означає, що вони мають недостатню прихованість від стороннього спостерігача.

Для вироблення хаотичних сигналів за допомогою генератора Ван дер Поля, представленого виразом (4.1), необхідно змінювати праметр А в діапазоні приблизно від 1 до 8. Як джерело інформації необхідно взяти генератор рівномірних прямокутних імпульсів, що працює в діапазоні [-1;1]. Серед інших особливостей процесу моделювання відзначимо той факт, що на сигнали, що передаються в каналі зв'язку діє адитивна гауссівська перешкода. В результаті процесу моделювання було отримано близько 50 різних часових реалізацій сигналів (довжина кожного 2000), що передаються

в каналі зв'язку. Оптимальним значенням вибірки для реальних систем зв'язку на основі шумоподібних сигналів є вибірка 70-100, а оптимальна довжина вибірки від 1000 до 4000. Виходячи з цього, отриманих даних буде достатньо для коректного аналізу процесів, що відбуваються в системі зв'язку.

На рис. 4.15 наведена часова діаграма сигналу, що передається в каналі зв'язку. Як легко помітити, вона має шумоподібний вигляд і з неї також візуально важко виділити вихідний інформаційний сигнал.

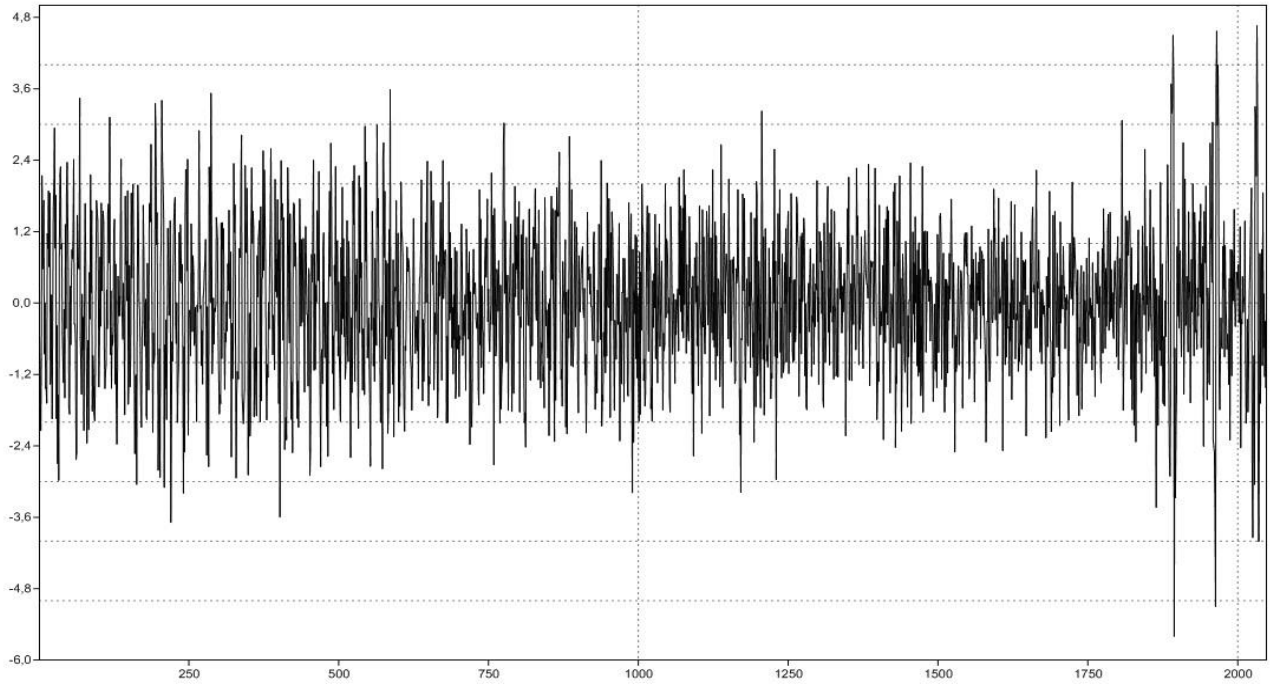


Рисунок 4.15 – Часова діаграма сигналу, що передається у каналі зв'язку за допомогою осцилятора Ван дер Поля

Як зазначено в першому розділі, для хаотичних сигналів важливим показником є значення пік-фактора, що обчислюється за допомогою виразу (1.20). На рис. 4.16 наведено розраховані значення пік-фактора сигналів, що передаються, створені за допомогою осцилятора Ван дер Поля, причому по осі ординат розташовані значення пік-фактора переданих сигналів Crest, а по осі абсцис - значення змінного параметра A.

Як видно з рис. 4.16, при використанні в якості коду розширення осцилятора Ван дер Поля значення пік-фактора сигналів дорівнює Crest = [1,8 ... 3,6], що є прийнятним показником, так як не перевищує значення пік-фактора, рівного 4.

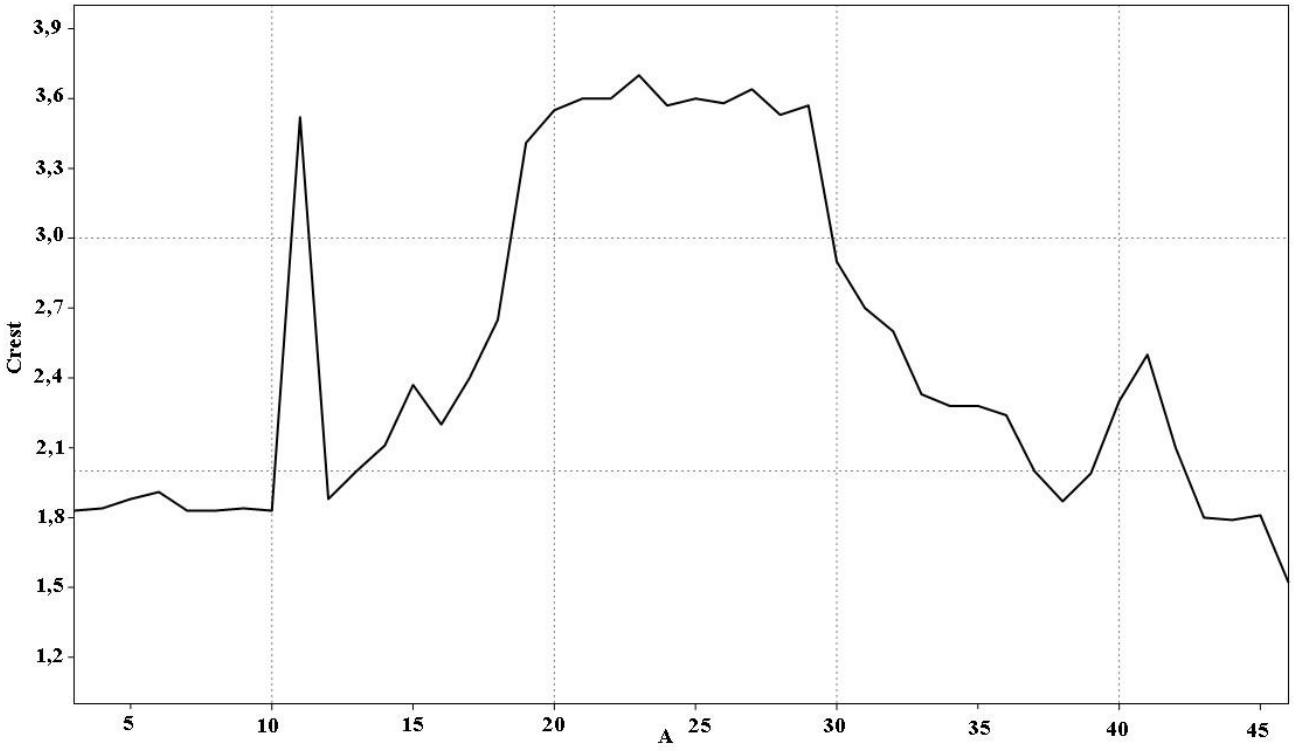


Рисунок 4.16 – Значення пік-фактора сигналів, отриманих під час використання осцилятора Ван дер Поля

Важливо відмітити, що передані сигнали мають прийнятний рівень пік-фактору і можуть використовуватися для бездротових систем передачі даних.

Ще одним важливим показником для хаотичних сигналів є значення BDS-статистики сигналів, що передаються. Для того, щоб коректно застосувати методи нелінійної динаміки до отриманих даних, спочатку необхідно визначити мінімальну розмірність атрактора. Відомо, що мінімальна розмірність атрактора (псевдоаттрактора) сигналів, що передаються, через осцилятор Ван дер Поля, дорівнює 3.

На рис. 4.17 наведено розраховані значення BDS-статистики для сигналів, отриманих за допомогою осцилятора Ван дер Поля, причому по осі

ординат розташовані значення BDS-статистики, а по осі абсцис - значення параметра A, що змінюється.

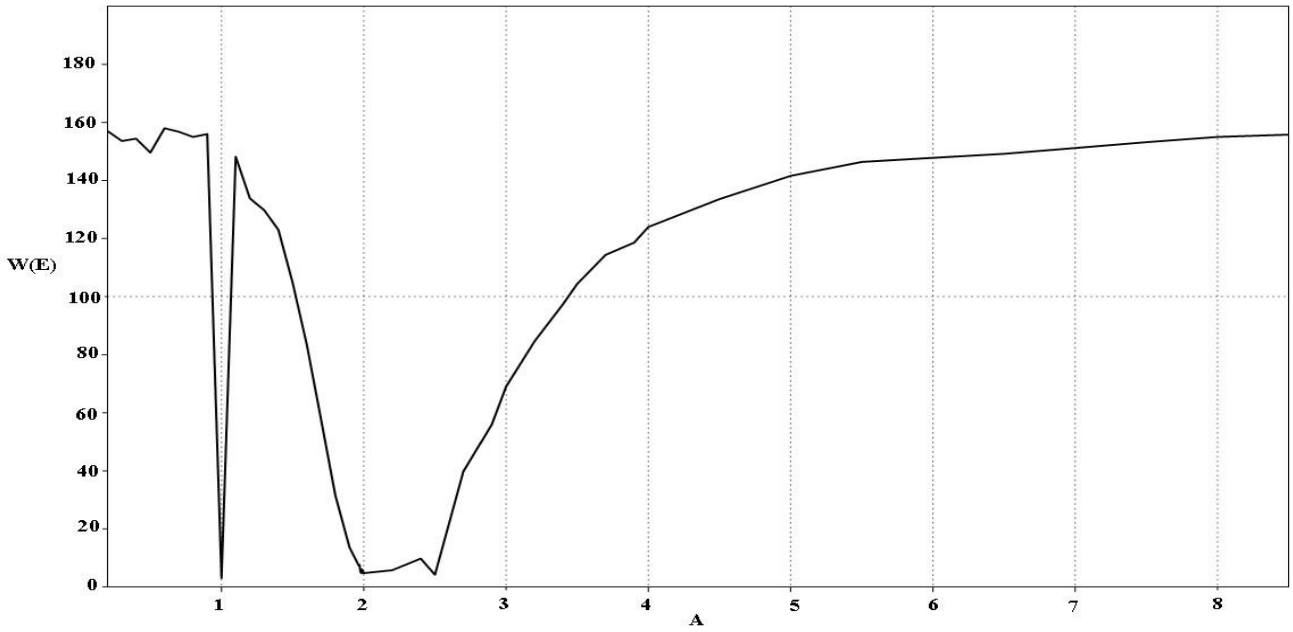


Рисунок 4.17 – Значення BDS-статистики сигналів, що передаються в каналі зв'язку, отриманих при використанні осцилятора Ван дер Поля

Значення BDS-статистики показують, що сигнали, отримані за допомогою осцилятора Ван дер Поля, визначаються досить близько, на певному відрізку, розташовані до значення BDS-статистики, яке визначає поняття «білого шуму» (потенційно відносяться до персистентних процесів (чорний шум), оскільки потрапляють у діапазон [3...19]), або мають значення BDS-статистики в 2-3 рази менше, ніж встановлено для хаотичних сигналів.

Дані обставини вказують на виконання умови виразу (1.30) для BDS-статистики, що описує постановку завдання магістерської роботи.

Таким чином, можливо, зробити висновок, що передані сигнали мають прихованість від стороннього спостерігача.

Також проведені розрахунки дозволили вибрати в якості генератора хаотичних сигналів ще один генератор – атрактор Ресслера [26].

Для генерації хаотичних сигналів за допомогою необхідно змінювати параметр *c* в діапазоні приблизно від 9 до 35. В якості джерела інформації

необхідно вибрати генератор рівномірних прямокутних імпульсів, що працює в діапазоні [-1;1]. Серед інших особливостей процесу моделювання відзначимо той факт, що на сигнали які передаються в каналі зв'язку діє адитивна гауссівська перешкода.

На рис. 4.18 наведено часову діаграму сигналу, що передається в каналі зв'язку. Як легко помітити, вона має шумоподібний вигляд і з неї також візуально важко виділити вихідний інформаційний сигнал.

