радужній оболонці ока або по спеціальному програмному забезпеченню). За допомогою цих заходів можна підвищити ступінь захисту від несанкціонованого доступу.

Література

1. *Партыка Т. Л., Попов И. И.* Информационная безопасность. Учебное пособие для студентов учреждений среднего профессионального образования. — М.: ФОРУМ: ИНФРА-М, 2002. - 368 с.: ил.
2. *Петров А.А.* Компьютерная безопасность. Криптографические методы защиты.-М.: ДМК, 2000. – 448с.: ил
3. http://www.intuit.ru

УДК 621.391:519.72

Н.Ф. Казакова
Міжнародний гуманітарний університет

СИНТЕЗ АЛГОРИТМУ РОБОТИ ТА ТЕХНІЧНА РЕАЛІЗАЦІЯ ДЕКОМПОЗИЦИОНОГО ГЕНЕРАТОРА ПОСЛІДОВНОСТІ GMW

Постановкою питання для дослідження в даному напрямку є завдання знаходження простого алгоритму генерації двійкових послідовностей GMW на основі генерації зрушених копій двійкової *m*- послідовності тієї ж довжини, а також освітлення переваг отриманого методу в порівнянні з відомими, які засновані на генерації *q*- та *m*- послідовностей [1]. Отже, метою є конструювання нового класу ПВП великого об'єму з близькою ідеальною автокореляцією і складною імітаційною структурою, а також розробка методу і структурної схеми пристрою їх генерації для захищених систем зв'язку. Рішення цієї проблеми розширює можливість вибору максимальної за об'ємом множини сигналів з заданою завадостійкістю і полегшує побудову пристроїв синхронізації абонентських приймачів, наприклад, для широкосмугових систем з CDMA, при заданому числі абонентів. На основі отриманої послідовності можуть бути синтезовані системи ортогональних кодових послідовностей великої лінійної складності та здійснене криптозахищене скремблювання передаваної інформації [2].

Пристрій, який розроблюється для формування двійкових ПВП GMW, дозволяє отримати одну або декілька форм ПВП при значно менших технічних витратах в порівнянні з відомими аналогічними пристроями. Значне зменшення витрат можна розглядати, як свого роду компенсацію за програш в числі форм, що генеруються [3]. Структурна схема пропонованого пристрою для генерації ПВП представлена на рис.1.

Робота пристрою полягає в наступному. Тактові імпульси, що поступають з генератора, з частотою f_T просувають записану в регістрі розподільника «одиницю», яка, проходячи через ту або іншу схему АБО комутатора, відкриває пов'язану з нею схему збігу, тим самим пропускаючи двійковий сигнал з виходу відповідного розряду регістра генератора базисної послідовності на вхід елементу АБО. Вихідні імпульси розподільника з частотою $\frac{f_T}{\varepsilon}$ поступають на тактовий вхід регістра зрушення генератора базисної послідовності, здійснюючи циклічне зрушення інформації в цьому регістрі. Таким чином, за тривалість періоду базисної послідовності на виході елементу АБО з'являться сигнали всіх 2^N-1 двійкових символів послідовності, що генерується пристроєм.

