Міністерство освіти і науки, молоді та спорту України

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

ШЕРНІН МИХАЙЛО ОЛЕКСАНДРОВИЧ

УДК 621.391

МЕТОДИ ФОРМУВАННЯ ЧИСЛОВИХ ВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ З ВИКОРИСТАННЯМ ІМОВІРНІСНИХ ХАРАКТЕРИСТИК МЕТЕОРНОГО РАДІОКАНАЛУ

05.12.17 - радіотехнічні та телевізійні системи

Автореферат дисертації на здобуття наукового ступеня кандидата технічних наук

Харків - 2012

Дисертація є рукопис.

Робота виконана у Харківському національному університеті радіоелектроніки Міністерства освіти і науки, молоді та спорту України.

Науковий керівник: доктор технічних наук, професор
Антіпов Іван Євгенійович,
Харківський національний університет
Радіоелектроніки, Міністерство освіти і науки, молоді та спорту України,
завідувач кафедри Радіоелектронних пристроїв;

Офіційні опоненти: доктор технічних наук, професор
Величко Анатолій Федорович,
завідувач відділу обробки радіосигналів Інституту радіофізики та електроніки ім. О.Я.Усикова НАН України;

доктор технічних наук, професор
Кузнєцов Олександр Олександрович,
начальник кафедри бойового застосування та експлуатації АСУ Харківського університету Повітряних Сил ім. Івана Кожедуба,
Міністерство оборони України.

Захист відбудеться «20» червня 2012 р. о 15^{00} годині на засіданні спеціалізованої вченої ради Д 64.052.03 у Харківському національному університеті радіоелектроніки за адресою: 61166, м. Харків, просп. Леніна, 14.

З дисертацією можна ознайомитися в бібліотеці Харківського національного університету радіоелектроніки за адресою: 61166, м. Харків, просп. Леніна, 14.

Автореферат розісланий «18» травня 2012 р.

Вчений секретар
спеціалізованої вченої ради В.М. Безрук

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність дослідження. Завдання формування числових випадкових послідовностей (ЧВП) прямо пов'язано з питаннями криптографічного захисту інформації.

Формування й поширення ключів шифрування/дешифрування для реалізації криптографічних алгоритмів є однією з актуальних проблем сучасної науки й техніки. Незалежно сформовані в різних кореспондентів ЧВП, які і є ключами, можуть бути або однаковими, але псевдовипадковими; або дійсно випадковими, але неоднаковими. На сьогодні захист інформації при її передачі по каналах зв'язку, як правило, здійснюється методами криптографії, заснованими на використанні псевдовипадкових послідовностей і секретних ключів шифрування/дешифрування.

Однак сучасними методами криптоаналізу такий захист принципово розкриваємий - це лише питання витрачених засобів і часу.

Гарантований захист інформації може забезпечити тільки постійна зміна ключів, але тоді виникає питання про спосіб їхньої доставки (поширення), що забезпечував би їхню схоронність. На сьогоднішній день не існує способів, яким можна довіряти передачу ключів шифрування на великі відстані.

Можна відзначити лише два способи канального захисту інформації, які теоретично забезпечують достатній захист для поширення ключів. По-перше, це квантова криптографія, заснована на принципі невизначеності Гейзенберга. Вона заснована на тому, що факт перехоплення інформації в оптичному каналі передачі може бути виявлений (але не відвернений). По-друге, метеорна криптографія, заснована на випадкових характеристиках метеорного радіоканалу (МРК), у дослідження властивості якого величезний внесок внесли Б. Л. Кащєєв, Ю. О. Коваль. Відомий до сьогодні метод формування двох однакових ЧВП у двох рознесених пунктах, що запропонований А. В. Карповим і В. В. Сідоровим, вимагає для своєї реалізації крім апаратури метеорного зв'язку, двох високостабільних еталонів часу зі зведеними шкалами. Це робить його надзвичайно складним і дорогим у використанні.

Таким чином, існує **актуальне наукове завдання** – теоретично обґрунтувати й розробити інноваційні методи формування однакових ЧВП у двох рознесених пунктах, причому так, щоб ця ЧВП була недоступна для сторонніх.

Зв'язок роботи з науковими програмами й темами.

Дисертаційні дослідження пов'язані з держбюджетною НДР № 239 (ДР 0109U001635) «Розробка принципів побудови вітчизняного комплексу інформаційно-вимірювальних систем для прогнозування й аналізу наслідків надзвичайних ситуацій», а саме, з 5-м розділом «Розробка альтернативних методів синхронізації, передачі й захисту інформації для використання в Державній інформаційній системі надзвичайних ситуацій», у якому був проведений аналіз випадкових характеристик МРК, розроблено, представлено модель для їхнього аналізу й технічні пропозиції щодо захисту інформації з використанням цих характеристик; а також з НДР «БЕЗПЕКА-5М» «Розробка концепції побудови захищених спеціальних цифрових систем передачі інформації», у першому розділі якої здобувачем були описані теоретичні й практичні можливості формування числових послідовностей, засновані на використанні випадкових характеристик МРК із метою їхньої подальшої інтеграції в спеціа-

льні цифрові системи передачі інформації. У зазначених роботах здобувач був виконавцем.

Мета та задачі дослідження, полягають у вдосконаленні існуючих систем захисту інформації заснованих на розробці методів формування числових випадкових послідовностей, що використовують унікальні характеристики метеорного радіоканалу. Довести їх випадковість, а разом з цим і можливість використання їх як ключів шифрування інформації.

Для досягнення поставленої мети в роботі вирішено такі наукові завдання.

1. Теоретично обґрунтовано можливість використання декількох характеристик метеорного сліду, доступних для виміру одночасно із двох рознесених пунктів (тривалість, просторові координати, інтервали між слідами, форма амплітудно-тимчасової характеристики та ін.) для формування в цих пунктах однакових ЧВП.

2. Розроблено нову модель МРК, призначену для аналізу випадкових характеристик метеорних слідів, що використовуються для формування ЧВП.

3. За результатами моделювання встановлено ступінь взаємозв'язку між різними характеристиками того самого метеорного сліду, що дозволяє вирішити питання про спільне використання декількох характеристик одночасно.

4. Експериментально підтверджено можливість формування ЧВП із використанням окремих вимірюваних характеристик метеорного сліду.

Об'єкт дослідження: процес формування ЧВП на основі випадкових характеристик МРК.

Предмет дослідження: методи формування й перевірки якості ЧВП, отримуваних з використанням випадкових характеристик МРК.

Методи дослідження. На етапі вибору характеристик МРК, придатних для формування ЧВП застосовувався *метод аналогій*. Для розрахунків граничних значень випадкових величин, законів їхнього розподілу й можливих похибок використовувався метод *математичного аналізу*, установлення ступеня статистичного взаємозв'язку між різними випадковими характеристиками МРК здійснювався за допомогою *імітаційного моделювання*, перевірка отриманих у ході *експериментальних досліджень* випадкових послідовностей на предмет наявності в них схованих закономірностей вироблялася методом *статистичного аналізу.*

Наукова новизна отриманих результатів.

1. Вперше показана можливість формування числових випадкових послідовностей із використанням таких характеристик метеорного сліду як тривалість, координати, інтервал між слідами, форма АЧХ. Відрізняється від попередньо запропонованого А. В. Карповим і В. В. Сідоровим способу формування випадкових числових послідовностей, вимірюючи час розповсюдження сигналу по метеорному радіоканалу тим, що були виміряні значення інших характеристик МРК, для вимірювання яких не потрібні високоточні еталони часу, що суттєво спрощує практичну реалізацію.

2. Вперше розроблено модель метеорного радіоканалу, призначену для оцінки його статистичних характеристик і аналізу наявності взаємозв'язку між ними. Відрізняється від існуючих моделей МРК тим, що отримана можливість тестування індивідуальних характеристик кожного окремого метеорного сліду.

3. Вперше запропонована можливість використання декількох характеристик метеорного сліду одночасно для формування однакових секретних ключів у рознесених до 2000 км. пунктах зв'язку. Відрізняється від попередніх тим, що зменшується час формування послідовностей та тим, що однакові ключі формуються безпосередньо в пунктах зв'язку одночасно .

Практичне значення отриманих результатів.

1. Суттєво зменшено витрати на практичну реалізацію використання імовірнісних характеристик метеорного зв'язку.

2. Отримано чисельні оцінки продуктивності методу на рівні 15 біт на слід за кожною з характеристик.