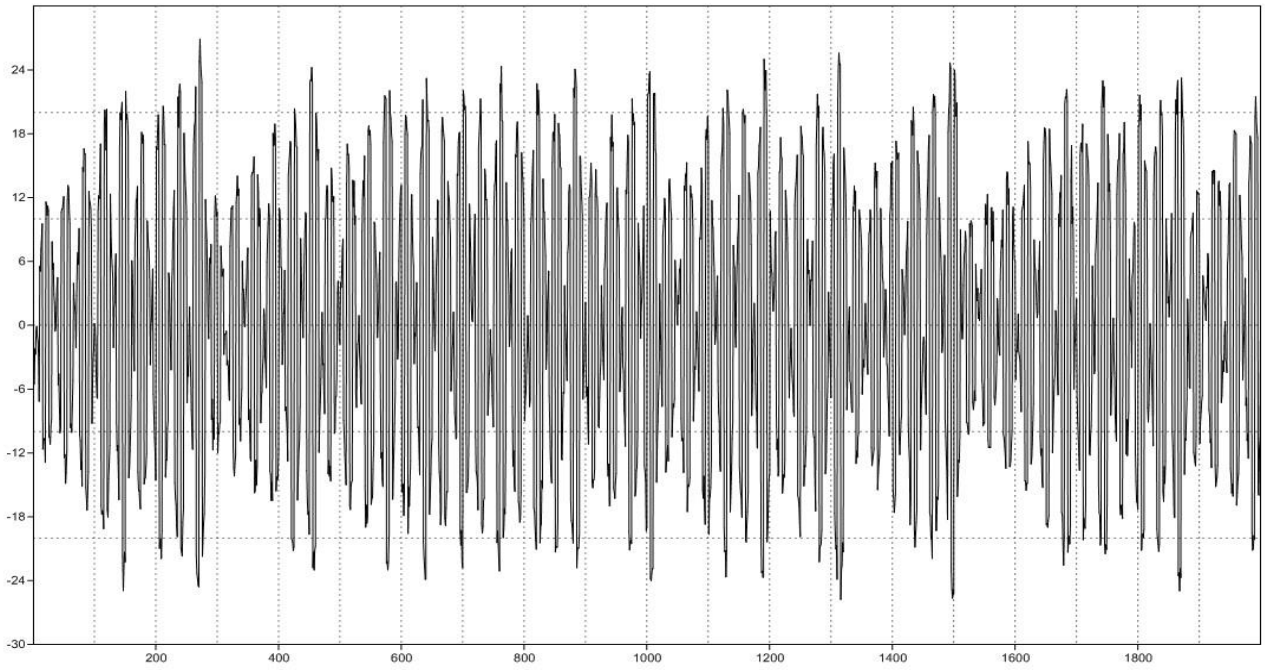


Рисунок 4.18 – Часова діаграма сигналу, що передається у каналі зв'язку з шумоподібним виглядом

На рис. 4.19 наведені розраховані значення пік-фактора сигналів, що передаються, створені за допомогою атрактора Ресслера, причому по осі ординат розташовані значення пік-фактора переданих сигналів Crest, а по осі абсцис - значення змінного параметра *c*.

Під час використання в якості коду розширення атрактора Ресслера значення пік-фактора сигналів дорівнює Crest [1,9 ... 2,6], що є прийнятним показником, так як не перевищує значення пік-фактора, рівного 4. Дані обставини вказують на виконання умови (1.30) для пік-фактора Crest.

Отже, можна стверджувати, що передані сигнали мають прийнятний рівень пік-фактору і можуть використовуватися для бездротових систем передачі даних.

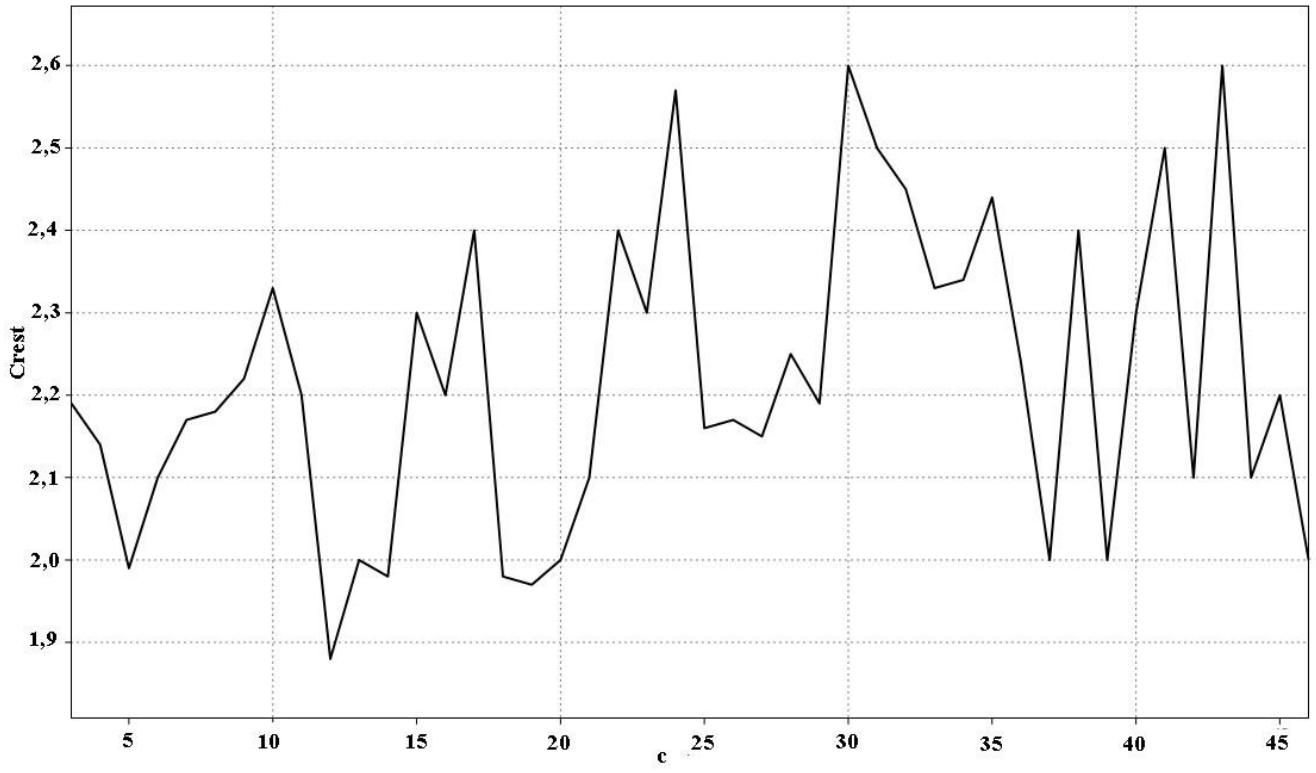


Рисунок 4.19 – Значення пік-фактора сигналів, отриманих під час використання атрактора Ресслера

Мінімальна розмірність атрактора (псевдоаттрактора) переданих сигналів, що використовують як генератор хаотичних сигналів атрактор Ресслера, дорівнює 3. На рис. 4.20 наведено значення BDS-статистики для сигналів, отриманих за допомогою атрактора Ресслера [26], причому по осі ординат розташовані значення BDS-статистики, а по осі абсцис - значення параметра *c*, що змінюється.

Значення BDS-статистики [100…125] сигналів, отриманих за допомогою атрактора Ресслера, мають значення BDS-статистики у 2–3 рази менше, ніж встановлено для хаотичних сигналів (діапазон [200…500]).

Отже, передані сигнали мають прихованість від стороннього спостерігача.

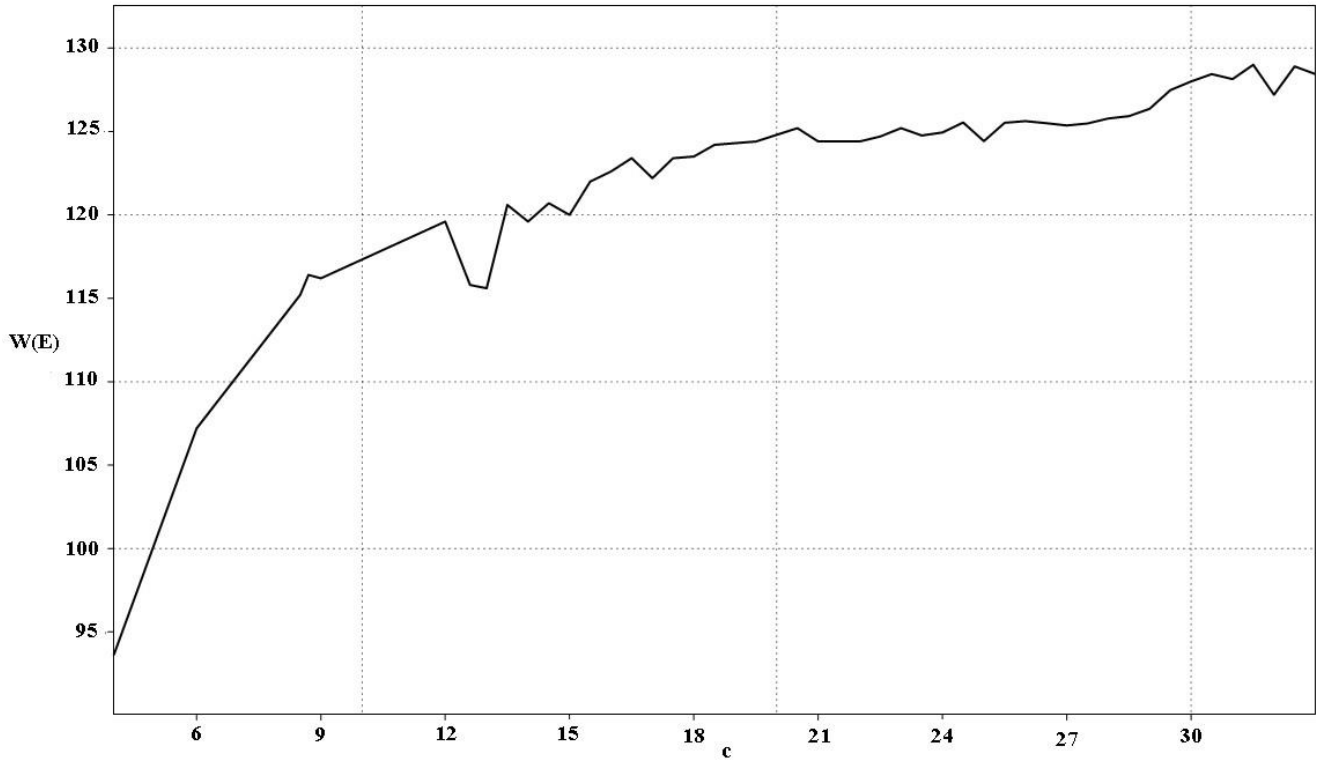


Рисунок 4.20 – Значення BDS-статистики сигналів, що передаються в каналі зв'язку, отриманих при використанні атрактора Ресслера

На рис. 4.21 введено структуру пристрою імітозахисту контрольованих об'єктів з підвищеною структурною прихованістю сигналів-переносників.

Пристрій має такі позначення: 1 – датчик, 2 – блок пам'яті стартової послідовності, 3 – блок порівняння, 4 – генератор ПСП-2, 5 – блок перетворення n-розрядної паралельної комбінації на послідовну, 6 – блок пам'яті, 7 – блок перетворення послідовної комбінації в n-розрядну паралельну, 8 - демодулятор, 9 - модулятор, 10 - узгоджувальний пристрій, 11 - блок обробки інформації, 12 - блок пам'яті стартової послідовності, 13 - блок перетворення n-розрядної паралельної комбінації в послідовну, 14 - модулятор , 15 - узгоджувальний пристрій, 16 - генератор ключа, 17 - генератор ПСП-1, 18 - блок пам'яті контрольного значення, 19 - демодулятор, 20 - генератор ПСП-2, 21 - блок першого пристрою, 22 - блок порівняння, 23 - блок перетворення послідовної комбінації в nрозрядну паралельну, 24 - блок другого пристрою, 25 - блок прийому інформації, 26 - блок управління, 27 -

блоку вибору сигналів, 28 - блок передавача, 29 - модулятор-передавач, 30 - накопичувач хаотичного сигналу, 3 – лінія зв'язку, 32 – блок приймача, 33 – смуговий фільтр, 34 – підсилювач, 35 – перший помножувач, 36 – другий помножувач, 37 – інвертор, 38 – накопичувач копії хаотичного сигналу, 39 – перший інтегратор, 40 – другий інтегратор, 41 - пристрій, що вичитує, 42 - вирішальний пристрій, 43 -блок вибору сигналів, 44 - блок передавача, 45 - модулятор-передавач, 46 - накопичувач хаотичного сигналу, 47 - блок 47 передачі інформації, 48 - лінія зв'язку, 49 - блок приймача, 50 – смуговий фільтр, 51 – підсилювач, 52 – перший помножувач, 53 – другий помножувач, 54 – інвертор, 55 – накопичувач копії хаотичного сигналу, 56 – перший інтегратор, другий 57 – інтегратор, 58 – вичитувальний пристрій, 59 – вирішальний пристрій, 60 - транслятор.