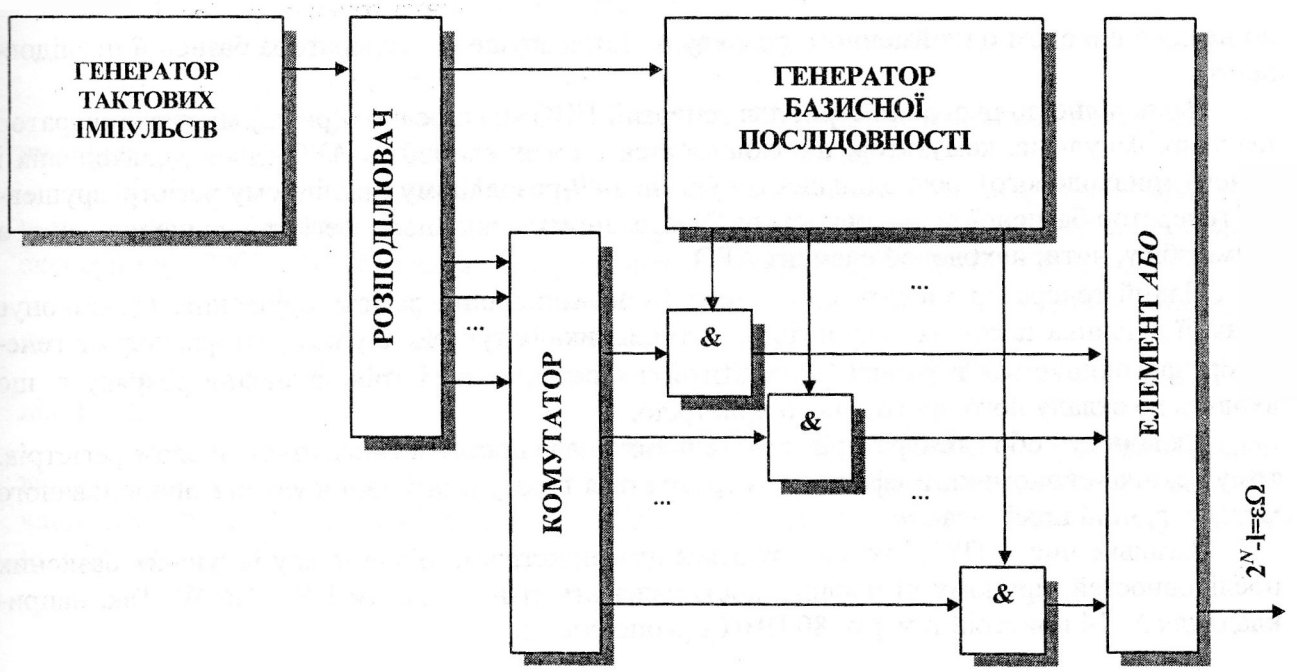

Рис.1. Структурна схема генератора ПВП GMW

При цьому, відповідно до особливостей структури ПВП GMW, комутатор проводить розбиття виходів розрядів регістра розподільника на певні групи, які відповідні різним розрядам регістра генератора базисної послідовності, а, отже, і різним зрушенням базисної послідовності. Це забезпечує формування сукупності з ε послідовностей із зрушень базисної та нульової.

Перші ε двійкових символів послідовності, що генерується, співпадають зі всіма першими двійковими символами сформованої сукупності. Наступні ε двійкових символів – зі всіма другими двійковими символами тієї ж сукупності і т.д. В результаті такої циклічної процедури в пристрої формуються всі 2^N-1=εΩ двійкових символів ПВП GMW.

Щоб зрозуміти роботу пристрою, розглянемо генерацію ПВП GMW значності 63 [3]. Ця послідовність має вигляд: 1010001101011001101000111010001000000011111011100111101 0010011011, і відповідає GMW-різницевій множині з параметрами ν=63, k=32, λ=16 і створюючим поліномом $\Omega(x) \equiv (1+x^2y^6+x^3y^3+x^4y^4+x^5y^4+x^6+x^7y^6+x^8y^4) \bmod (x^{63}-1)$, де $y=x^9$. У загальному випадку члени полінома $\Omega(x)$ містять всю інформацію про структуру комутатора 6 пристрою, а саме:

– члени з різними ступенями «у» відповідають різним елементам АБО комутатора;

– члени з однаковими ступенями «у» відповідають входам одного елементу АБО комутатора;

– вихід певного розряду розподільника з'єднується з певним входом одного з елементів АБО комутатора таким чином, що вихід розряду з номером на одиницю більшим показника ступеня «х», з'єднується з входом елементу АБО, відповідного ступеню «у» в члені, що містить цей ступінь «х»;

– вихід кожного елементу АБО підключається до входу схеми збігу з номером, на одиницю більшим величини показника відповідного ступеня «у».

При цьому слід мати на увазі, що одновходові елементи АБО, передбачувані даним описом комутатора, насправді відсутні. Тому розряди розподільника, відповідні цим одновходовим елементам АБО, підключаються безпосередньо до входів схем збігу. Кожна схема збігу (а число таких схем, як випливає з опису комутатора, може бути менше Ω), з'єднується

по входу з виходом однойменного розряду регістра зрушення генератора базисної послідовності.