3. Скорочено час формування числових послідовностей. На підставі модельних розрахунків виділено характеристики метеорного сліду, між якими відсутній взаємозв'язок, що дозволяє використовувати їх спільно. Показано відсутність кореляції між ЧВП, які сформовані з використанням координат метеорного сліду й інтервалів між слідами. Що підвищує продуктивність методу у рази.

4. Підвищення безпеки, що засноване на методиці поліпшення якості ЧВП, які сформовані з використанням інтервалів між метеорними слідами.

5. Експериментально підтверджено можливість формування ЧВП на основі інтервалів між метеорними слідами. Продуктивність дорівнює 128 бітам на годину.

Особистий внесок здобувача. Автор дисертації особисто отримав основні наукові результати, викладені в роботі, розробив алгоритм і програму моделі, обробив експериментальні дані. У роботах, виконаних у співавторстві, авторові належать такі ідеї й пропозиції:

- у [1 і 3]- принцип формування ЧВП на основі координат метеорного сліду, а також спосіб їхнього виміру й оцінка можливої погрішності методу;
- у [2]- структурна схема пристрою для формування ЧВП;
- у [4 і 6]- спосіб перевірки ЧВП на наявність схованих закономірностей;
- у [5]- доповнення й зміни, які необхідно внести в модель для розрахунку статистичних характеристик метеорного радіоканалу для трас будь-якої довжини, а також програмна реалізація моделі;
- у [7]- спосіб поліпшення характеристик випадкової послідовності, а також алгоритм і програма обробки результатів експериментальних спостережень.

Апробація результатів роботи. Результати роботи доповідалися й обговорювалися на XIII і XV Форумах «Молодь і електроніка в XXI столітті», 30 березня – 1 квітня 2009 р. і 18 – 20 квітня 2011 р., (Харківський національний університет радіоелектроніки, м. Харків), на X-й Міжнародній конференції TCSET'2010, 23 – 27 лютого 2010 р. (університет «Львівська політехніка», Львів); на конференції «Захист інформації в інформаційно-комунікаційних системах» 24 – 26 травня 2010 р. (Національний авіаційний університет, Київ).

Публікації. За темою дисертації опубліковано 8 наукових праць, у тому числі 3 статті у фахових виданнях, що входять у перелік ВАК України, 1 патент на корисну модель, 4 тези доповідей на наукових конференціях.

Структура й обсяг дисертації. Дисертація складається із вступу, чотирьох розділів, висновків, списку літератури з 38 найменувань і 5 додатків. Повний обсяг дисертації складає 120 стор., 56 рисунків, 5 таблиць.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** визначено актуальність досліджуваної теми, сформульовано мету й задачу наукового дослідження, зазначено наукову новизну й практичну значущість отриманих результатів.

У **першому розділі** розглядаються відомі способи формування ЧВП, шляхи оцінки їх якості, а також фізичні основи виникнення й технічних прийомів використання метеорного радіоканалу.

Описано, що існують способи формування ЧВП зокрема генератори шуму.

Значна увага приділяється генераторам псевдовипадкових послідовностей, які мають всі зовнішні ознаки випадковості, але насправді випадковими не є, тому що кожне чергове значення такої псевдовипадкової послідовності є функцією попередніх значень. Такі послідовності можна застосовувати для моделювання яких-небудь процесів, але для криптографічного захисту інформації вони непридатні.

Для оцінки якості ЧВП застосовуються різні тести, наявність яких або закономірностей у ЧВП призводить до зниження їхньої якості, тобто, до фактичного їхнього скорочення.

Також розглядаються складності, які виникають при доставці (розподілі) ключів.

При розгляді властивостей МРК відзначається, що він виникає випадковим чином у випадковому місці у результаті вторгнення в атмосферу Землі дрібних космічних часток. Фізика метеорного поширення радіохвиль така, що сигнал, відбитий від метеорного сліду, може бути прийнятий тільки у вузькій смузі поблизу місця розташування кожного з кореспондентів. Ця обставина ускладнює перехоплення інформації, переданої по МРК, а також не дозволяє стороннім вимірювати параметри МРК, але на основі яких, як буде показано надалі, можна формувати ЧВП. Дальність зв'язку по МРК може становити до 2000 км, для виявлення корисного для зв'язку метеорного сліду й передачі по ньому інформації застосовуються спеціальні алгоритми.

За підсумками першого розділу зроблені отримані висновки, а саме:

- формування числових випадкових послідовностей є актуальним науковим і практичним завданням;
- існуючі методи формування числових випадкових послідовностей, застосовуваних у криптографічних цілях, не вирішують питання їхнього розподілу (доставки). Застосовувані методи доставки ЧВП не гарантують їхню схоронність;
- метеорний радіоканал має унікальні властивості: численні випадкові характеристики й скритність.

Тому існує актуальне наукове й практичне завдання-формування ЧВП із використанням МРК.

У **другому розділі** проаналізовано кілька способів формування ЧВП із використанням п'яти різних випадкових характеристик метеорного сліду. Результати, наведені в розділі, опубліковані в [1, 2, 3].

Стисло розглянуто уже відомий спосіб формування ЧВП із використанням МРК, заснований на вимірі часу поширення сигналу каналом зв’язку. Основний фізичний принцип, що лежить в основі цього способу-принцип взаємності МРК, тобто, рівність часу поширення сигналу по ньому в прямому й у зворотному напрямках.

Традиційно ця властивість МРК використовувала для високоточної синхронізації еталонів часу й частоти, причому, сам час поширення виключався з розрахунків шляхом застосування відповідних алгоритмів. Але, якщо шкали часу в обох пунктах зведені, то виникає можливість вимірювати час поширення. На жаль, для реалізації такого способу кожний з пунктів має бути оснащений високостабільним еталоном часу, причому, шкали обох еталонів мають бути зведені з охибкою, що не перевищує 1 нс. Це значно ускладнює його практичну реалізацію.

При вимірі часу поширення з точністю ΔТ весь діапазон вимірювання часу поширення дасть N_0 реалізацій випадкового процесу. Таким чином, кожному виміру може бути приписане випадкове двійкове число із числом розрядів *m (*довжина ключа).

$$m = \log_2(N_0 - 1). \tag{1}$$

Практичний приклад реалізації показав величину *m,* що дорівнює 19 бітам на один метеорний слід.

Інша можливість формування ЧВП, запропонована в роботі, заснована на використанні інтервалів між метеорними слідами. Інтервал є випадковим, оскільки визначається моментами вторгнення в атмосферу дрібних космічних часток і може змінюватися від долей секунди до декількох хвилин. Даний спосіб заснований на двох фізичних принципах. По-перше, незалежно від місця й часу виникнення метеорного сліду, одночасно випромінені у двох пунктах сигнали, будучи відбитими від даного сліду, приймаються також одночасно. По-друге, передній фронт сигналу, відбитого від метеорного сліду, як правило, досить крутий, що виключає неоднозначність у визначенні моменту початку існування МРК.

На рис. 1 наведено структурну схему пристрою, що реалізує зазначений спосіб формування ЧВП.

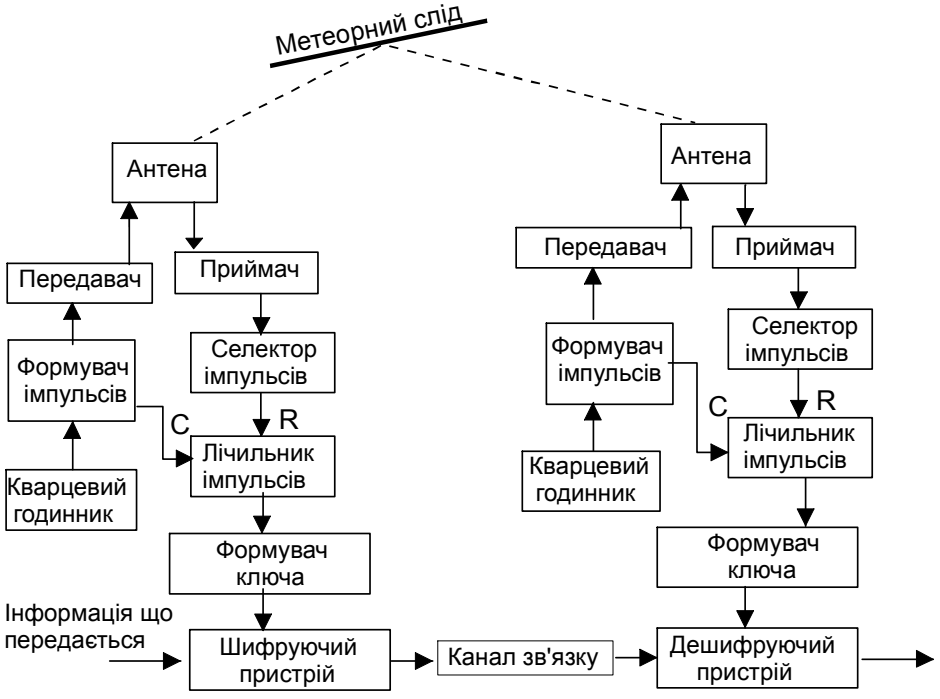

Рис. 1. Структурна схема метеорної системи зв'язку для використання інтервалів часу між слідами

Для реалізації такої схеми не потрібні високостабільні еталони часу, що істотно спрощує практичне застосування. При використанні кварцового резонатора похибка виміру не має перевищувати інтервалу між зондувальними імпульсами, що становить не більше 20 мс. Цієї стабільності цілком достатньо для використання даної характеристики з метою формування ЧВП.