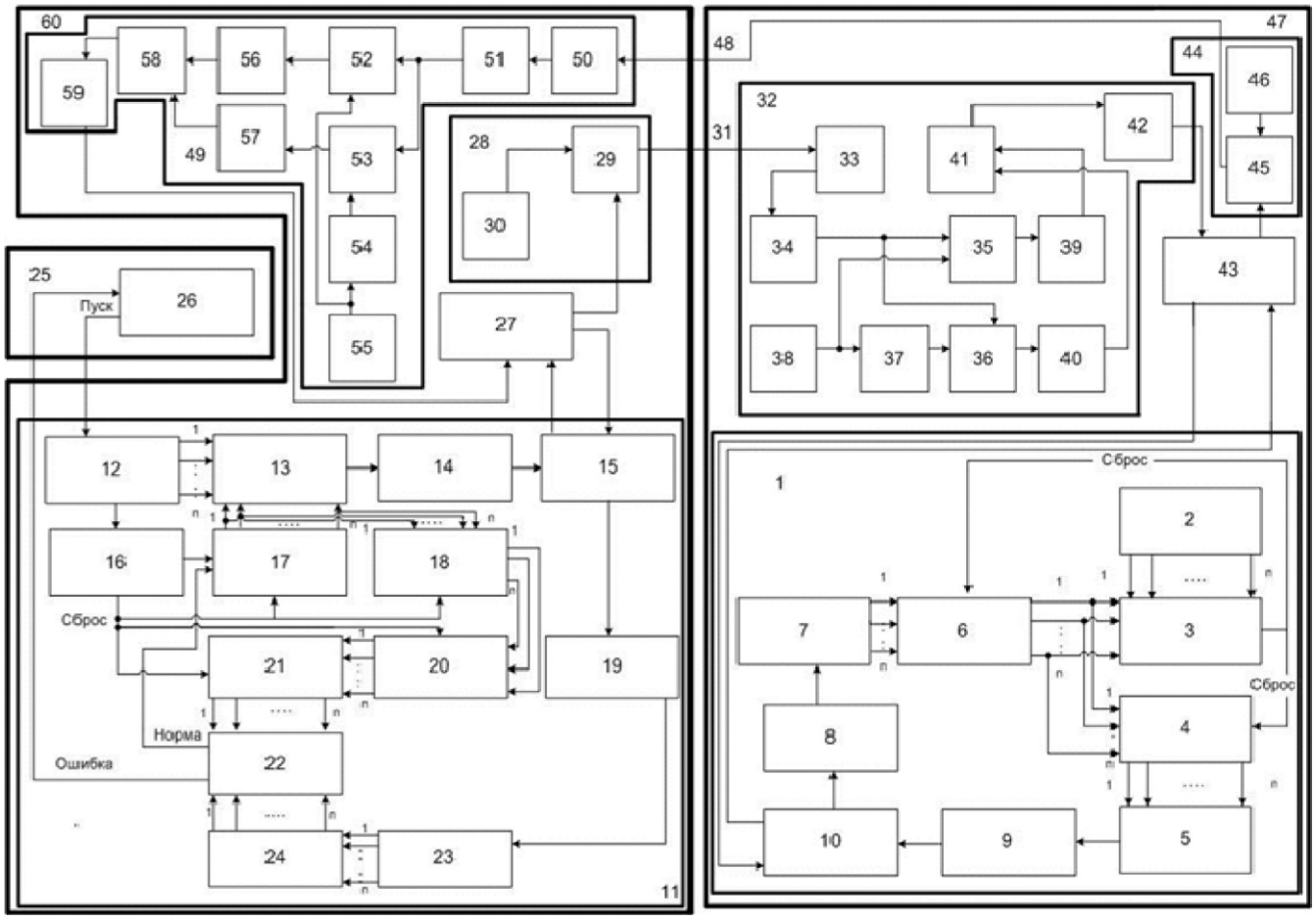


Рисунок 4.21 – Структурна схема пристрою імітозахисту контрольованих об'єктів з підвищеною структурною прихованістю сигналів

Цей пристрій функціонує так. Для запуску блоку контролю на вхід генератора 17 ПСП-1 подається стартова команда. Після цього 17 генератор ПСП-1 виробляє перше псевдовипадкове число. Отримане значення відправляється на 20 генератор ПСП-2 блоку контролю і одночасно з цим перемножується з 30 хаотичною послідовністю через лінію зв'язку передається на контрольований об'єкт (датчик). Після цього відбувається декодування отриманого сигналу за допомогою копії 36 хаотичного сигналу, ідентичної хаотичної послідовності в блоці контролю, і далі декодований сигнал у вигляді послідовності надходить в 4 генератор ПСП2, функція генерації послідовності якого ідентична функції 20 генератора ПСП-2 блоку контролю. Потім відбувається перемноження послідовності ПСП-2 контрольованого об'єкта (датчика) з хаотичною послідовністю 46 і через лінію зв'язку передається на блок контролю. Після цього відбувається декодування отриманого сигналу за допомогою 55 копії хаотичної послідовності, ідентичної хаотичної послідовності в контрольованому об'єкті (датчику), і далі декодований сигнал у вигляді послідовності надходить на пристрій порівняння 22, в якому перевіряється відгук раніше прийшов значення 20 генератора ПСП-2 блоку контролю та відгук 4 генератора ПСП-2 контрольованого об'єкта (датчика). У разі збігу значень, що прийшли від контрольованого об'єкта (датчика) і блоку контролю, виробляється сигнал Норма, який служить для генерації наступного псевдовипадкового числа 17 генератором ПСП-1. При розбіжності значень пристрій порівняння видає команду «Тривога».

Другим розробленим пристроєм є пристрій імітозахисту контрольованих об'єктів із затримкою відповіді за часом, побудований на основі моделі процесу забезпечення потайного інформаційного обміну та модифікованого алгоритму її реалізації з ускладненою імітовставкою.

Даний пристрій представлено на рис. 4.22 й має такі позначення: 1 – блок контролю, 2 – керуючий пристрій, 3 – блок підготовки датчика до роботи, 4 – блок програмованого постійного пам'яті таблиці датчиків, 5 –

генератор унікального ідентифікатора, 6 – суматор, 7 – генератор ПСП- 1, 8 – буфер вхідної кодограми; 9 – генератор ПСП-2; 10 – блок буферизації кодограми; 11 – буфер вихідної кодограми; 2, 15 – блок логічної операції «що виключає АБО» (XOR), 16 – блок оперативного пам'яті ПСП-2, 17 – буфер FIFO (First In – First Out: перший прийшов – перший вийшов), 18 – лінія зв'язку, 19 – блок контролю справності, 20 – блок порівняння serial number – серійного номера, 21 – блок датчика, 22 – блок постійного запам'ятовуючого пристрою serial number, 23 – блок ініціалізації датчика, 24 – блок програмованого постійного пам'яті унікального ідентифікатора (ППЗУ УІД), таймер, 26 - суматор, 27 - генератор ПСП-2, 28 - буфер вихідної кодограми, 29 - буфер, 30 - блок формування вихідної кодограми, 31 - буфер вхідної кодограми, 32 - ключ, 33 - блок приймального пристрою.

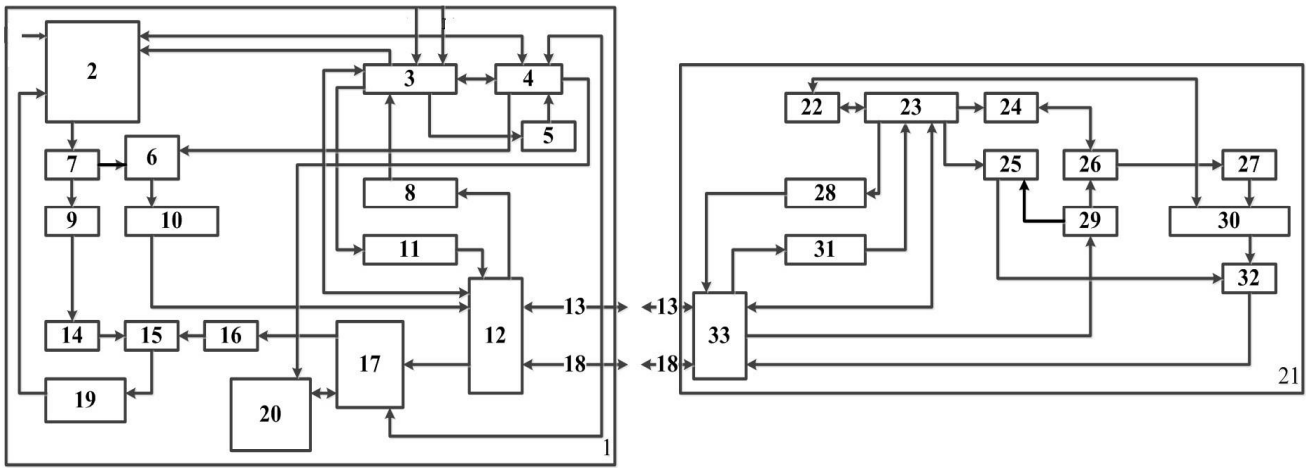


Рисунок 4.22 – Схема розробленого пристрою імітозахисту контрольованих об'єктів із затримкою відповіді за часом

Пристрій функціонує в такий спосіб.

У блоці контролю 4 ПЗП зберігається таблиця унікальних кодових послідовностей, що присвоюються кожному підключеному контрольованому об'єкту (датчику). Відповідна датчику кодова послідовність так само зберігається у його 24 ПЗП. При кожному циклі опитування датчиків 7 генератор ПСП-1 виробляє значення першої ПСП-1 і, одночасно з цим,

вибирається датчик з ПЗП датчиків, якого перевіряється на справжність, якого складається в блоці логічної операції XOR зі значенням першої ПСП-1. Отримане значення відправляється на 12 ППУ та через лінії зв'язку широкомовним запитом відправляється на всі контрольовані об'єкти. У всіх датчиках виробляється однакова послідовність дій: спочатку надіслане значення обробляється 33 ППУ і далі передається на блок логічної операції XOR, який одночасно з цим приходить датчика, який записаний в 24 ПЗП контрольованого об'єкта. Справжнє значення першої ПСП-1, сформоване 7 генератором ПСП-1, може декодувати лише той датчик, чий УІД збігається з переданим блоком ПЗП таблиці датчиків блок логічної операції XOR значенням УІД. Незважаючи на це, усі датчики роблять декодування переданого повідомлення. Отримане таким чином значення відправляється на 27 генератор ПСП-2, ініціалізуючи його на вироблення значення другої ПСП-2, яка передається в 33 ППУ і через лінію зв'язку блок контролю. Одночасно з цим 7 генератор ПСП-1 блоку контролю ініціалізує 9 генератор ПСП-2 значенням першої ПСП-1, яка була відправлена блок логічної операції XOR для відправки в контрольовані об'єкти. Значення другої ПСП-2 блоку контролю, і значення другий ПСП-2 заздалегідь обраного датчика, функції генерації послідовностей яких є однаковими, перевіряються в пристрої порівняння і оскільки вони були ініціалізовані значенням першої ПСП-1 блоку контролю, пристрій порівняння повинен видати сигнал « Норма», інакше видається сигнал «Тривога», що сигналізує про компрометацію датчика, що перевіряється. Крім того, в блоці контролю підраховується кількість відгуків, що прийшли, від інших датчиків і якщо їх менше або більше кількості датчиків в ПЗП датчиків, то теж видається сигнал «Тривога».

Зауважимо, що At-рівень деструктивної дії є високим. Відповідно до таблиці 4.1, в якій описано переведення нечіткого параметра At у чисельне значення й рівень деструктивного впливу буде At = 4 або вище.

Виходячи з цього, вони матимуть високий Р-рівень забезпечення пихованості інформаційного обміну від «перегляду», «підміни», «перехоплення» та «радіоелектронного придушення».

Відповідно до таблиці 4.2, в якій описаний переведення нечіткого параметра Р у чисельне значення означає, що рівень забезпечення скритності від перегляду, заміни, перехоплення та придушення перешкодами буде високим, тобто Р=2. Отримані розрахунки наведено у таблиці 4.5.

У табл.. 4.5 введено такі позначення: «ДВ1» – деструктивний вплив «перегляд», «ДВ2» – деструктивний вплив «підміна», «ДВ3» – деструктивний вплив «перехоплення», «ДВ4» – деструктивний вплив «радіоелектронне придушення», «ПІКО1 » – пристрій імітозахисту контрольованих об'єктів з підвищеною скритністю сигналів-переносників, «ПІКО2» – пристрій імітозахисту контрольованих об'єктів із затримкою відповіді за часом.

Таблиця 4.5

Рівні забезпечення прихованості та рівні деструктивного впливу для розроблених моделі процесу забезпечення потайного інформаційного обміну та пристроїв на її основі

ДВ	Р-рівень забезпечення прихованості		At- рівень деструктивного впливу	
	ПІКО1	ПІКО2	ПІКО1	ПІКО2
ДВ1	2	2	4	4
ДВ2	3	2	4	4
ДВ3	2	2	4	4
ДВ4	2	2	4	4

Спочатку проводяться обчислення за допомогою виразу (2.1). Далі на основі таблиці 4.5 та виразів (2.5) – (2.6) обчислюються узагальнені показники рівня забезпечення прихованості та рівня деструктивної дії, які

рівні P_0=2+3+2+2=9, At_0=4+4+4+4=16 і P_0=2+2+2+2=8, At_0=4+4+4+4=16 відповідно.

При цьому нормуючий коефіцієнт k(m), який береться при максимальних значеннях A_t і P (оскільки кожній нечіткій змінній відповідає позитивне ціле число в діапазоні [1…5], максимальним числом є 5). Звідси P_0=5+5+5+5=20 та At_0=5+5+5+5=20, і відповідно до виразу (2.7), k(m)=0,0025. Остаточні розрахунки оцінки прихованості проводяться за допомогою виразу (2.8): $P_{прихср}$ =1- 0,0025 9 16=0,64 та $P_{прихср}$ =1-0,0025 8 16=0,68

Отримані оцінки прихованості наведено у табл.. 4.6. У таблиці 4.6 введено такі позначення: «ПІКО1» – пристрій імітозахисту контрольованих об'єктів з підвищеною прихованістю сигналів-переносників, «ПІКО2» – пристрій імітозахисту контрольованих об'єктів із затримкою відповіді за часом.

Таблиця 4.6

Оцінки прихованості розробленої моделі процесу забезпечення потайного інформаційного обміну та пристроїв на її основі

№	Назва		
		Кількісна оцінка	Якісна оцінка
1	ПІКО1	0,640	В
2	ПІКО2	0,680	В

Розрахунки, наведені в таблиці 4.6 показали, що розроблена модель процесу забезпечення потайного інформаційного обміну та пристрої, побудовані на її основі, мають високий рівень прихованості від деструктивних впливів, рівний Рскрср=0,64 і Рскрср=0,68.

