Нейронні системи використовують штучні нейронні мережі (ШНМ). Цей метод вимагає або великої кількості прикладів завдання розпізнавання при навчанні, або спеціальної структури нейронної мережі, яка враховує специфіку даного завдання. Проте, його відрізняє більш висока ефективність і продуктивність. Цей поділ на класи є умовним, адже система розпізнавання в своїх алгоритмах може використовувати комбінацію методів. Наприклад, система розпізнавання, результат ідентифікації якої ґрунтується на використанні ШНМ і додатковому статистичному підході.

Сучасні системи голосової аутентифікації, як і інші біометричні системи, мають низькі якісні характеристики. Останні можуть бути покращені за рахунок збільшення значення сигналу/шум, покращення обробки даних або аналізу більшої кількості інформаційних параметрів сигналу, що обробляється.

Здійснюючи процедуру цифрової обробки даних, що розглядається в дослідженні, основна увага приділяється врахуванню фазової інформації голосового сигналу, що, як показують дослідження, дозволяє значно збільшити ефективність досліджуваної процедури аутентифікації.

Література

1. Берштейн С. І., Колокольцев Н. К., Єрмолаєва В. В. Голосова аутентифікація // Молодий вчений. - 2018. - №25. - С. 93-94. - URL https://moluch.ru/archive/211/51686/

2. Біометрична аутентифікація: захист систем і конфіденційність користувачів. [Електронний ресурс] // URL: https://www.osp.ru/os/2012/10/13033122

3. Задорожний В. Огляд біометричних технологій [Електронний ресурс] // URL: http://www.bre.ru/security/20234.html

УДК 621.395

Коджебаш В. П.
ОНАЗ ім. О.С.Попова
vladu4ic@gmail.com
Керівник: к.т.н., доц. Йона Л.Г.

АЛГОРИТМ ШИФРУВАННЯ ДАНИХ ЗА ДОПОМОГОЮ ГЕНЕРАТОРА ХАОСА

Анотація. *Зараз в основі всіх технологій із захисту даних від несанкціонованого доступу або електронною комерції лежить наука криптографія, яка є частиною науки криптології. У свою чергу, ця наука використовує різні методи і алгоритми перетворення інформації. Для того, щоб інформація після шифрування, перетворилася в "інформаційне сміття", безглуздий набір символів для стороннього, використовуються спеціально розроблені методи - алгоритми шифрування.*

Метою дослідження є аналіз алгоритму шифрування даних на основі реалізації принципу одноразового блокнота з використанням гамма-послідовності, що формується за допомогою програмного генератора динамічного хаосу. Крім того, вдосконалюється генерація ключів (змінних) для датчиків динамічного хаосу, що полегшує і збільшує швидкість шифрування / розшифрування.

Під динамічним хаосом розуміється деяка нерегулярна, аперіодична зміна стану (рух) нелінійної динамічної системи, що володіє основними властивостями випадкового процесу [1]. Для формування значень хаотичної послідовності використовується генератор хаосу, який є детермінованим пристроєм, тому, сформований за певним алгоритмом процес, також є детермінованим. Найменша зміна початкових параметрів

генератора хаосу приводить до істотної зміни значень згенерованих коливань (рис. 1), що дає можливість формування різних траєкторій хаотичного процесу.

Розглянемо реалізацію сигналу на виході дискретного генератора хаосу на основі логістичних відображень [2]:

$$x_{n+1} = ax_n(1 - x_n), \tag{1}$$

де a − керуючий параметр, x_n − початкове значення хаотичної послідовності. Також відомі й інші програмні датчики хаотичного сигналу. На рис. 1 приведена реалізація сигналу $x(t)$ такого генератора при початковому значенні $x_{n=0} = 0{,}5$ і $a = 3{,}9$.