Кількість біт ключа, що може бути сформоване на кожному інтервалі між метеорними слідами визначається за формулою:

$$N = \log_2 \frac{T_s}{T_{\max}}, \qquad (2)$$

де $T_{\max}$- максимально можливий час очікування появи МРК; T_s- період проходження зондувальних імпульсів.

Слід зазначити, що при використанні цієї характеристики МРК необхідно враховувати нерівномірний закон розподілу часу очікування його виникнення. Не виключені також ситуації, коли результати одиничних вимірів відрізнятимуться в пунктах зв'язку через завади, що призведе до формування різних ЧВП у різних пунктах. Для виключення подібних ситуацій необхідно передбачити обмін хеш-функціями ЧВП.

Зроблена в роботі оцінка дозволяє оцінити продуктивність способу не гірше, ніж 15 біт на кожний метеорний слід, або, виходячи з їхнього закону розподілу, 128 біт на годину.

Третя характеристика МРК, що може бути використана для формування ЧВП, це координати метеорного сліду. Метеорні сліди можуть виникати в досить великій області простору. Місце виникнення чергового сліду заздалегідь невідомо.

Спосіб заснований на тому, що в кожному з пунктів зв'язку вимірюються кути й затримки, які дозволяють знайти координати метеорного сліду. На рис. 2 зображено просторову схему радіолінії метеорного зв'язку, де показано кути α1, β1, α2, β2, які виміряються з пунктів зв'язку.

Для визначення координати сліду в просторі використовуємо фазо-кутомірний спосіб. Для цього п'ять антен розташовують у формі «хреста». Зміні напрямку на метеорний слід відповідатиме зміна різниці фаз у прийомних антенах. Знаючи відстань між антенами й різницю фаз, можна розрахувати кутові координати сліду.

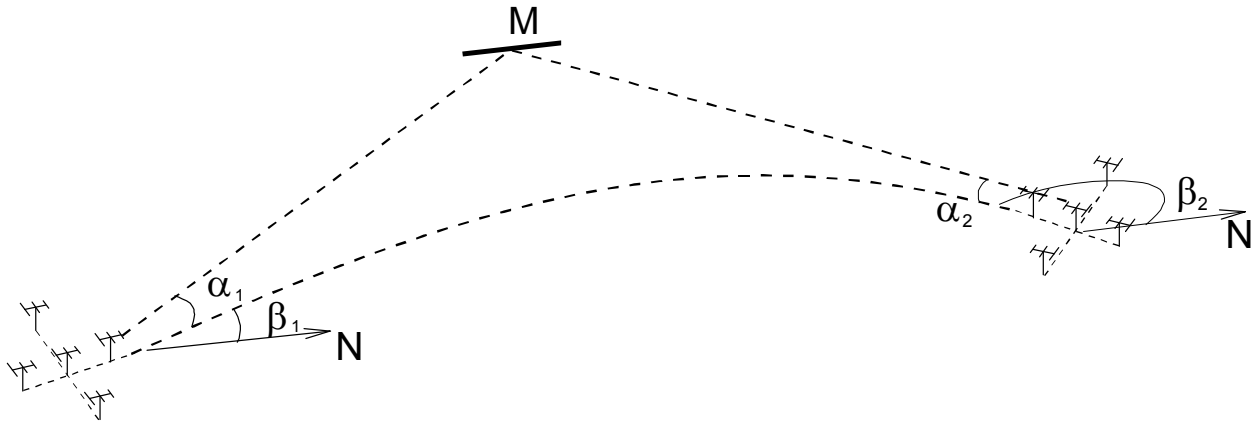

Рис. 2. Визначення координат сліду із двох пунктів

Далі за заздалегідь установленими закономірностями числові значення координат перетворяться в ЧВП. Розраховано похибки, показано проблемні місця цього способу, шляхи вирішення й підвищення продуктивності.

Продуктивність способу по кожній з координат (поздовжньої, поперечної й по висоті) може бути знайдена за формулою:

$$N = \log_2 \frac{W_{\max} - W_{\min}}{\sigma_W} \ , \tag{3}$$

де $W_{\max}$ і $W_{\min}$ - максимальне й мінімальне значення координати метеорного сліду, у межах яких можуть виникати метеорні сліди; σ_W - похибка визначення зазначеної координати.

У випадку використання всіх трьох координат метеорного сліду одночасно, продуктивність способу може бути оцінена у 15- 18 біт на кожний метеорний слід.

Четверта випадкова характеристика МРК, що також може бути використана для формування ЧВП- тривалість метеорного радіовідбиття. Як відомо, час існування МРК розподілено в діапазоні від десятків мілісекунд до декількох секунд за експонентним законом.

Момент початку метеорного сліду в рознесених пунктах можна зафіксувати однозначно, тому що швидкість зростання переднього фронту сигналу, відбитого від метеорного сліду, може становити до 500 дБ/с. Що ж стосується моменту закінчення сліду, то він є не цілком однозначним. Хвилеподібний характер зміни амплітуди відбитого сигналу, що описується амплітудно-часовою характеристикою (АЧХ), не дозволяє точно вказати момент закінчення відбиття. Тому мову можна вести, наприклад, про зменшення амплітуди прийнятого сигналу в 10 разів. Але навіть у цьому випадку виміри у різних пунктах можуть дати різний результат, оскільки в них може бути різний рівень перешкод. Це основний недолік даного способу формування ЧВП. Тому має сенс розглянути питання більш широко й аналізувати не тільки час існування сліду або його постійну часу, але й поводження амплітуди відбитого сигналу за увесь час його існування, оскільки вона унікальна для кожного з них.

Як п'яту випадкову характеристику МРК можна використовувати АЧХ відбитого сигналу, оскільки електронна щільність сліду й ряд інших параметрів щоразу виявляються різними. Вираз, що задає модель метеорної АЧХ, можна записати у вигляді:

$$I_m = A_н \sqrt{\left(\frac{1}{\sqrt{2}} \int_0^{x_0} \cos(\frac{\pi}{2} x^2) e^{-\Delta(x_0 - x)} dx \right)^2 + \left(\frac{1}{\sqrt{2}} \int_0^{x_0} \sin(\frac{\pi}{2} x^2) e^{-\Delta(x_0 - x)} dx \right)^2} \ , \tag{4}$$

де $A_н$- незалежний параметр моделі, x_0 - величина, пов'язана з положенням голови сліду s_0 описується виразом $x_0 = \frac{2s_0}{\sqrt{R\lambda}}$, а $\Delta = \frac{8\pi^2 D\sqrt{R}}{V\sqrt{\lambda^3}}$ містить у собі довжину хвилі λ, проекцію швидкості V, відстань до сліду R й коефіцієнт амбіполярної дифузії D. Всі параметри, що входять у вираз (4) є випадковими для кожного нового метеорно-

го сліду. Але, якщо виходити з того, що АЧХ того самого метеорного сліду, що спостерігається з різних пунктів, буде однакова, той і зазначені параметри в них, відновлення шляхом моделювання, також будуть однакові. Отже, їх також можна використовувати як основу для формування ЧВП.

Суть методу в тому, що в кожному з пунктів виконуються оцінки параметрів, які входять у формулу (4), і на їхній основі відбувається формування ЧВП. Оцінка продуктивності й імовірності помилки для даного способу в справжній роботі не здійснювалася.