Отже, за допомогою розроблених моделей процесу забезпечення потайного інформаційного обміну, алгоритму її реалізації та пристроїв, побудованих на їх основі, вдалося досягти рівня прихованості $P_{прихср}$=0,64 і

$P_{прихср}$=0,68. Отримані значення рівня прихованості входять до умовного інтервалу значень рівнів прихованості.

4.4 Висновки за розділом

Запропонована практична реалізація обчислювального методу оцінки прихованості інформаційного обміну для бездротових систем передачі даних на основі нечіткої логіки та програмна реалізація розробленої моделі процесу забезпечення потайного інформаційного обміну та алгоритму її реалізації.

Встановлено, що за допомогою запропонованої моделі можливо отримати сигнали, що передаються, й мають шумоподібний вигляд, з яких візуально важко виділити вихідний інформаційний сигнал. Запропонована модель дозволяє отримати сигнали, що передаються, та володіють прийнятним рівнем значення пік-фактору Crest та BDS-статистики, забезпечуючи виконання початкових умов.

Наведено практичні рекомендації щодо використання розробленої моделі процесу забезпечення потайного інформаційного обміну та алгоритму її реалізації для систем охоронно-пожежної сигналізації, що дозволяють їх використовувати для підвищення прихованості інформаційного обміну існуючих та перспективних бездротових систем передачі даних.

Висновки

В ході виконання кваліфікаційної роботи магістра отримано такі результати:

Підтверджено актуальність використання бездротових систем передачі в різних галузях. Показано переваги бездротових систем передачі даних над традиційними системами.

Проведено аналіз деструктивних впливів на інформаційний обмін у бездротових системах передачі даних та методів їх реалізації, в результаті якого встановлено, що основними деструктивними впливами на інформаційний обмін є перехоплення, перегляд, заміна та радіоелектронне придушення, які можуть застосовуватися одночасно.

Здійснено аналіз відомих методів та алгоритмів забезпечення прихованості інформаційного обміну у бездротових системах передачі даних в умовах зазначених деструктивних впливів.

Здійснено вибір критерію оцінювання прихованості та методів його реалізації для оцінки прихованості інформаційного обміну у бездротових системах передачі даних.

Розроблений обчислювальний метод оцінки прихованості на основі нечіткої логіки.

Розроблено модель процесу забезпечення прихованості інформаційного обміну. Її перевагами є облік у своєму складі оператора формування хаотичних сигналів і оператора взаємодії сигналів, що передаються, з навмисними і ненавмисними деструктивними впливами в каналі зв'язку.

Розроблено алгоритм реалізації моделі процесу забезпечення потайного інформаційного обміну, який дозволяє підвищити прихованість від деструктивних впливів переданих керуючих та службових команд за рахунок використання в блоці контролю та контрольованому об'єкті однакових накопичувачів хаотичних послідовностей, а також однакових генераторів ПСП -2, ініціалізація яких здійснюється псевдовипадковим числом, що

періодично змінюється, генератором, що виробляється ПСП-1 блоку контролю.

Розроблено модифікований алгоритм реалізації моделі процесу забезпечення потайного інформаційного обміну, який заснований на алгоритмі забезпечення потайного інформаційного обміну, який дозволяє підвищити прихованість від деструктивних впливів переданих керуючих та службових команд за рахунок використання ускладненої імітаційної вставки для команд, що передаються, заснованої на додаванні за правилом XOR вихідного значення ПСП-1 та контрольованого об'єкта.

Запропонована практична реалізація обчислювального методу оцінки прихованості інформаційного обміну для бездротових систем передачі даних на основі нечіткої логіки та програмна реалізація розробленої моделі процесу забезпечення потайного інформаційного обміну та алгоритму її реалізації.

Встановлено, що за допомогою запропонованої моделі можливо отримати сигнали, що передаються, й мають шумоподібний вигляд, з яких візуально важко виділити вихідний інформаційний сигнал. Запропонована модель дозволяє отримати сигнали, що передаються, та володіють прийнятним рівнем значення пік-фактору Crest та BDS-статистики, забезпечуючи виконання початкових умов.

Наведено практичні рекомендації щодо використання розробленої моделі процесу забезпечення потайного інформаційного обміну та алгоритму її реалізації для систем охоронно-пожежної сигналізації, що дозволяють їх використовувати для підвищення прихованості інформаційного обміну існуючих та перспективних бездротових систем передачі даних.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Системи пожежної та охоронної сигналізації: навч. посіб. / Кушнір А.П., Чалий Д.О. Львів: СПОЛОМ, 2022. - 298 с.

2. Тактико-спеціальна підготовка працівників Національної поліції: навч. посібник / О. І. Тьорло, Ю. Р. Йосипів, В. М. Синенький та ін. Львів: ЛьвДУВС, 2018. - 480 с.

3. Інтелектуальні системи в технічній експлуатації автомобілів: монографія / В. Д. Мигаль. Х.: Майдан, 2018. - 262 с.

4. Верьовкін Л.Л. Світанько М.В., Кісельов Є.М., Хрипко С.Л. Цифрова схемотехніка: Підручник. – Запоріжжя: ЗДІА, 2016. 214.

5. Щур Н.О., Покотило О.А. Основи криптології: навч. посібник. – Житомир: Державний університет «Житомирська політехніка», 2021. - 120 с.

6. Бобало Ю. Я. Інформаційна безпека: навч. посібник / Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник та ін.; за заг. ред. Ю. Я. Бобала. – Львів: Видавництво Львівської політехніки, 2019. – 580 с.

7. Електротронний ресурс. Режим доступу: https://mil.in.ua/uk/d0-bf-d0-be-d0-b3-d0-bb-d1-8f-d0-b4-d0-b8-d0-ba-d0-be-d0-bc-d0-b0-d0-bd-d0-b4-d1-83-d0-b2-d0-b0-d0-bd-d0-bd-d1-8f-d0-bf-d1-81-d1-81-d1-88-d0-b0-d0-bd-d0-b0-d0-bf-d1-96-d0-b4-d0-b2-d0-b8-d1-89/

8. Електротронний ресурс. Режим доступу: https://tvtdigital.com.ua/typy-okhoronnykh-system-drotova-vs-bezdrotova-yakyy-typ-okhoronnoi-systemy-obraty-krashche/

9. Челомбитько В.В. Захист інформації в телекомунікаційних системах: конспект лекцій з дисципліни «Захист інформації в телекомунікаційних системах» для підготовки студентів за спеціальністю 172 «Телекомунікації та радіотехніка» / Челомбитько В.В. – Львів: ЛННЦ ОНАЗ, 2018.– 32 с.

10. Горбенко І. Д. Захист інформації в інформаційно-телекомунікаційних системах: Навч. посіб. для студ. Ч. 1. Криптографічний

захист інформації / І. Д. Горбенко, Т. О. Гріненко. – Х. : Харк. нац. ун-т радіоелектрон., 2004. – 368 с.

11. Burlyai I. V. Systems of Radio Communication and Their Application by the Emergency Rescue Service /I. V. Burlyai, B. B. Orel, O. M. Dzhulai: Guide. Chernihiv: RVK “Desnianska Pravda”, 2007. 288 p.

12. Zakharchenko N. Information security of Time-Controlled Signals in Confidential Communication Systems / N. Zakharchenko, V. Korchinsky, B. Radzimovsky // Modern problems of radio engineering, telecommunications and computer science: XI International Conference TCSET 2012, (Lviv-Slavske, 21-24 february 2012) – Lviv; Publishing House of Lviv Polyteshnic, 2012. C. 317.

13. Lian, S. Multimedia Content Encryption: Techniques and Applications / S. Lian. – CRC: Taylor&Francis, 2009. – 217 p.

14. Kehui, Sun Chaotic Secure Communication: Principles and Technologies / Kehui Sun. Tsinghua University Press and Walter de Gruyter GmbH, 2016. – 333 p.

15. Безвесільна О.М., Подчашинський Ю.О., Тимчик Г.С. Наукові дослідження в галузі вимірювання механічних величин. Інформаційно-комп'ютерні системи та технології: Підручник. -Житомир: ЖДТУ, 2011. – 876 с.

16. Петрик В.М. Інформаційна безпека держави. Том 1 / В.М. Петрик, М.М. Присяжнюк, Д.С. Мельник, В.В. Остроухов та інші. – К: ДПУ «Книжкова палата України», 2016. – 264 с.

17. Fayyad, Piatetsky-Shapiro, Smyth, Uthurusamy. Advances in Knowledge Discovery and Data Mining. – AAAI/MIT Press, 1996. – P. 196.

18. Смірнов Ю. О. Основи радіоелектронної розвідки. Частина 1. Розвідувально-інформаційний процес, основні моделі системи РЕР ефективність і напрями її подальшого розвитку. Київ : НДІ ГУР МО України, 2009. 155 с.

19. Шолохов С.М., Самборський І.І., Вакуленко О.В., Ніколаєнко Б.А.

20. Завадозахист радіоелектронних засобів. Частина 1. Основи завадо захисту систем зв'язку: навчальний посібник. Київ: ІСЗЗІ КПІ ім. Ігоря Сікорського, 2021. 210 с.

21. Denk Aytug. Detection and jamming low probability of intercept (LPI) radars / Aytug Denk. – Monterey, California: Naval Postgraduate School, 2006. – 123 p.

22. Сучасні методи дослідження нелінійних динамічних систем. Посібник для студентів спеціальностей 123 «Комп'ютерна інженерія» та 151 «Автоматизація та комп'ютерно-інтегровані технології»/ О. О. Сердюк. – Краматорськ : ДДМА, 2018. – 120 с.

23. Yongqing, Fu Performance Evaluation of a New Secured Coded Hybrid Spread Spectrum System under Effect of Different Channels Types / Yongqing Fu, Hany A.A. Mansour // Applied Mechanics and Materials. – 2014. – V. 543-547.

24. Borwein, Peter; Mossinghoff, Michael J. (2008). Barker sequences and flat polynomials. У James McKee; Chris Smyth (ред.). Number Theory and Polynomials. LMS Lecture Notes. T. 352. Cambridge University Press. с. 71-88.

25. Kaplan, D. and Glass, L., Understanding Nonlinear Dynamics, Springer, 240–244, (1995).

26. Електротронний ресурс. Режим доступу: https://openarchive.nure.ua/server/api/core/bitstreams/718f62f0-fdc5-40bc-acb6-464e8df86664/content

27. Hordiichuk, V. Method of accuracy increase in radio control systems with orthogonal frequency multiplexising at the consideration of the timer signal constructions use / Hordiichuk V. // Advanced Information Systems. – 2018. – V. 2. – No. 4. – pp. 108-113.

28. Yu, Xinghuo Chaos Control Theory and Applications / Yu Xinghuo, Guanrong Chen. Springer. 2003. – 343 p.

29. Xiangjun, Wu A secure communication scheme based generalized function projective sunchronization of new 5D hyperchaotic system / Xiangjun Wu, Zhengye Fu, Jurgen Kurths // Physica Scipra. – 2015. – No. 90. – 12 p.

30. Vovchuk, D.A. Experimental research of the process of masking of digital information signals using chaotic oscillations / Vovchuk D.A., Politanskii L.F., Haliuk S.D. // Eastern European Scientific Journals. – 2014. – No. 3. – Pp. 245-253.

31. Tilborg, van Henk C.A. Fundamental of cryptology: a professional references and interactive tutorial / Tilborg van Henk C.A. Kluwer academic publishers, 2000 – P 492.

32. Гончарова Л.Л. Комп'ютерні методи організації мікропроцесорних систем контролю і прогнозу залишкового ресурсу енергетичних об'єктів / Гончарова Л.Л. // Збірник наукових праць. «Моделювання та інформаційні технології», Інститут проблем моделювання в енергетиці – 2009.– № 53 – С. 103-108.

ДОДАТКИ

2 DESIGN PART

2.1 Selection of criteria for assessing the secrecy of information exchange in wireless data transmission systems

To assess the effectiveness of methods and algorithms for ensuring secrecy, an assessment is necessary that allows determining the level of secrecy based on quantitative and qualitative assessment. Currently, many different computational methods and models for assessing secrecy are known. In general, they can be divided into large groups: analytical methods and statistical methods.

Analytical methods allow obtaining the characteristics of the system as a function of its operating parameters. Typically, an analytical model is a set of mathematical symbols and relations, during the solution of which the parameters and necessary estimates of the system under study are obtained. Often, such parameters are probabilistic or other characteristics.

Statistical methods are based on computer modeling of models that simulate the behavior of real objects, processes and systems in time, during a given period and are repeated many times for further statistical processing of the obtained data in order to confirm their adequacy.

The combination of analytical and statistical methods is very useful, as it allows not only to effectively study various objects, but also to understand and explain the physical essence of the processes and phenomena occurring in the system under study.

According to the assessment of secrecy, 4 levels are distinguished (S1, S2, S3, S4). The most secret levels S3 and S4 provide for the mandatory use of signal encoding with a certain number of original codes.

The analysis shows that the disadvantages of this assessment method include:

a) the lack of quantitative indicators;

b) the method does not pay attention to specific approaches to destructive effects on the radio channel and specific methods for ensuring the secrecy of the radio channel.

As a result, for example, the use of methods and algorithms for ensuring secret information exchange based on a cryptographic protection method and a noise-like signal with the same number of original code sequences is placed in the same class, although it is well known that methods and algorithms for ensuring secret information exchange based on a noise-like signal provide a higher level of secrecy from complex destructive effects (review, substitution, interception, electronic suppression), while methods and algorithms for ensuring secret information exchange based on a cryptographic protection method are not able to withstand interception and suppression of interference [16].