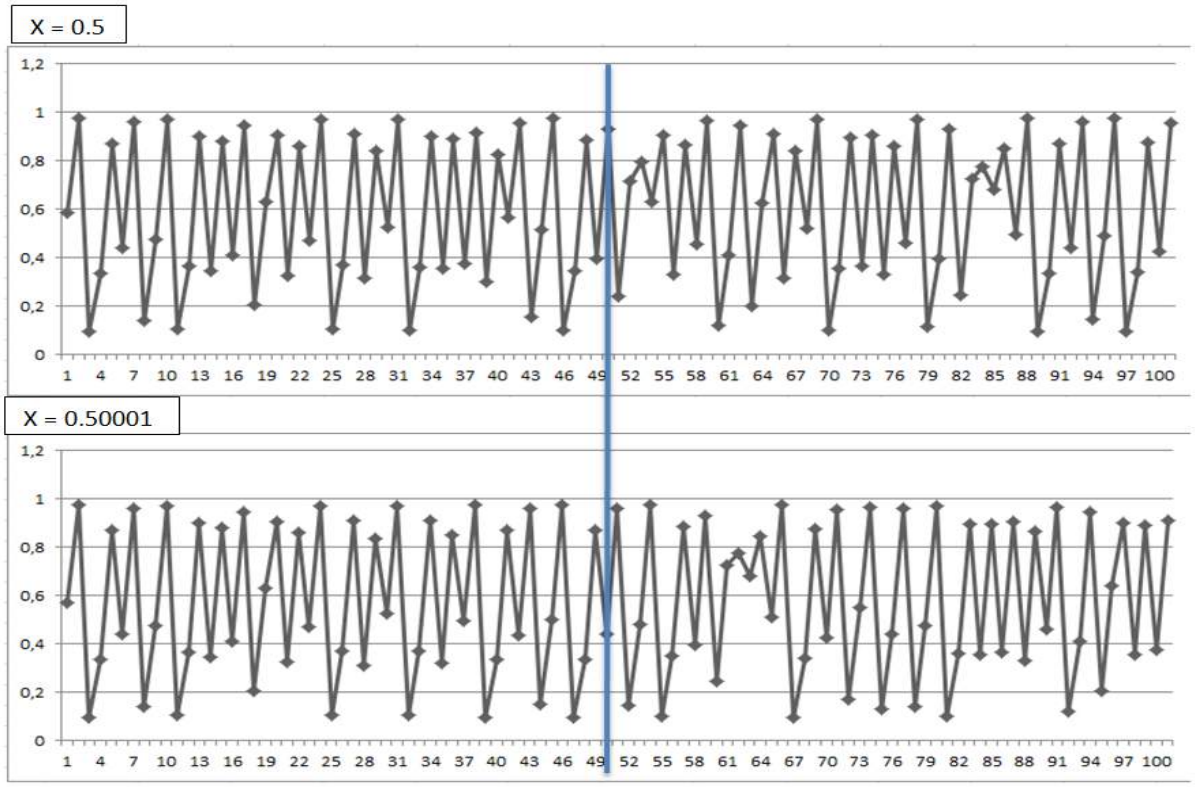

Рисунок 1 − Реалізація хаотичного сигналу

Такий процес має всі властивості шумоподібного процесу, так як для нього характерна неперіодична траєкторія в часі (рис. 1);
де КП – керуючий пристрій; ГК – генератор ключів, генеруючий початковий параметр для генератора хаоса; ДХ1-n – датчики хаоса; + - пристрій, що поєднує інформацію з ключем за допомогою операції додавання за модулем 2, утворюючи шифротекст.

Для збільшення криптостійкості можна використовувати 2 і більше датчиків хаосу (рис. 2) і різні маніпуляції з ними (додавання по модулю 2), при цьому при зміні початкового значення хаотичної послідовності (x_n)навіть на 1 мільйонну крива хаотичного сигналу повністю змінюється. Тому може бути нескінченна кількість варіацій цього сигналу, що робить шифротекст стійким до зламу (навіть при використанні одного датчика хаосу).

Для абсолютної криптографічного стійкості ключ повинен володіти трьома критично важливими властивостями :

1. Мати випадковий рівномірний розподіл;
2. Збігатися за розміром із заданим відкритим текстом;
3. Застосовуватися тільки один раз.

Даний алгоритм має всі властивості алгоритму з абсолютною криптографічною стійкістю, практично нескінченну кількість згенерованих різних ключів, а отримана гама такого ж розміру, як і відкритий текст.

Головною загрозою для будь-якого шифру є момент передачі шифротекста і самого ключа. Відомо, в даному алгоритмі ключ має такий же розмір, як і сам файл, який необхідно зашифрувати, що ускладнює і збільшує час передачі ключа. Це можна вирішити, якщо розглядати ключ не як отриману гаму, а тільки як початкове значення хаотичної послідовності в сукупності з номерами датчиків хаосу і різними маніпуляціями з ними.

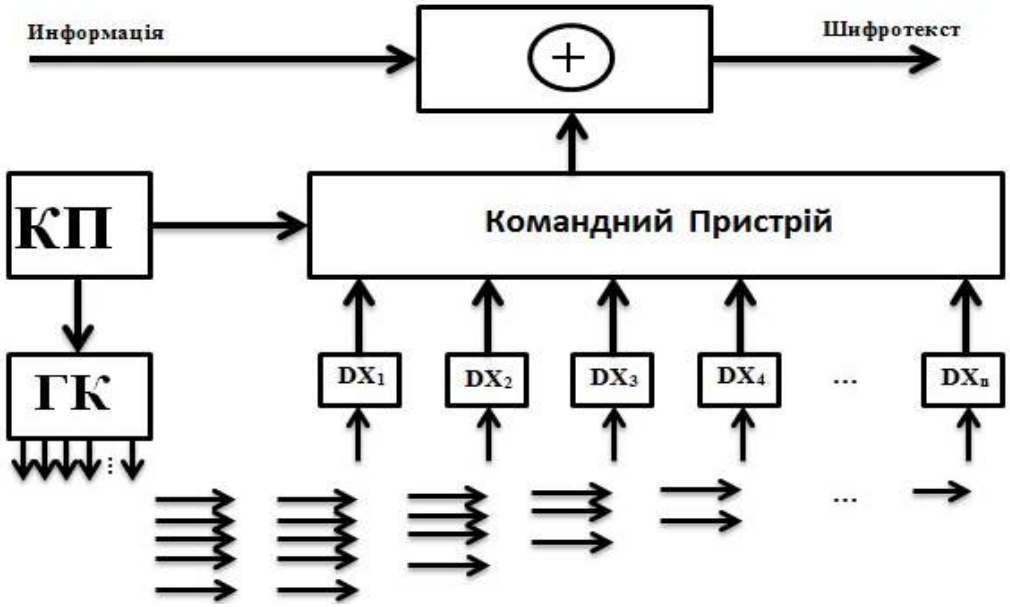

Рисунок 2 – Схема роботи шифрувального пристрою

Збільшення датчиків хаосу збільшує криптостійкість, але і збільшує час розшифрування.