Загальною перевагою зазначених способів є те, що сформовані в такий спосіб послідовності не можуть бути перехоплені сторонніми внаслідок унікальних властивостей метеорного радіоканалу, що забезпечує зв'язок тільки між двома кореспондентами. Для будь-кого стороннього, за наявності аналогічної апаратури та можливості виміряти ті ж параметри МРК, які є основою для формування послідовності, відрізнятимуться. Отже, відрізнятимуться й сформовані послідовності. А в пунктах розміщення кореспондентів метеорного зв'язку послідовності формуються одночасно, що виключає необхідність їхньої передачі.

Слід зазначити, що всім даним способам властивий і ряд загальних недоліків. По-перше, ЧВП, сформовані кожним із зазначених способів матимуть нерівномірний закон розподілу, що вимагає їхньої спеціальної обробки. По-друге, добовий хід метеорної активності призведе до того, що в ранкові години швидкість формування ЧВП буде більше, а у вечірні – менше.

По третє, необхідно враховувати можливий взаємозв'язок між ЧВП, сформованими різними способами. Цей взаємозв'язок можна виявити тільки шляхом моделювання (або експериментально).

Таким чином, у другому розділі проаналізовано 5 різних характеристик МРК і показано, що всі вони придатні для формування ЧВП. Показано переваги й недоліки. Середня продуктивність розглянутих способів оцінюється в 15...19 біт на слід. Залежно від часу доби, траси й параметрів апаратури кожний з названих способів може забезпечувати формування послідовності від 300 до 2000 біт у годину.

У **третьому розділі** наведено та розроблено модель МРК, що дозволяє моделювати випадкові характеристики метеорних слідів, і результати моделювання. Результати розділу опубліковані у [5].

Структуру моделі метеорного радіоканалу можна подати з декількох основних компонентів: 1) астрономічна модель припливу метеорної речовини на Землю; 2) методика геометричного відбору; 3) фізична модель утворення сліду; 4) математична модель приймально-передавальної станції й енергетичної селекції. Як астрономічна база можуть використовуватися гіпотетичні або емпіричні моделі припливу метеорної речовини.

Для моделювання були обрані дві траси: Харків – Київ (довжина 450 км, орієнтація «схід – захід») і Харків – Балаклейський науковий полігон (довжина 80 км, орієнтація близька до «північ – південь»). Моделювалися годинні інтервали спостережень у вечірній і ранковий час. Результатом моделювання були випадкові характеристики метеорних слідів, такі як електронна щільність, косинус кута між метеорним слідом еліпсоїдом з фокусами в пунктах зв'язку, постійна часу розсіювання сліду й відносні просторові координати.

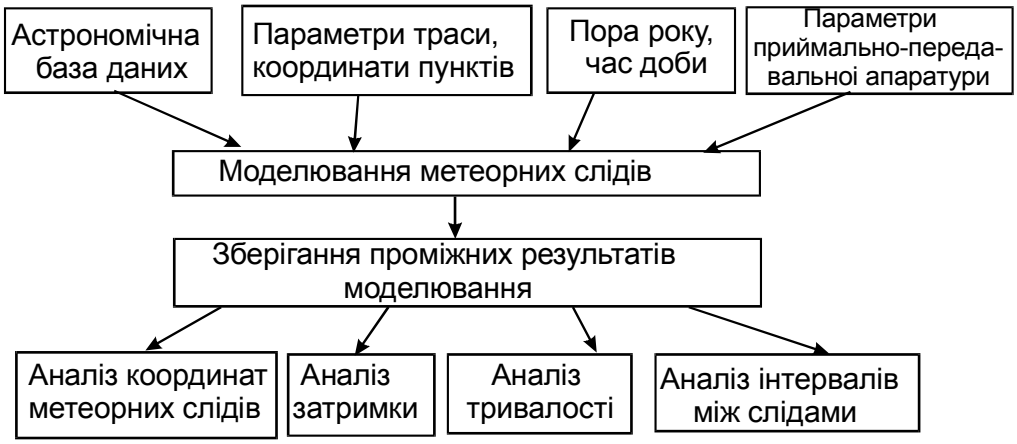

Рис. 3. Структура моделі МРК

Моделювання координат метеорних слідів містило в собі, перебір всіх можливих координат у межах заданої області простору й виявлення таких відносних просторових координат x_0, y_0 і z_0, для яких виконувалася умова відбиття.

Гістограми, що характеризують закони розподілу цих значень для кожної координати й для кожної з розглянутих трас, наведено на рис. 4- 9.

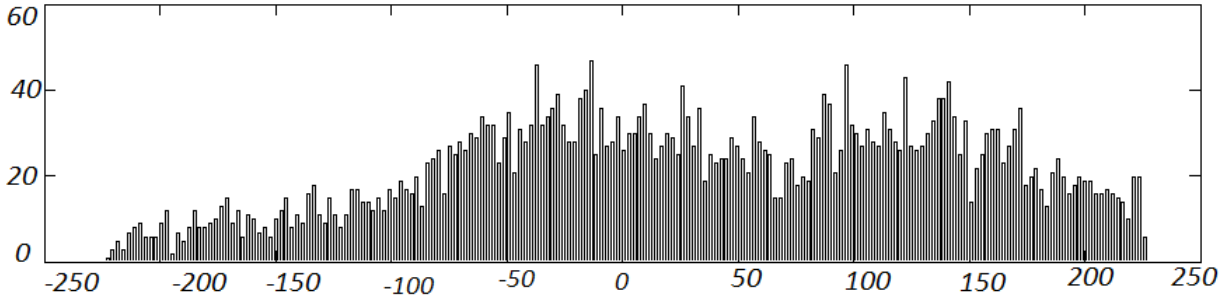

Рис.4. Гістограма значень поздовжньої координати (траса 80 км)

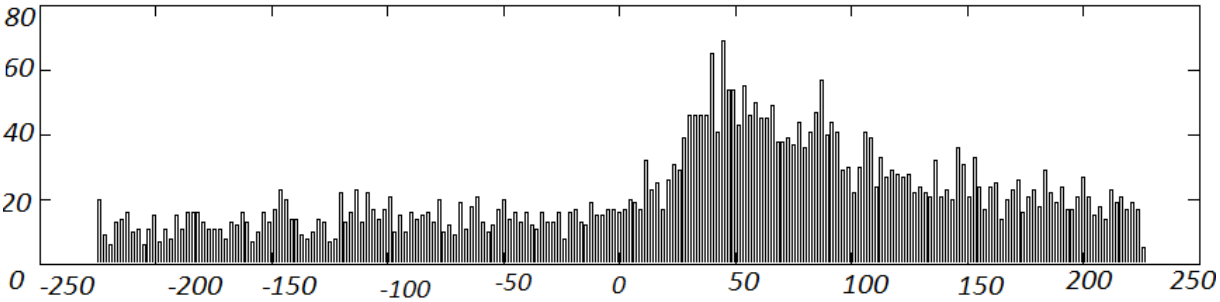

Рис.5. Гістограма значень поперечної координати (траса 80 км)

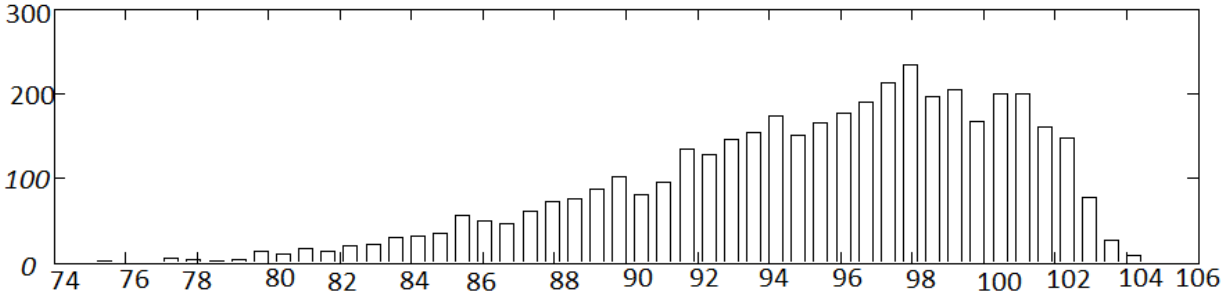

Рис.6. Гістограма значень висоти (траса 80 км)