Based on this, the issue of quantitative assessment of the secrecy of information exchange in wireless data transmission systems is important, which is based on the analyzed methods and algorithms for ensuring secret information exchange. Currently, one of the most famous quantitative models for assessing the secrecy of wireless data transmission systems is the probabilistic assessment of secrecy [17]. Secrecy is understood as the ability of a communication system to resist detection by the enemy of its working state using radio reconnaissance. As is known [18], radio reconnaissance of communication systems consists of the following steps: signal detection, determination of the signal structure and disclosure of the transmitted information. The listed tasks of radio reconnaissance can be contrasted with three types of signal secrecy: energy, structural and information.

Energy secrecy characterizes the ability to resist measures aimed at detecting a signal by reconnaissance receiving devices, and structural secrecy is the degree of complexity of determining the signal structure. Information secrecy is determined by the stability of the cryptographic key. A quantitative measure of energy secrecy is the possibility of correct detection Pdetect. A quantitative measure of structural secrecy is the possibility of revealing the structure of the

signal Pstr, provided that the signal is detected. A quantitative measure of information secrecy is the possibility of revealing the content of the transmitted information Pinfo, provided that the signal is detected and its structure is revealed.

Therefore, the probability of reconnaissance Pp is determined by the following expression:

$$Pp = Pвияв * Pстр * Pінф. \quad (2.1)$$

Often the task of assessing information secrecy is not set, since the detection of the transmitted signal and the determination of its structure will allow the attacker to put up an obstacle from which information secrecy does not protect. Therefore, an effective solution to the problem of ensuring the secrecy of transmitted data in communication systems, including when the decryption key is compromised, should lie in the field of ensuring high energy and structural secrecy of transmitted signals. Hence, expression (2.1) is transformed into the following form:

$$Pp = Pвияв * Pстр. \quad (2.2)$$

Based on expression (2.2), the overall latency estimate Pprhy is calculated:

$$Pприх = 1 - Pp = 1-Pвияв * Pстр. \quad (2.3)$$

For estimating the concealment described by expression (2.3), it is important to note that different mathematical expressions are proposed for calculating the energy Pcover and structural Pcover. For example, for estimating the structural concealment for known noise-like signals:

$$P_{стршпс} = P\,|\,\varepsilon\,| < \varepsilon_0 = \Phi(\frac{3\varepsilon_0}{2})qFT(1-\rho^2)), \quad (2.4)$$

where Φ(z) is the probability integral, ε0 is the confidence interval limit, ρ is the time-frequency coupling coefficient.

To estimate the structural secrecy for chaotic signals:

$$P_{cmpxc} = P\,|\,\varepsilon\,| < \varepsilon_0 = \Phi(\frac{3\varepsilon_0}{2}\frac{1}{\sigma_\lambda}). \quad (2.5)$$

The potential structural latent factor Sp can be calculated using the following expression:

$$S_p = \log_2 A, \quad (2.6)$$

where A is an ensemble of implementations, which is determined by the number of all possible values of any parameters.

2.2 A comprehensive approach to assessing the secrecy of information exchange in wireless transmission systems

A comprehensive approach is required to assess secrecy - the operating conditions of radio engineering systems must be assessed taking into account both the technical capabilities of intelligence and the technical capabilities of the radio engineering systems themselves, but this is a rather laborious process due to the need to calculate the secrecy assessment in different conditions, including under conditions of complex destructive influences for radio engineering systems for various purposes.

When assessing the probability of secrecy, the assessment of information secrecy is usually not taken into account, which distorts the overall assessment of secrecy.

As a promising direction for the development of computational methods and models for assessing secrecy, the fuzzy logic apparatus is currently highlighted, which, in conditions of incompleteness and weak structure of the initial data, allows obtaining both a quantitative assessment of secrecy and a qualitative one.

Definition of the formula for the importance of a confidentiality violation incident:

$$Ilm = k(m)\ At\ P. \quad (2.7)$$

Definition of the formula for the numerical assessment of the confidentiality of transmission systems in a local area network (LAN):

$$Pprsr = 1\text{-}Ilm. \quad (2.8)$$

Calculation of the assessment of the confidentiality of data transmission systems in a LAN:

$$Pprsr = 1\text{-}k(m)\ AtiAsi\ Plmi\ Ti, \quad (2.9)$$

where k(m) is a normalizing coefficient that allows us to represent the obtained result in the range [0,1]; Ati is the level of destructive impact on the i-th local computing network; Asi is the criticality of the assets of the i-th local computing network; Plmi is the level of ensuring the confidentiality of the i-th local network; Ti is the level of trust of the i-th local network device.

Therefore, according to this computational method, the secrecy is calculated using expression (2.9), which allows, in conditions of incompleteness and weak structure of the initial data, to calculate an estimate of the secrecy of information exchange in wireless data transmission systems.

Therefore, knowing the numerical values, it is possible to obtain a numerical (quantitative) assessment of the secrecy of information exchange in wireless data transmission systems from destructive influences in general [19]:

$$Ppryk = 1\text{-}Ipryk. \quad (2.10)$$

To calculate the assessment of the secrecy of information exchange in wireless transmission systems from destructive influences:

$$Ppryk=1-k(m)\ At\ P. \quad (2.11)$$

Expression (2.11) does not take into account the variety of destructive influences, therefore, for a more accurate determination of the quantitative and qualitative assessment of the secrecy of information exchange, it is proposed to take into account the main destructive influences for the radio channel of wireless data transmission systems and all methods of ensuring secrecy from them. Next, each method should be assigned a numerical value and summed up, which are generalized indicators of the level of ensuring the secrecy of PO and the level of destructive influence AtO:

$$AtO= \Sigma Ati, \quad (2.12)$$

Expression (2.12) allows us to obtain the normalization coefficient k(m) (2.13), while PO and AtO are calculated at maximum values:

$$k(m)=1/AtO\ Pc. \quad (2.13)$$

2.3 Conclusions on the section

The developed computational method for assessing secrecy based on fuzzy logic includes the following stages:

1) setting the secrecy of wireless data transmission systems;

2) converting the fuzzy values of the variables “very low”, “low”, “medium”, “high”, “very high” into numerical values;

3) determining the formula for the importance of a secrecy violation incident, which is described by expression (2.7);

4) determination of the formula for numerical assessment of the secrecy of information exchange in wireless data transmission systems from destructive influences in general, which is described by the expression (2.10);

5) calculation of generalized indicators of the level of destructive influence and the level of ensuring secrecy;

6) calculation of the normalization coefficient, which is described by the expression (2.13);

7) calculation of the assessment of the secrecy of information exchange in wireless data transmission systems, which is described by the expression (2.9);

8) conversion of the quantitative assessment into a qualitative assessment using the tabular method.

Міністерство освіти і науки України
Національний університет «Полтавська політехніка імені Юрія Кондратюка»

Кафедра автоматики, електроніки та телекомунікацій

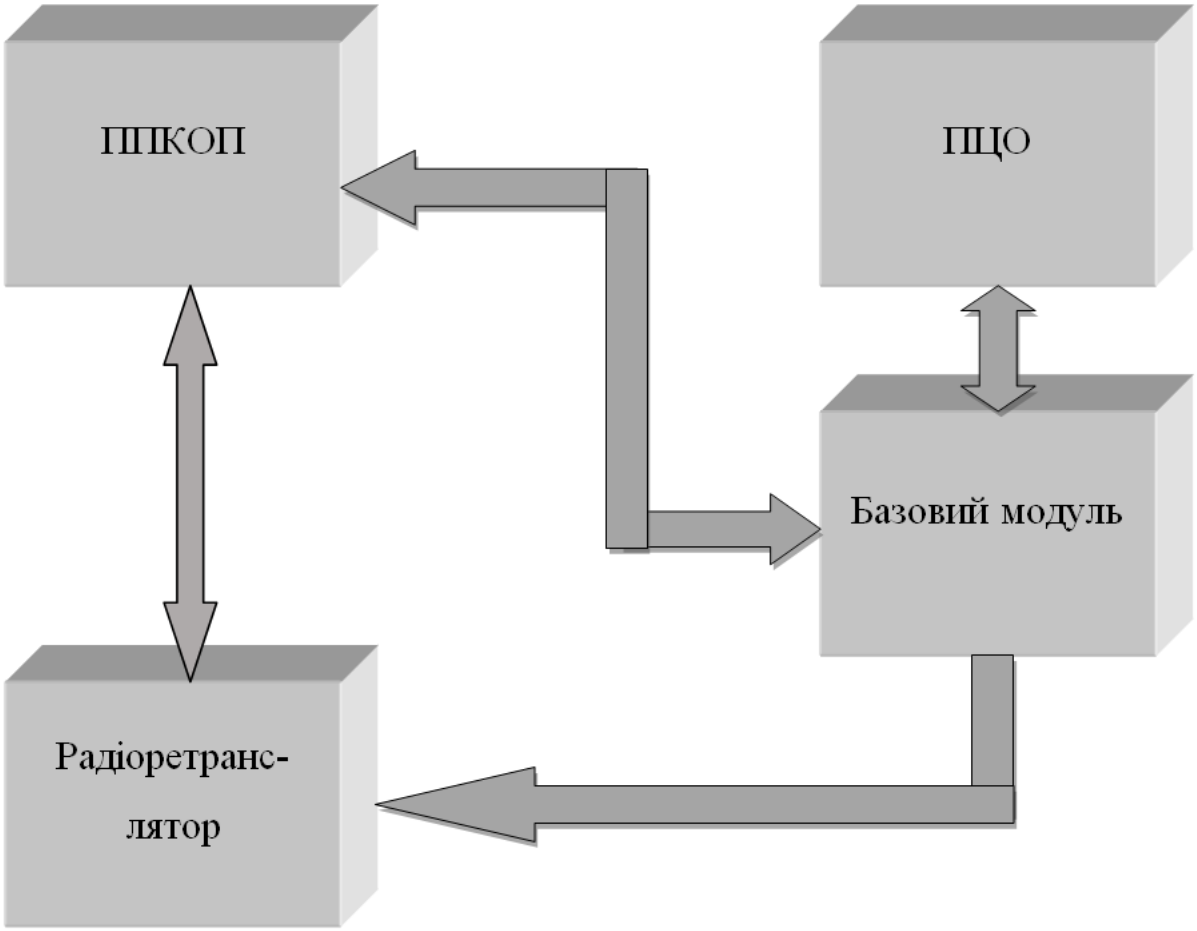
Розроблення алгоритму прихованого інформаційного обміну для бездротових систем передачі даних