Для усунення людського чинника можна використовувати генератор ключів (рис. 2), де вказуються межі від 0 до 1 і значення після коми, це дозволяє збільшити швидкість шифрування і розшифрування та максимально виключити процес витоку інформації.

Алгоритм шифрування даних зводиться до наступного:

1) задається ключ шифрування за допомогою генератора ключів, який видає випадковий x_n в зазначених межах і розрядністю;
2) кожен символ даних перетворюється в бітову послідовність $\{c_i\}$;
3) визначається кількість біт N в вихідної послідовності $\{c_i\}$;
4) формується двійкова гама-послідовність $\{s_i\}$ довжиною N за допомогою генератора хаосу з урахуванням системи за таких умов:

$$\begin{cases} a_i < 0{,}5, \text{ то } s_i = 0; \\ a_i \geq 0{,}5, \text{ то } s_i = 1; \end{cases}$$

5) здійснюється шифрування даних $\{c_i\}$ шляхом порозрядного підсумовування за модулем 2 з гама-послідовністю $\{s_i\}$:

$$C_i = c_i \oplus s_i.$$

Висновки. Запропонований алгоритм шифрування даних на основі програмних генераторів динамічного хаосу дозволяє використовувати принцип одноразового блокнота. Вибір значень ключа за допомогою генератора ключа вибирає параметр та дає необмежену можливість по формуванню нових траєкторій хаотичного сигналу, що є одним з важливих умов формування гама-послідовності. Використання декількох датчиків хаосу збільшує криптостійкість, а передача початкового значення хаотичної

послідовності в сукупності з номерами датчиків хаосу і різними маніпуляціями з ними збільшує швидкість передачі інформації.

Література

1. Кузнецов С.П. Динамический хаос / Кузнецов С.П. – М.: Физматлит, 2006. – 356 с.

2. Шахтарин Б.И. Генераторы хаотических колебаний / Шахтарин Б.И. – М.: Гелиос АРВ, 2007. – 248 с.

УДК 681.7.068

Копитов М.С.
ОНАЗ ім. О.С. Попова
Науковий керівник – ст. викл. Стащук О.М.

ВТРАТИ ПОТУЖНОСТІ ОПТИЧНОГО СИГНАЛУ НА СТИКУ ВОЛОКОН З РІЗНИМИ ДІАМЕТРАМИ МОДОВОЇ ПЛЯМИ

Анотація. *Встановлено характер залежності величини втрат потужності оптичного сигналу в оптичному волокні від різниці радіусів модових полів оптичних волокон, що стикуються. Надано рекомендації по врахуванню даних видів додаткових втрат при монтажних роботах на лінійних спорудах зв'язку.*

Оптичне волокно в даний час вважається найдосконалішим фізичним середовищем для передачі інформації, а також найперспективнішим середовищем для передачі великих потоків інформації на значні відстані. По одному волокну можна передати одночасно 10 мільйонів телефонних розмов і мільйон відеосигналів. Швидкість передачі даних може бути збільшена за рахунок передачі інформації відразу в двох напрямах, оскільки світлові хвилі можуть поширюватися в одному волокні незалежно один від одного.

Системи зв'язку на основі оптичних волокон стійкі до електромагнітних перешкод, а інформація, що передається по світловодах захищена від несанкціонованого доступу.

Основними параметрами, що характеризують оптичне волокно (ОВ) з огляду на передачу інформації є загасання та дисперсія.

Причини виникнення дисперсійних ефектів та способи визначення величини різних видів дисперсії наведена в [1, 2, 3, 4]. В роботах [5, 6, 7, 8, 9] розроблено компенсатори різних видів дисперсій.

Значний вплив на умови розповсюдження хвиль в ОВ причиняють різноманітні неоднорідності, які з'являються в них з різних причин.

В роботі встановлено додаткові втрати, пов'язані з неоднаковістю діаметрів модових полів ОВ, що стикуються.

Розрахунок неоднаковісті діаметрів модових полів визначається за формулою [10]:

$$a_w = 10 \cdot \lg\left(\frac{2w_1 w_2}{w_1^2 + w_2^2}\right), \quad (1)$$

де w_1 – радіус поля моди розраховується за формулою [10]:

$$w_1 = a \cdot \left(0.65 + 1.61 \cdot V_c^{-1.5} + 2.879 \cdot V_c^{-6}\right), \quad (2)$$

де V_c – нормована частота, для ОВ дорівнює 2,405; а – радіус осердя ОВ.