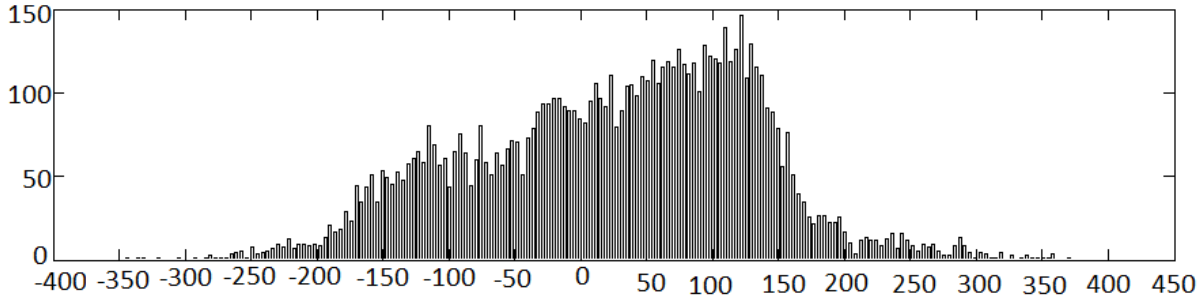

Рис.7. Гістограма значень поздовжньої координати (траса 450 км)

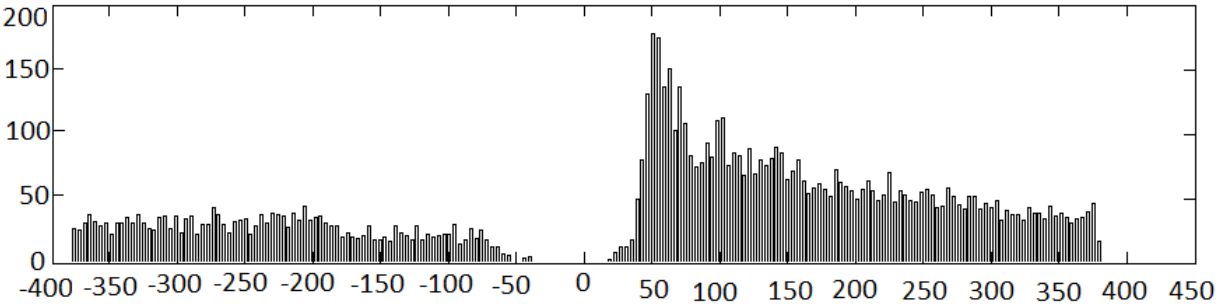

Рис.8. Гістограма значень поперечної координати (450 км)

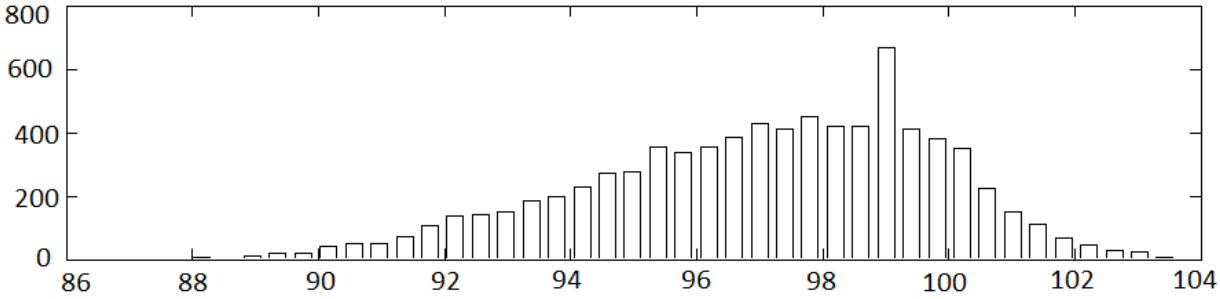

Рис. 9. Гістограма значень висоти (траса 450 км)

Візуальний аналіз отриманих результатів дозволяє зробити висновок про нерівномірність законів розподілу. Цього слід було очікувати, оскільки «корисні» для зв'язку метеорні сліди розподілені в просторі нерівномірно й у цьому значенні координати сліду не цілком випадкові. Причому, протягом доби спостерігається зсув «гарячих зон» – областей з перевагою корисних для зв'язку метеорних слідів. Даний факт може бути відомий потенційному криптоаналітику, тому при формуванні ЧВП необхідно вживати заходів з вирівнювання закону розподілу, щоб виключити з нього загальновідомі закономірності.

Метеорна область, як відомо, лежить у межах 70...110 км, але й у ній метеорні сліди виникають нерівномірно, тому при вимірі реальних координат у ході експерименту отримані залежності мало відрізнятимуться від змодельованих. Тому все сказане про координати сліду рівною мірою відноситься також і до його висоти.

Час поширення моделювався на підставі знайдених координат x_0, y_0 і z_0:

$$t_{PPB} = \frac{L}{c}\left(\sqrt{(1-x_0)^2 + y_0^2 + z_0^2} + \sqrt{(-1-x_0)^2 + y_0^2 + z_0^2}\right), \qquad (5)$$

де c – швидкість світла у вакуумі, L- довжина траси.

Результати моделювання наведено на рис. 10. Як видно, закон розподілу часу поширення також нерівномірний. Спостерігається мода в області мінімальних значень, обумовлена великою кількістю слідів, розташованих поблизу осі траси, відносно рівномірний розподіл в області середніх значень і спад за більших значень часу поширення.

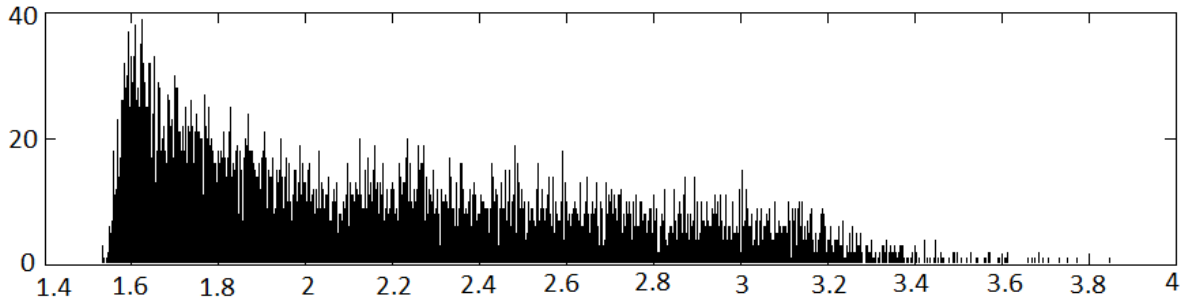

Рис. 10. Гістограма значень часу поширення (мс) для траси довжиною 450 км

Моделювання тривалості було здійснено на підставі припущення про експонентний спад амплітуди відбитого сигналу. На рис. 11 і 12 відображено значення постійної часу розсіювання сліду τ, тобто, часу, протягом якого амплітуда сигналу зменшується у *e* раз. (Реальні тривалості сигналів приблизно втричі більше).

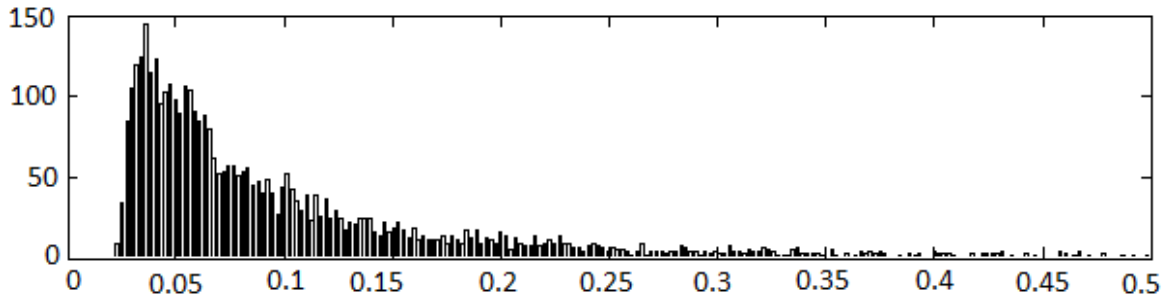

Рис. 11. Гістограма тривалості (мс) для траси довжиною 450 км

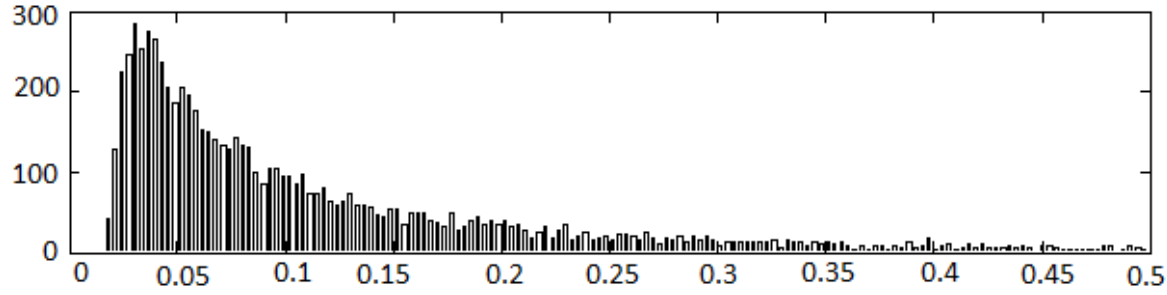

Рис. 12. Гістограма тривалості (мс) для траси довжиною 80 км

Як видно з рисунків, закон розподілу має експонентний характер. Для його вирівнювання може бути застосована відповідна методика. Але, на думку автора, використання цього параметра для формування ЧВП недоцільно через різний рівень шумів у пунктах зв'язку.