Кваліфікаційна робота магістра

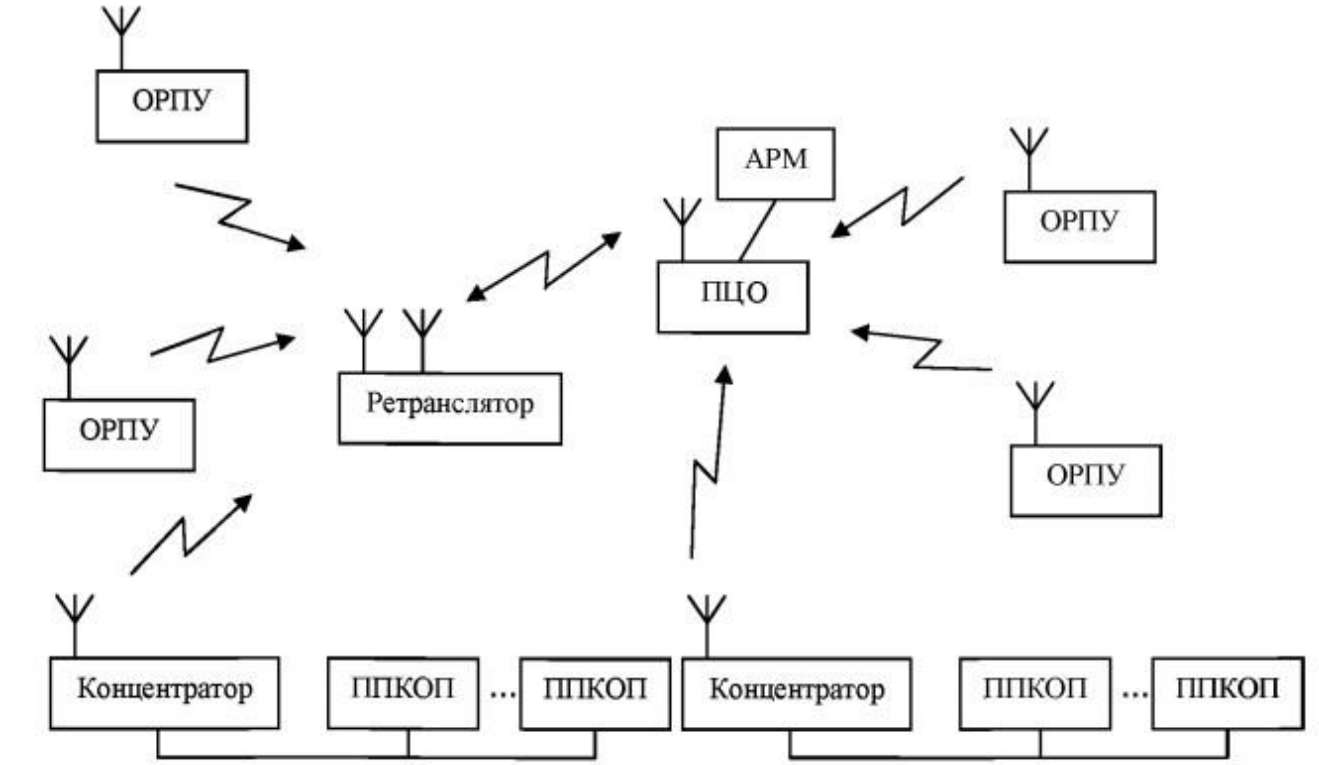
Виконав: **Є. Д. Гладкий**

Керівник:
к.т.н. **О.С. ФОМІН**

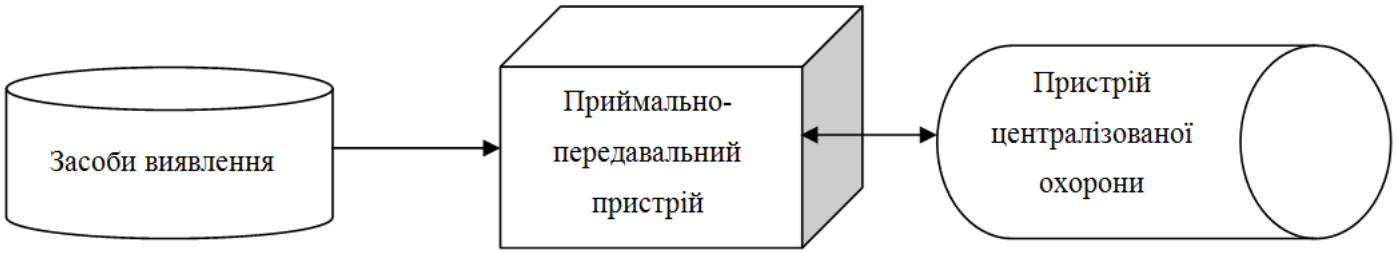
Полтава 2025



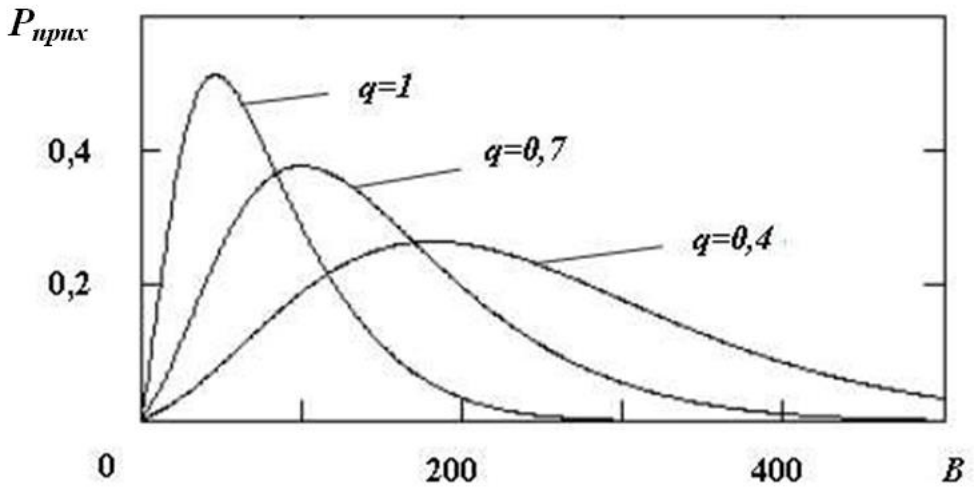
Спрощена структурна схема
системи зв’язку



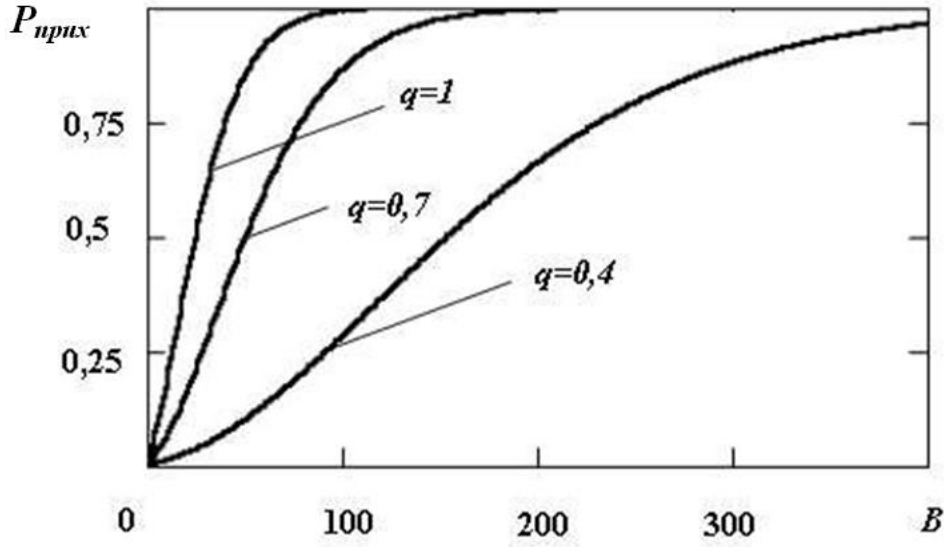
Структурна схема системи зв’язку з однократною ретрансляцією



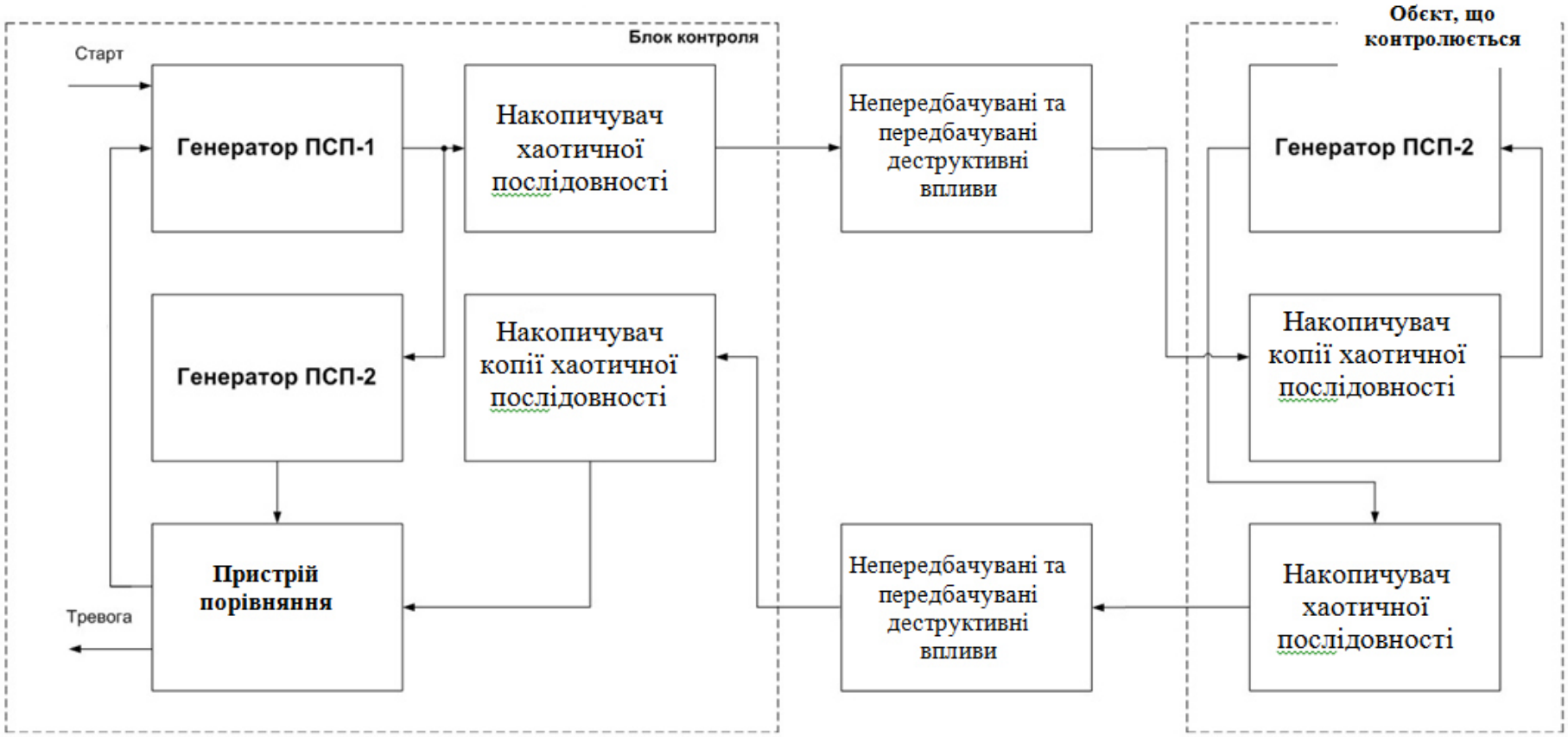
Спрощена структурна схема системи зв’язку



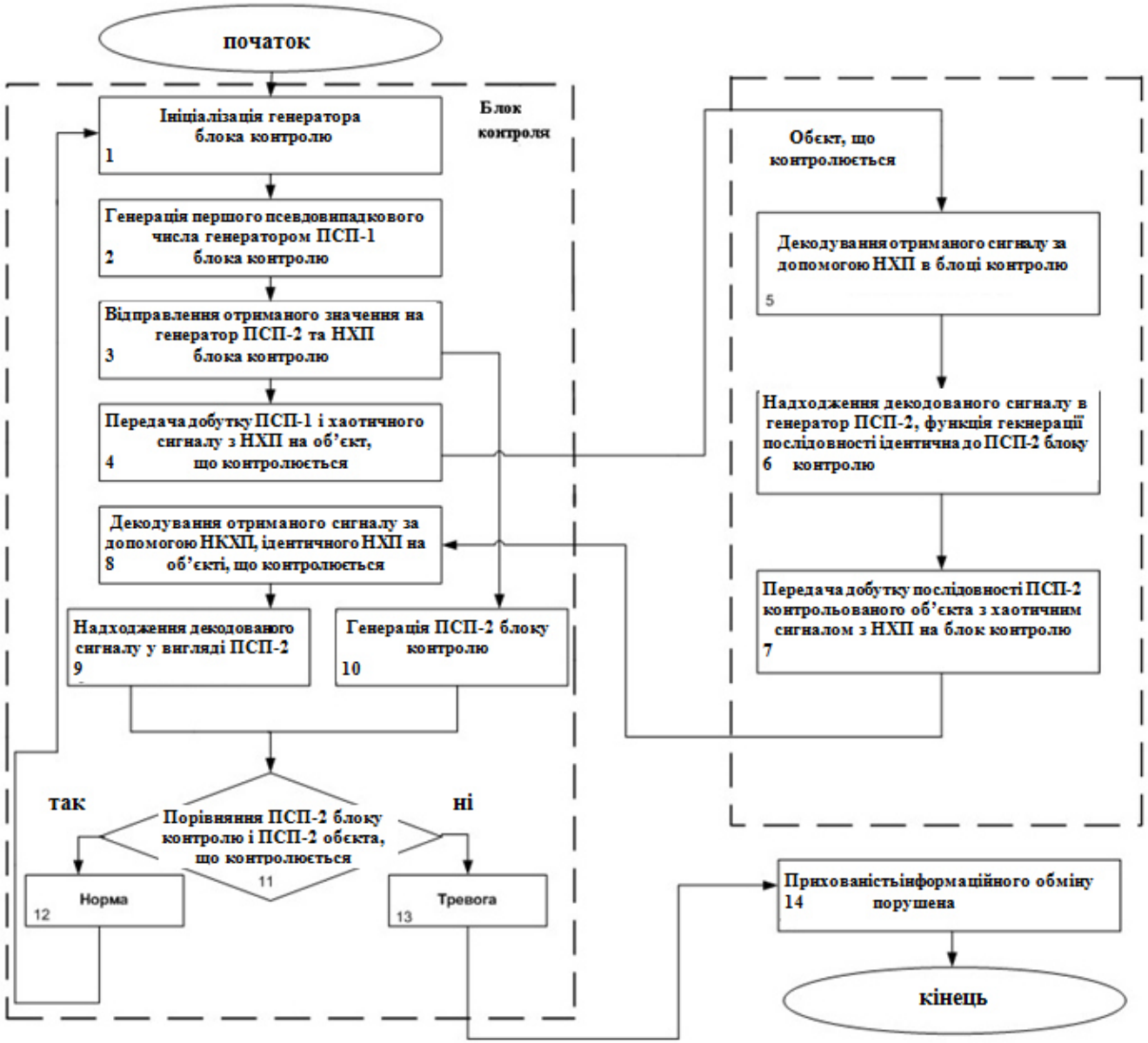
Залежність прихованості $P_{прих}$ від бази сигналу B за різного відношення сигнал/шум q для систем зв'язку на основі шумоподібного сигналу