Для моделювання інтервалів між слідами було накопичено більше 300 тис. радіовідбиттів.

Отриманий закон розподілу можна апроксимувати як:

$$F(t) = 1 - e^{\frac{-t-6}{20}}. \quad (6)$$

Апроксимацію зображено на рис. 13, (час у хвилинах).

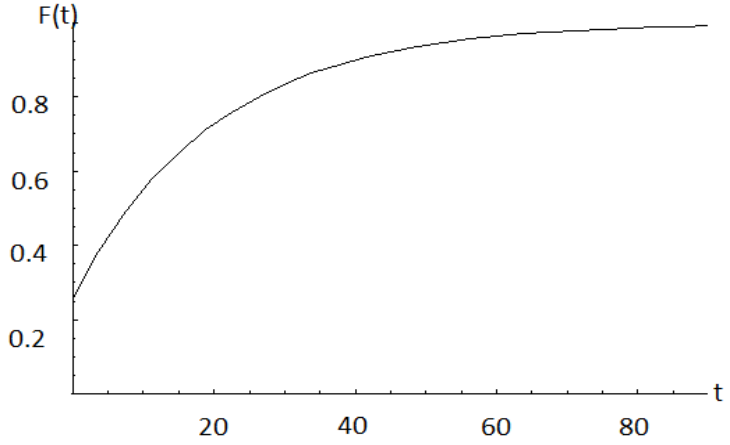

Рис. 13. Апроксимація закону розподілу часу очікування МРК (*t* у *хв.*)

Як видно із графіка, закон розподілу часу очікування сеансу зв'язку також нерівномірний. Для підвищення криптографічної стійкості методу, закон розподілу був перетворений з експонентного в рівномірний. У розділі також розроблено алгоритм такого перетворення.

Також був проведений аналіз взаємозв'язку різних випадкових характеристик МРК.

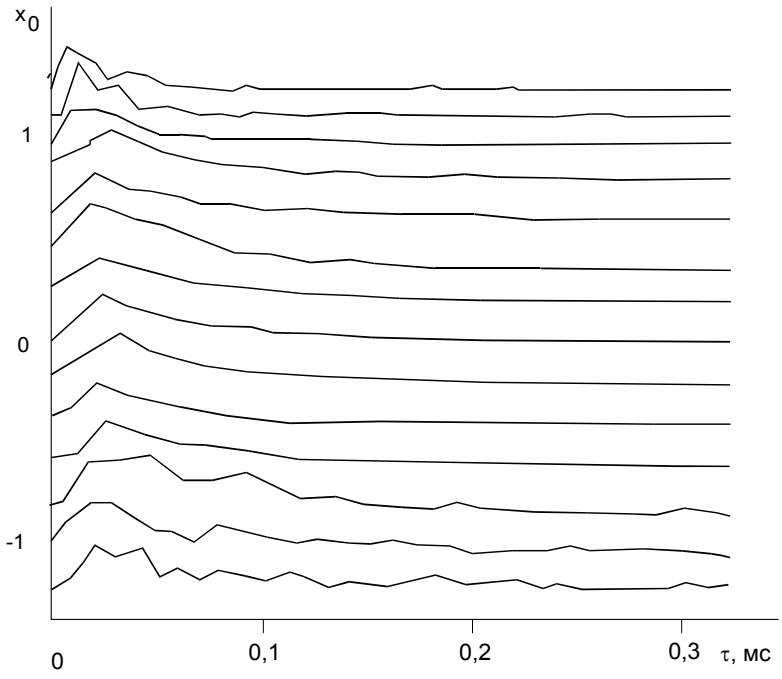

Рис. 14. Залежність тривалості метеорних слідів від поздовжньої координати

Також був проведений аналіз взаємозв'язку різних випадкових характеристик МРК. Для моделювання взято всього дві пари характеристик: координати сліду й тривалість відбиття. Їхній взаємозв'язок не очевидний, але й незалежність викликала сумнів. Аналіз був зроблений для траси довжиною 400 км.

На рис. 14 наведено сімейство кривих (по суті гістограм, аналогічних рис. 12), побудованих окремо для різних поздовжніх координат сліду. Як видно з рисунка, якої-небудь залежності закону розподілу тривалості від поздовжньої координати не спостерігається.

Аналогічна картина спостерігається й для поперечної координати – її взаємозв'язок із тривалістю відсутній.

Інакше складається справа з висотою метеорного сліду. Для аналізу залежності тривалості від висоти весь діапазон висот метеорної зони був розділений на 8 піддіапазонів по 0,02 відносні одиниці кожний (що для траси довжиною 400 км відповідає 4 км). Для кожного піддіапазону був отриманий розподіл тривалості, що графічно зображено на рис. 15.

Як видно із графіка, спостерігається чіткий взаємозв'язок між максимумом розподілу тривалості й висотою сліду – зі збільшенням висоти мода розподілу зміщується

вбік менших значень τ. Це наслідок того, що на більших висотах процес руйнування сліду відбувається швидше, у результаті чого там переважають більш короткі сліди.

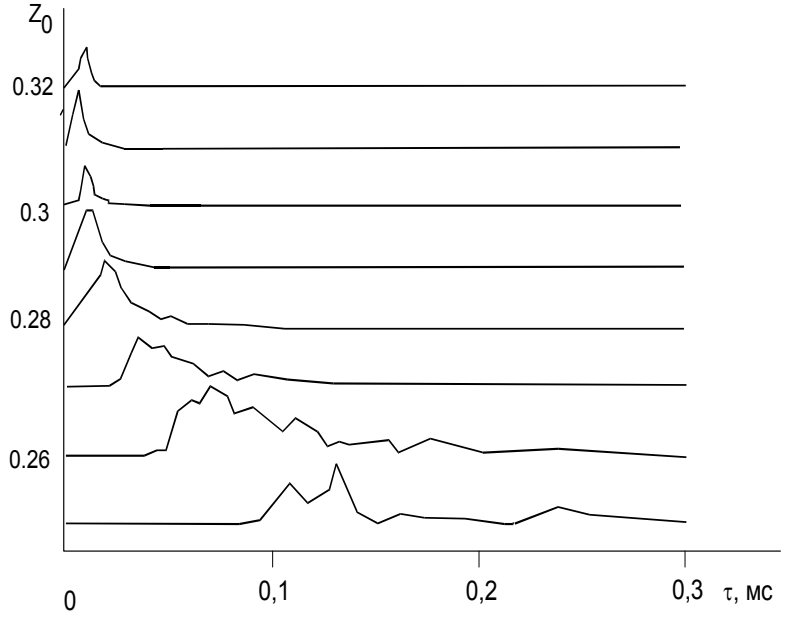

Рис. 15. Залежність тривалості метеорних слідів від висоти

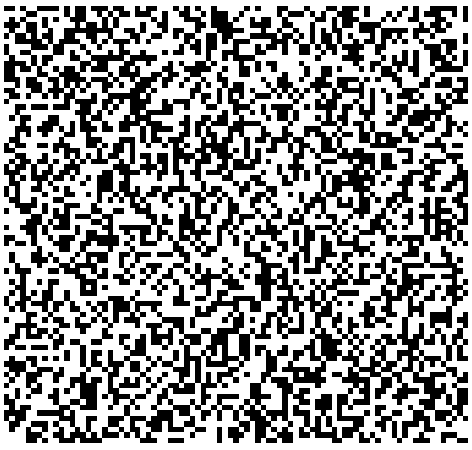

Рис. 16. Візуальне подання експериментально отриманої ЧВП

Отже, випадкові числа, отримані з висоти й із тривалості метеорного радіовідбиття, не можна використовувати спільно. Спільному використанню тривалості й горизонтальних координат ніщо не перешкоджає.