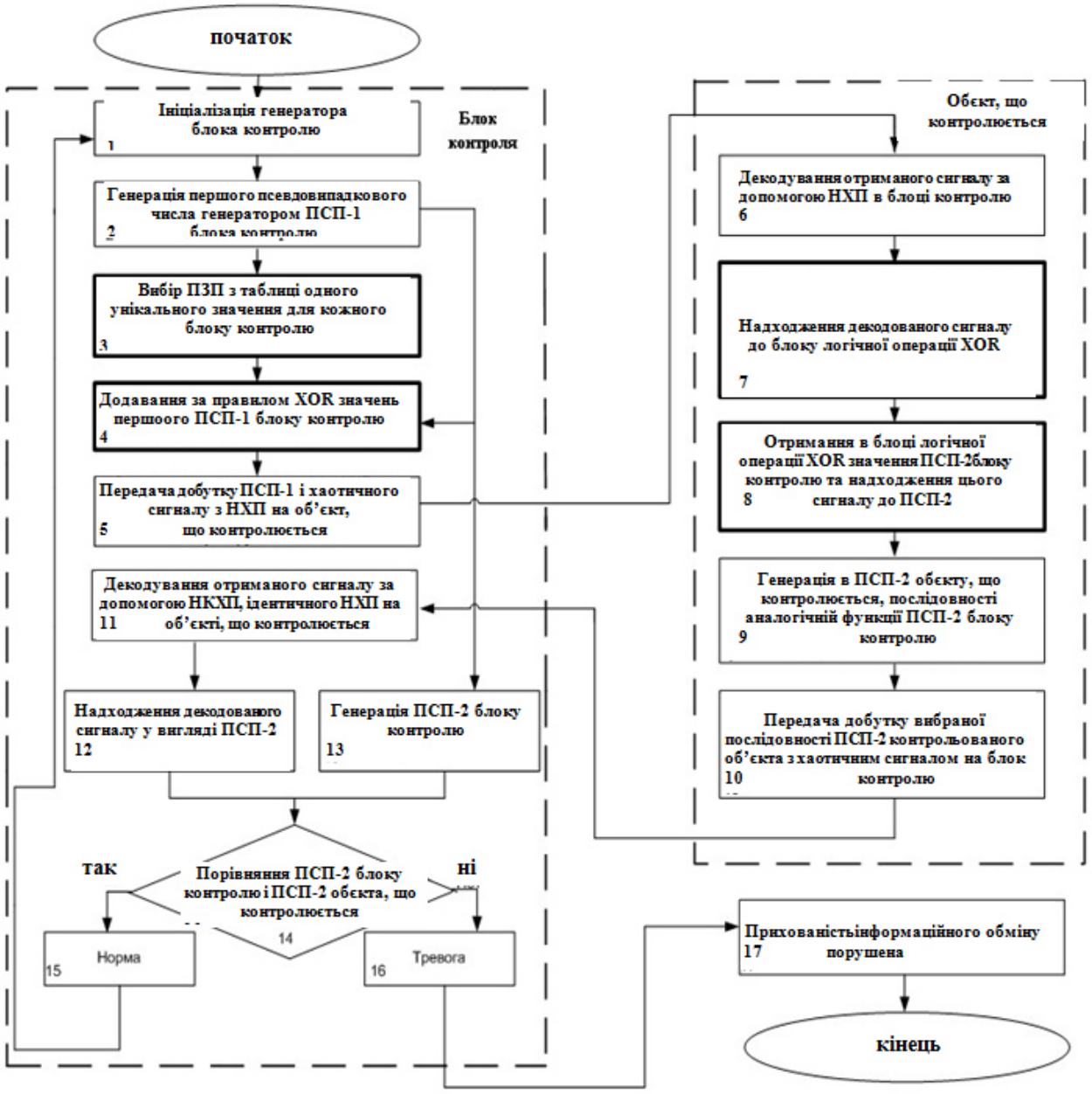
Залежність прихованості $P_{прих}$ від бази сигналу B за різного відношення сигнал/шум q для систем зв'язку на основі хаотичного сигналу



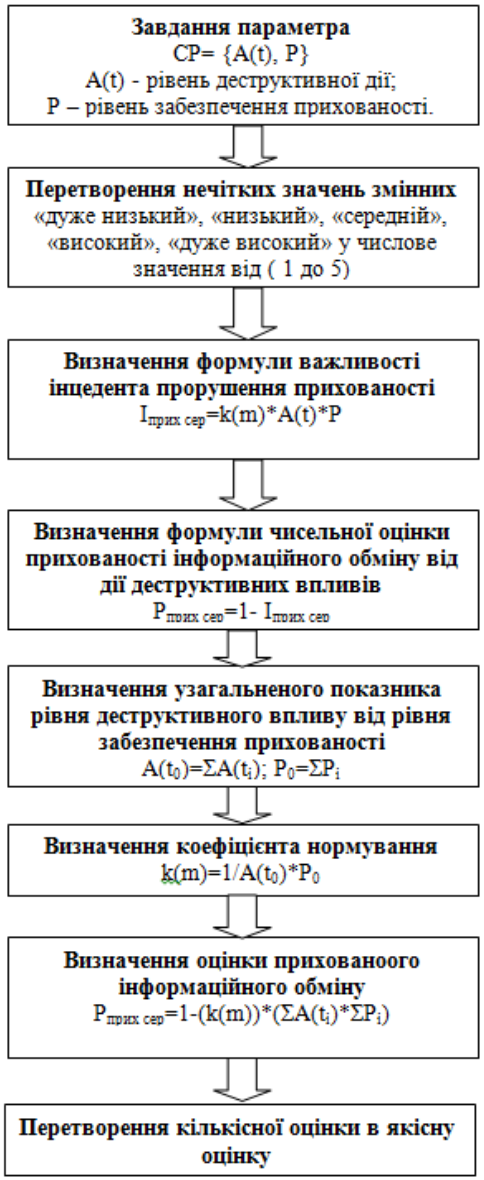
Узагальнена схема розробленого підходу забезпечення прихованості інформаційного обміну в бездротових системах передачі на основі застосування хаотичних сигналів

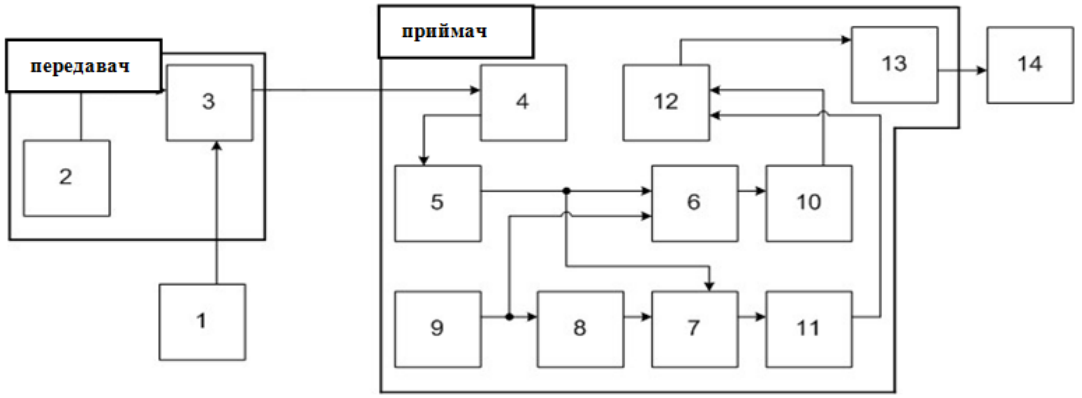


Розроблений алгоритм реалізації моделі процесу забезпечення прихованого інформаційного обміну



Розроблений модифікований алгоритм реалізації моделі процесу забезпечення потайного інформаційного обміну з ускладненою імітаційною вставкою

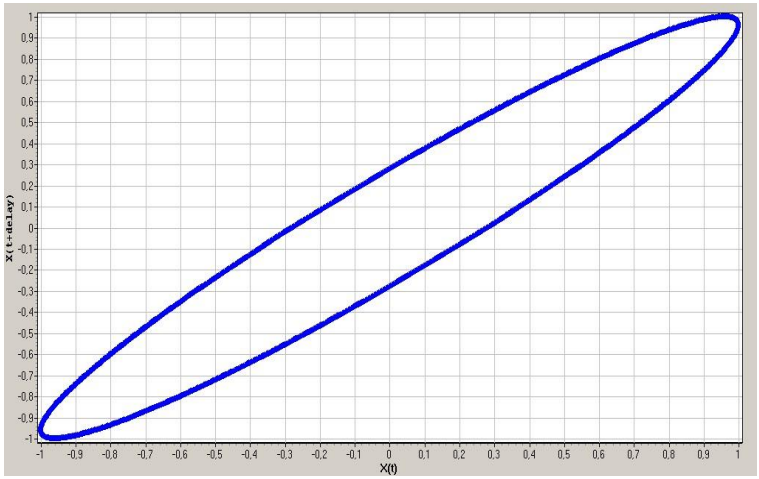


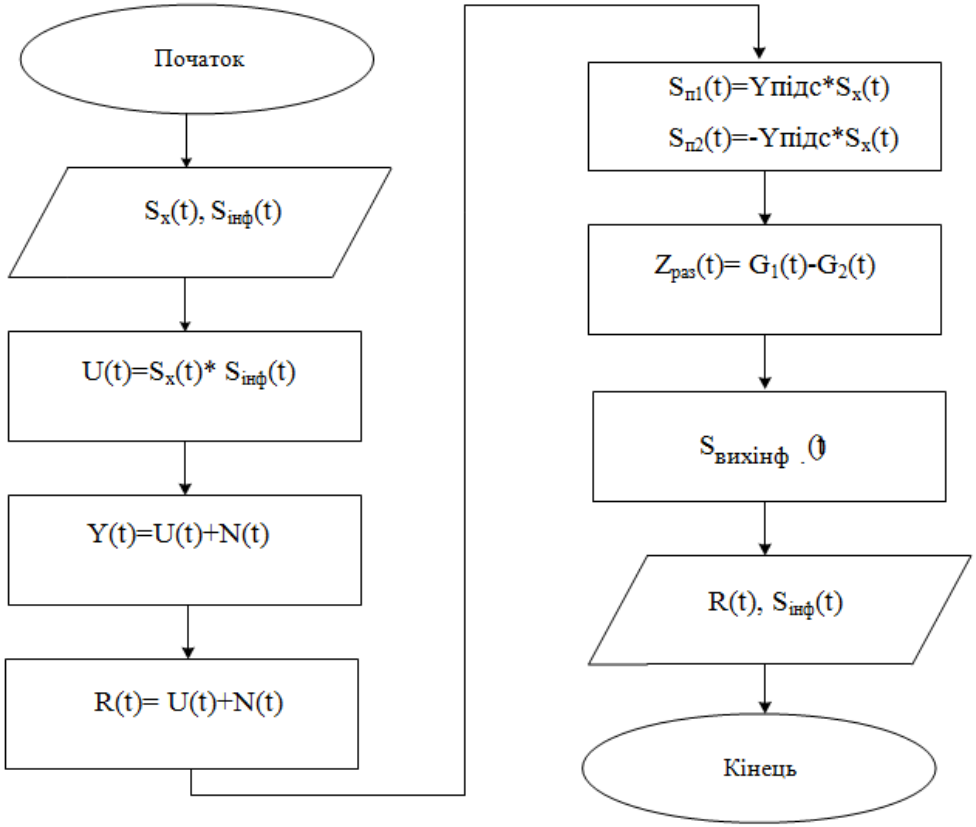


Графоаналітичне представлення програмної реалізації запропонованої моделі процесу забезпечення прихованого інформаційного обміну

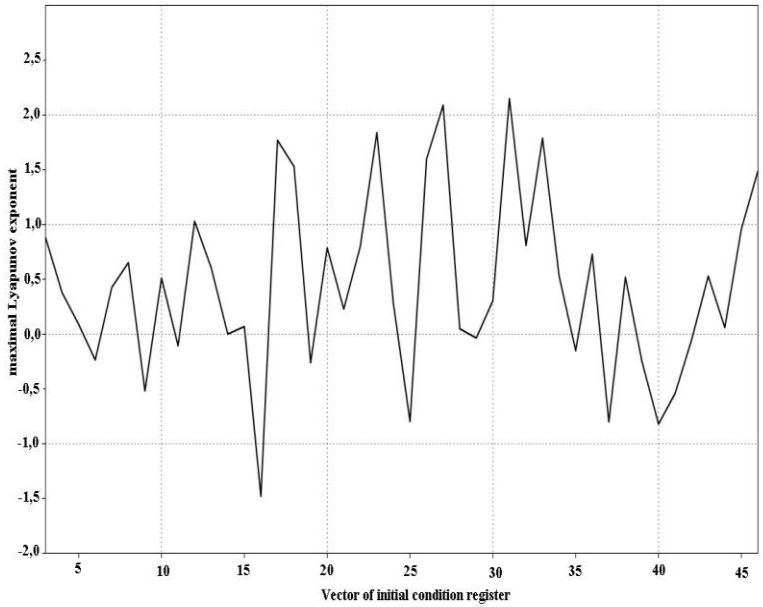
Графоаналітичне представлення програмної реалізації розробленого обчислювального методу оцінки прихованості