Таким чином, у розділі розроблено модель МРК і на її основі отримано закони розподілу ймовірності ряду характеристик МРК.

Отримані закони розподілу мають нерівномірний характер, тому, у випадку їхнього використання для криптографічного захисту інформації, потрібно додаткове перетворення. Установлено, що ряд характеристик МРК, зокрема, координати й час поширення, взаємозалежні. Якщо із числа координат виключити висоту метеорного сліду, то між двома координатами, що залишилися, і тривалістю сліду взаємозв'язку не виявлено.

У **четвертому розділі** наведено експериментальні дані й результати їхньої обробки, проведених у рамках даної роботи. Матеріали розділу опубліковані в [4, 6, 7].

Перед початком експериментальної частини роботи аналізувалися різні варіанти її проведення й ті характеристики, випадковість яких можна було б перевірити. Виходячи з наявних ресурсів і можливостей, були експериментально проаналізовані можливість формування ЧВП із використанням інтервалів між метеорними слідами.

Як дані для аналізу імовірнісних характеристик МРК і перевірки зроблених у роботі теоретичних припущень використовувалися матеріали, отримані на Метеорній автоматизованій радіолокаційній станції (МАРС) у серпні 2006 року. Потужність передавача 400 кВт, носійна частота 31,5 МГц, ДС орієнтовані на схід під кутом місця 30°, частота повторення імпульсів 100 Гц. Для прийому й передачі використовувалися 4-х елементні антени «хвильовий канал».

Вихідні дані були записаним у вигляді файлу сигналом з виходу 12-розрядного АЦП, підключеного до виходу радіолокаційного приймача. Для обробки цих даних був розроблений алгоритм і складено відповідну програму, що передбачає виявлення метеорного сигналу й фіксацію моменту його появи. Далі програмно обчислювалася різниця між моментами появи метеорних радіовідбиттів, з яких і формувалася необхідна ЧВП. Результати обчислень зберігалися у файл.

Усього за підсумками обробки результатів чотиригодинних спостережень, була сформована послідовність довжиною близько 20000 біт. Її візуальне подання показано на рис. 16. Тут безперервна послідовність розбита на рядки довжиною по 140 біт у кожній і розміщена у вигляді 140 розташованих поряд ліній. Чорні елементи відповідають «0», а білі «1».

Отримана послідовність була протестована. Для тестування використовувався моно бітний тест (перевірка рівності частот «0» і «1»), покер тест (рівність частот однакових блоків з 4 біт), серійний тест (перевірка кількості однакових елементів, що послідовно зустрічаються) і тест довжини серії (визначення максимальної довжини серії з однакових елементів). Результати тестування, наведені в першій частині табл. 1, показали, що послідовність не може бути використана як криптографічний ключ,оскільки в ній є деякі закономірності. Так, частота появи «0» і «1» виявилася різною. Аналіз послідовності вроздріб (дві послідовності по 10 000 біт, чотири по 5 000) дав той же результат.

Поглиблений аналіз причин, за якими послідовність не пройшла тести, показав, що частота появи «0» і «1» не однакова через велику кількість зайвих нулів перед «короткими» числовими значеннями.

Була запропонована методика поліпшення якості даної послідовності, що полягає у видаленні зайвих нулів, кількість яких кратне 4. При незначному зменшенні довжини послідовності, її якість помітно покращилася. Результати тестування «поліпшеної» послідовності наведено в другій частині табл. 1.

Таблиця 1 - Результати тестування випадкових послідовностей

Назва тесту	Вихідна послідовність (20 000 біт)				Послідовність після поліпшення (19 820 біт)			
	Статистика			Результат	Статистика			Результат
Монобітний тест	10519 біт			-	9950 біт			+
Покер тест	74,53			-	48,83			+
Серійний тест	Довжина серії	Серій «0»	Серій «1»	-	Довжина серії	Серій «0»	Серій «1»	+
	1	2447	2705		1	2561	2650	
	2	1315	1292		2	1296	1249	
	3	678	648		3	682	651	
	4	308	256		4	324	280	
	5	167	106		5	137	153	
	≥6	188	96		≥6	123	140	
Потоковий тест довжини	15 біт			+	13 біт			+

З таблиці 1 видно, що сформована в такий спосіб послідовність має кращі статистичні характеристики й проходить тест. Можна очікувати, що більш поглиблені методи вирівнювання частоти появи 0 і 1 дадуть ще кращий результат.

Таким чином, експериментальна перевірка показала, що інтервали між метеорними слідами можуть використовуватися для формування ЧВП.

Показано, що така послідовність без додаткової обробки є «не досить випадковою» – у ній не однакова кількість нулів і одиниць. Запропоновано методику поліпшення характеристик випадкових послідовностей, отриманих шляхом виміру інтервалів між метеорними слідами.

ОСНОВНІ ВИСНОВКИ Й РЕЗУЛЬТАТИ РОБОТИ

Внаслідок виконаних досліджень в рамках даної дисертаційної роботи вирішена актуальна науково-технічна задача формування випадкових числових послідовностей на основі розробки методів використання імовірнісних характеристик метеорного радіоканалу. При цьому отримані наукові та практичні результати, що зводяться до наступного:

1. Теоретично обґрунтовані п'ять різних способів формування ЧВП із використанням різних випадкових характеристик метеорного радіоканалу. Показано, що на кожному метеорному сліді по кожній з його випадкових характеристик може бути сформований 15...20 випадкових біт. Таким чином, швидкість формування ЧВП може становити до 1000 біт у годину. Основні переваги сформованих ЧВП у тому, що вони є дійсно випадковими, а не псевдовипадковими; вони формуються у двох пунктах зв'язку одночасно і їх не потрібно передавати; перехоплення послідовностей сторонніми або формування в них ідентичних ЧВП важко реалізуються через унікальні властивості МРК.

2. Розроблено модель МРК, що дозволяє моделювати його випадкові характеристики, такі як координати метеорного сліду (включаючи висоту), тривалість радіовідбиття, інтервали між слідами й час поширення сигналів по трасі.

3. З використанням розробленої моделі отримано закони розподілу ймовірності таких характеристик метеорного радіоканалу, як координати, час поширення, тривалість та інтервали між слідами. Показано, що закони розподілу є нерівномірними й мають потребу в додатковому перетворенні. Розроблено алгоритм такого перетворення.

4. Виявлено взаємозв'язок тривалості радіовідбиття з висотою метеорного сліду. Показано відсутність взаємозв'язку тривалості радіовідбиття з поздовжньою й поперечною координатами сліду, так само як і з іншими випадковими характеристиками МРК.

5. Експериментально підтверджено можливість формування числової випадкової послідовності шляхом виміру інтервалів між метеорними слідами. Отримана послідовність після нескладної обробки успішно проходить тестування на відсутність закономірностей.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Шернин М.А. Использование метеорного радиоканала для формирования случайной числовой последовательности / И.Е.Антипов, А.А.Костыря, М.А. Шернин // Радиотехника. Всеукр. межвед. науч.-техн. сб. 2009. № 157. С. 25 – 29.

2. Пат. 40880 Україна МПК (2009) H04L 9/00, H04B 7/22. Спосіб незалежного формування випадкової числової послідовності, однакової у двох рознесених пунктах / Антіпов І.Є., Костиря О.О, Шернін М.О.; заявник та власник Харківський національний університет радіоелектроніки. – № u200814112; завл. 08.12.2008; опубл. 27.04.09, Бюл. № 8. – 4 с.

3. Шернин М.А. Формирование случайных числовых последовательностей с помощью метеорного радиоканала / М.А. Шернин//Радиоэлектроника и молодежь в XXI веке: XIII Международный молодежный форум, 30 марта-1 апреля. 2009 г.: тезисы докл. Ч1. – Х.,2009. – С.25

4. Mykhailo Shernun Experimental checking of forming random numerical sequence by using meteor burst channel/ Ivan Antipov, Mykhailo Shernun, Inna Tkalich // TCSET'2010: Proceedings of the Xth International Conference, 23-27 February 2010: - L.,2010. - p. 245.

5. Шернин М. А. Моделирование характеристик метеорного радиоканала для формирования случайных числовых последовательностей / И.Е. Антипов, А.А. Костыря, М.А. Шернин // Радиотехника. Всеукр. межвед. науч.-техн. сб. 2010. № 161. С. 82 – 86.

6. Шернин М. А. Тест случайной последовательности, полученной по характеристикам метеорного радиоканала/ М.А. Шернин, И.А. Ткалич // Радиоэлектроника и молодежь в XXI веке: 15й Международный молодежный форум, 18-20 апреля. 2011 г.: тезисы докл. Т.3. – Х:,2011. – С. 250– 251.

7. Шернин М. А. Статистические характеристики числовых последовательностей, полученных с использованием метеорного радиоканала/ И.Е.Антипов, М.А.Шернин // Восточно-Европейский журнал передовых технологий, 2011. - №. 5/9 (53). – С. 20- 22.

8. Шернин М. А. Исследование методов дистанционной генерации ключа одинакового для двух разнесенных пунктов/ И.Е.Антипов, И.А.Ткалич, М.А.Шернин // Защита информации в информационно-коммуникационных системах научно-практическая конференция, 24-26 травня 2010г.: тезисы докл. – К:, 2010. – С.3.

АНОТАЦІЯ

Шернін Михайло Олександрович. Методи формування числових випадкових послідовностей з використанням імовірнісних характеристик метеорного радіоканалу. – Рукопис.

Дисертація на здобуття вченого ступеня кандидата технічних наук за спеціальністю 05.12.17 – радіотехнічні та телевізійні системи. – Харківський національний університет радіоелектроніки, Харків, 2012.

Дисертаційна робота присвячена розвитку теми використання випадкових характеристик метеорного радіоканалу для формування випадкових числових послі-

довностей. Проаналізовано основні методи та способи формування числових випадкових послідовностей та шляхи їх реалізації. Описано розподілення випадкових величин та функцій розподілення. Також описано основні властивості, характеристики та фізичні основи метеорного радіоканалу, як джерел числових випадкових послідовностей. Точніше час розповсюдження сигналу у каналі, інтервал між слідами, координати сліду, тривалість та амплітуда АЧХ. Кожна з характеристик розглядається з точки зору практичної реалізації, шляхів поліпшення ефективності, продуктивності та звісно захищеності. Також розглянуто варіанти сумісного використання декількох випадкових характеристик.

Проведено моделювання усіх розглянутих характеристик метеорного радіоканалу. Розроблено модель метеорного радіоканалу, що допускає моделювання випадкових характеристик метеорних слідів та отримувати їх закони розподілення.

Оцінено продуктивність способів, що в середньому дорівнює 15- 20 біт на один метеорний слід (для кожного способу),а також працеспроможність кожного способу, що дорівнює близько 1000 біт на годину. Головна перевага запропонованих способів у тому, що випадкові послідовності формуються одночасно у двох пунктах, рознесених до 2000 км. Сформовані послідовності не можуть бути перехоплені стороннім через унікальність властивостей метеорного радіоканалу.

Експериментально доведено, що інтервали між метеорними слідами можуть бути використані для формування числових послідовностей. Запропоновано методику поліпшення характеристик випадкових послідовностей, отриманих шляхом вимірювання інтервалів між метеорними слідами.

Ключові слова: метеорний радіоканал, генератор випадкових числових послідовностей.

АННОТАЦИЯ

Шернин Михаил Александрович. Методы формирования числовых случайных последовательностей с использованием вероятностных характеристик метеорного радиоканала. – Рукопись.

Диссертация на соискание ученой степени кандидата технических наук по специальности 05.12.17 – радиотехнические и телевизионные системы. – Харьковский национальный университет радиоэлектроники, Харьков, 2012.

Диссертация посвящена развитию темы использования случайных характеристик метеорного радиоканала для формирования случайных числовых последовательностей, которые в последующем формируют секретные цифровые ключи.

Проанализированы основные методы и способы формирования числовых случайных последовательностей и пути их реализации. Описано распределение случайных величин и функции распределения. Показаны истинные генераторы случайных и генераторы псевдослучайных последовательностей, способы оценки качества реализуемых ими последовательностей. Так же описаны основные свойства, характеристики и физические основы метеорного радиоканала, подробный анализ характеристик метеорного радиоканала как источников числовых случайных последовательностей. А именно время распространения сигнала в канале, интервал между следами, координаты следа, длительность и амплитуда АВХ. Каждая из

характеристик рассматривается с точки зрения практической реализации, путей повышения эффективности, производительности и конечно защищенности. Так же рассмотрены варианты совместного использования нескольких случайных характеристик.

Проведено моделирование всех рассматриваемых характеристик метеорного радиоканала, из которого видно, что метеорный канал пригоден для формирования случайных числовых последовательностей. Разработана модель метеорного радиоканала, позволяющая моделировать случайные характеристики метеорных следов и получать их законы распределения.

Оценена производительность способов в среднем равная 15- 20 бит на один метеорный след (для каждого способа), а так же работоспособность каждого способа равная до 1000 бит в час. Главное достоинство предложенных способов является то, что случайные последовательности формируются одновременно в двух разнесенных на расстояние до 2000 км пунктах связи. Сформированные последовательности не могут быть перехвачены посторонним вследствие уникальности свойств метеорного радиоканала. Для любого постороннего измеренные параметры МРК будут отличаться. Следовательно, и числовые последовательности так же будут отличаться.

Экспериментально подтверждено, что интервалы между метеорными следами могут использоваться для формирования числовых последовательностей. Показано, что такая последовательность без дополнительной обработки является «не достаточно случайной»- в ней не равное количество нулей и единиц. Предложена методика улучшения характеристик случайных последовательностей, полученных путём измерения интервалов между метеорными следами. Получено подтверждение того, что последовательность, полученная улучшенным образом, может быть использована для формирования секретных ключей.

Ключевые слова: метеорный радиоканал, генератор случайных числовых последовательностей.

ABSTRACT

Shernin A. Mykhailo Methods of forming numerical casual sequences by using unexpected characteristics of meteoric channel.-The manuscript

Thesis for a candidate degree of technical sciences on specialty 05.12.17 – radio and television systems. – Kharkiv National University of Radio Electronics, Kharkiv, 2012.

The dissertation is devoted to developing theme of using random characteristics of a meteoric burst channel (MBC) for random numerical sequences formation which in the subsequent form can be used as confidential digital keys.

There are analyzed cores methods and ways numerical random sequences formations and a way of their realization. Distribution of random variables and distribution function is described. There are shown true random generators and pseudo random generators, ways of an estimation of quality of sequences realized by them. As the basic properties, characteristics and physical bases of a meteoric radio channel are described.

The detailed meteoric radio channel characteristics analysis as sources of numerical random sequences. Namely signal time distribution in the channel, an interval between traces, trace coordinates, duration and amplitude time characteristics. Each of characteristics is considered from the practical realization, ways of increase of efficiency, productivity and certainly security point of view. There are considered sharing of several random characteristics.

Modeling all considered characteristics of meteor radio channel from which it is visible that the meteoric channel is suitable for formation of random numerical sequences. The model of the meteoric radio channel is developed, allowing to model random characteristics of meteoric traces and to receive their laws of distribution.

Productivity of ways on the average equal 15-20 bits on one meteoric trace (for each way) is estimated. And as working capacity of each way equal to 1000 bits in one hour. The main advantage of the offered ways is that random sequences are formed simultaneously in two places carried on distance to 2000 km. The generated sequences can't be intercepted by somebody else because uniqueness consequence properties of a meteoric radio channel. For anybody the measured parameters MBC will differ so as numerical sequences.

It is experimentally confirmed that intervals between meteoric traces can be used for formation of numerical sequences. It is shown that such sequence without in addition processing is «not enough random » - in it not equally quantity of zero and units. The technique of improvement of characteristics of the random sequences received by measurement of intervals between meteoric traces is offered. Acknowledgement of is received that the sequence received can be used in the improved image for formation of confidential keys.

Key worlds: meteor burst channel, generator random numerical sequences, casual characteristics of a MBC.

Підп. до друку 15.05.2012. Формат 60x84 1/16. Спосіб друку – ризографія.
Умов.друк.арк. 1,2. Облік. вид.арк. 1,1. Тираж 100 прим.
Ціна договірна Зам №

ХНУРЕ. Україна. 61166, Харків, просп. Леніна, 14

Віддруковано в навчально-науковому
видавничо-поліграфічному центрі ХНУРЕ
61166, Харків, просп. Леніна, 14