Фазовий портрет сигналу, що передається у каналі зв'язку



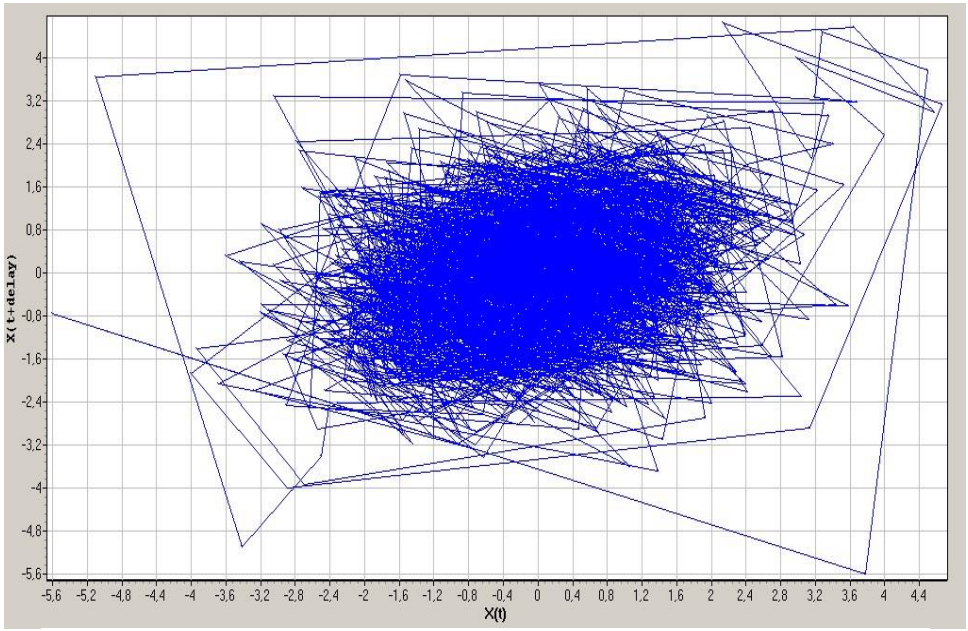


Спрощений алгоритм роботи системи

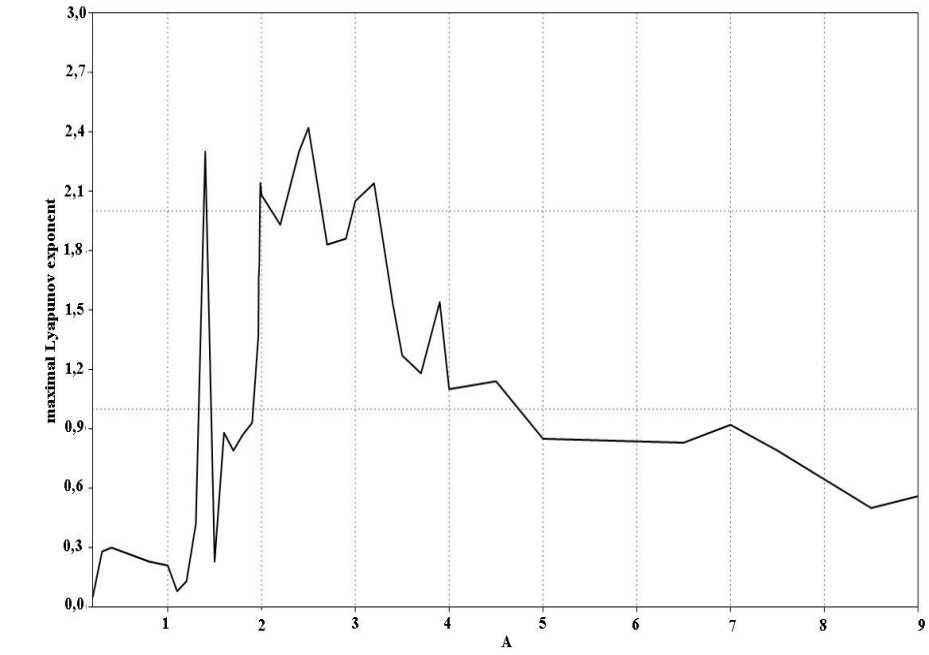


Значення максимального показника Ляпунова сигналів зв’язку, що передаються, з прямим розширенням спектра з допомогою m-послідовностей

Графоаналітична послідовність розробленого алгоритму, що реалізує модель системи зв'язку із простими сигналами

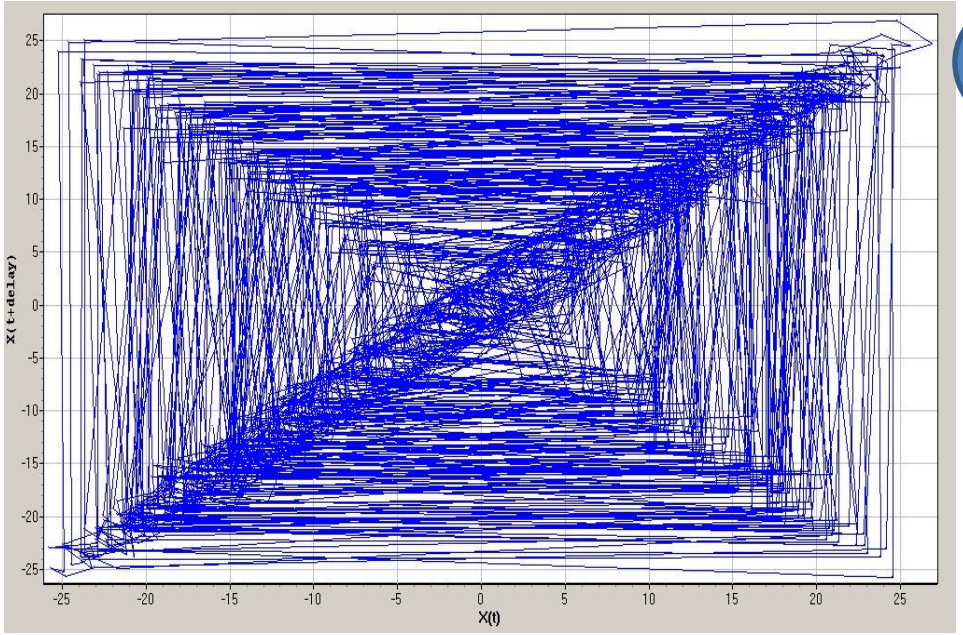


Фазовий портрет сигналу, що передається в каналі зв’язку з осцилятором Ван дер Поля

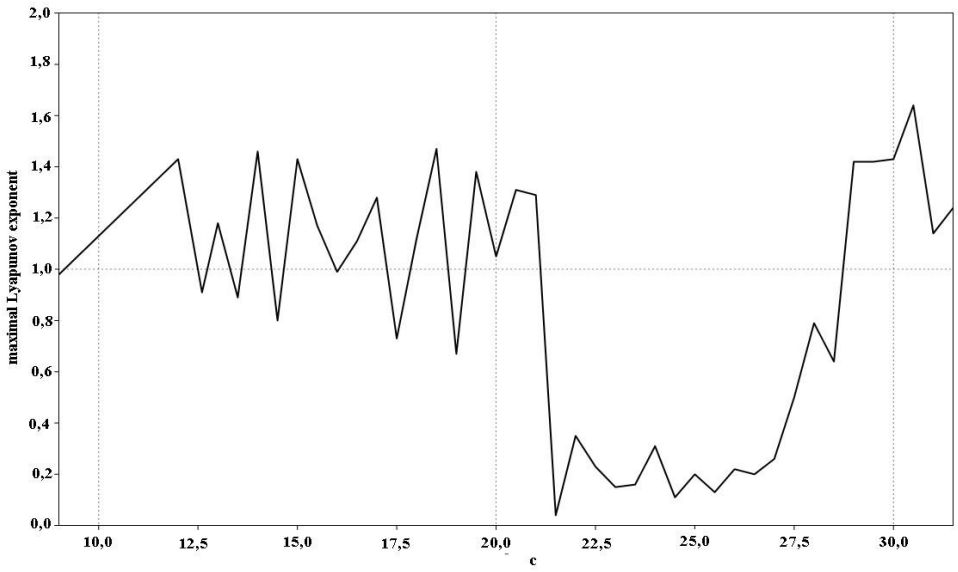


Значення максимального показника Ляпунова сигналів, що передаються в каналі зв'язку з осцилятором Ван дер Поля

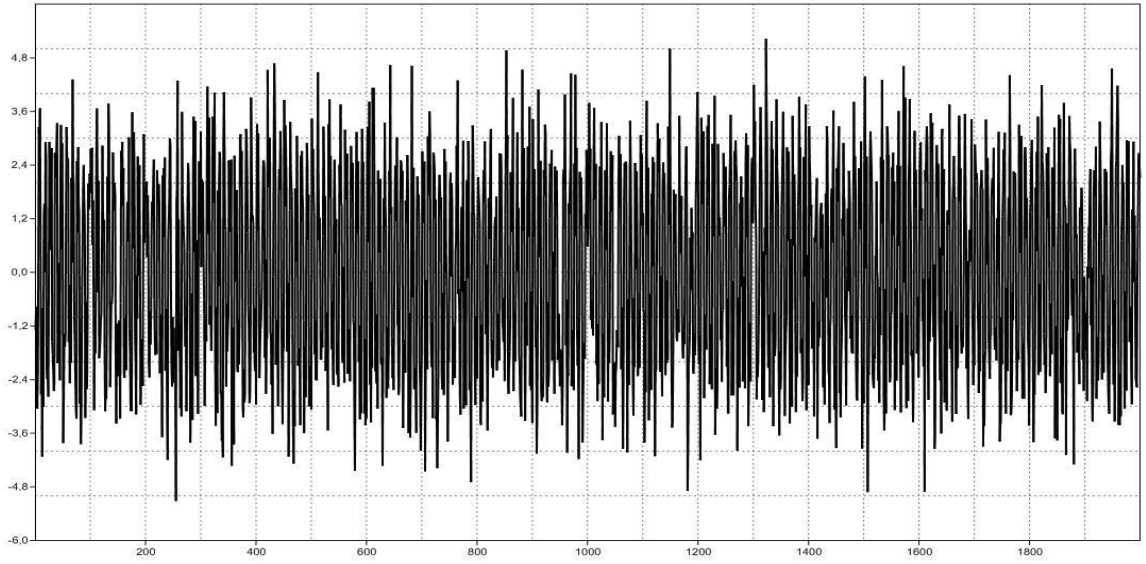
Фазовий портрет сигналу, що передається у каналі зв'язку з атрактором Ресслера



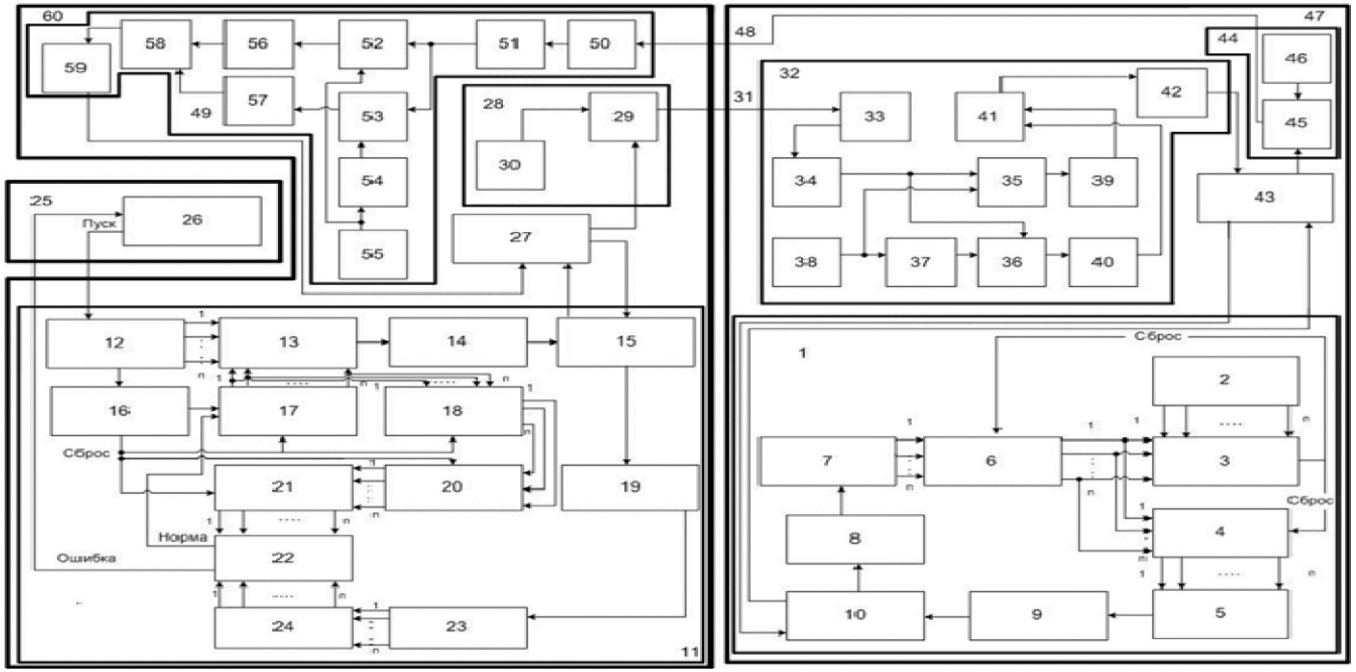
Значення максимального показника Ляпунова для даного спектру сигналів з атрактором Ресслера



Графоаналітичне представлення розробленої програми, що реалізує модель системи зв'язку на основі прямого розширення спектра



Часова діаграма переданого сигналу в каналі звязку з прямим розширенням спектра



Пристрій має такі позначення: 1 – датчик, 2 – блок пам'яті стартової послідовності, 3 – блок порівняння, 4 – генератор ПСП-2, 5 – блок перетворення n-розрядної паралельної комбінації на послідовну, 6 – блок пам'яті, 7 – блок перетворення послідовної комбінації в n-розрядну паралельну, 8 - демодулятор, 9 - модулятор, 10 - узгоджувальний пристрій, 11 - блок обробки інформації, 12 - блок пам'яті стартової послідовності, 13 - блок перетворення n-розрядної паралельної комбінації в послідовну, 14 - модулятор , 15 - узгоджувальний пристрій, 16 - генератор ключа, 17 - генератор ПСП-1, 18 - блок пам'яті контрольного значення, 19 - демодулятор, 20 - генератор ПСП-2, 21 - блок першого пристрою, 22 - блок порівняння, 23 - блок перетворення послідовної комбінації в nрозрядну паралельну, 24 - блок другого пристрою, 25 - блок прийому інформації, 26 - блок управління, 27 - блоку вибору сигналів, 28 - блок передавача, 29 - модулятор-передавач, 30 - накопичувач хаотичного сигналу, 3 – лінія зв'язку, 32 – блок приймача, 33 – смуговий фільтр, 34 – підсилювач, 35 – перший помножувач, 36 – другий помножувач, 37 – інвертор, 38 – накопичувач копії хаотичного сигналу, 39 – перший інтегратор, 40 – другий інтегратор, 41 - пристрій, що вичитує, 42 - вирішальний пристрій, 43 -блок вибору сигналів, 44 - блок передавача, 45 - модулятор-передавач, 46 - накопичувач хаотичного сигналу, 47 - блок 47 передачі інформації, 48 - лінія зв'язку, 49 - блок приймача, 50 – смуговий фільтр, 51 – підсилювач, 52 – перший помножувач, 53 – другий помножувач, 54 – інвертор, 55 – накопичувач копії хаотичного сигналу, 56 – перший інтегратор, другий 57 – інтегратор, 58 – вичитувальний пристрій, 59 – вирішальний пристрій, 60 - транслятор.

ДЯКУЮ ЗА УВАГУ!