Відповідно до цього пристрій для генерації ПВП значності 63 (рис.2) містить генератор тактових імпульсів, комутатор, що складається з трьох елементів АБО (двох двовходових і одного тривходового), розподільник імпульсів на 9-розрядному циклічному регістрі зрушення, генератор базисної послідовності на 7-розрядному циклічному регістрі зрушення, чотири схеми збігу, чотиривходовой елемент АБО.

Даний генератор містить один ε-розрядний циклічний регістр зрушення, що виконує функції дільника тактових імпульсів і розподільника імпульсів для комутатора, тоді як генератор, що описується в роботі [4], містить m циклічних регістрів зрушення розряду ε, що входять до складу його програмного пристрою.

Складність обох генераторів при великих значеннях N визначається числом регістрів, тому техніко-економічний ефект, що отримується в результаті застосування пропонованого методу, рівний приблизно m.

Загальне число ПВП, які генеруються цим пристроєм, рівне числу існуючих базисних послідовностей, причому ці послідовності належать різним класам ПВП GMW. Так, наприклад, для N=14 пристрій генерує 80 ПВП з різних класів.

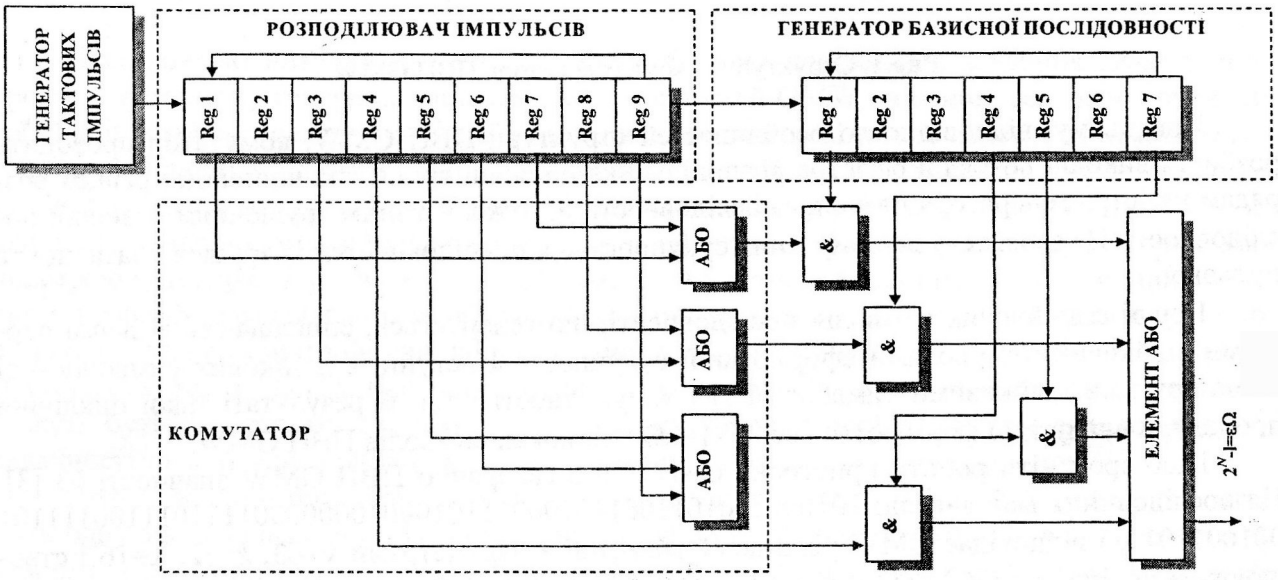

Рис.2. Пристрій для генерації ПВП GMW значності 63

Описаний генератор має наступну особливість: якщо регістри розподільника імпульсів і генератора базисної послідовності формувача зробити реверсивними, то число ПВП, які генеруються, може бути збільшене удвічі. При цьому якщо зрушення інформації у вказаних регістрах відбувається вправо, пристрій генерує одні псевдовипадкові послідовності, а при зрушенні вліво генерує інші ПВП, «зворотні» до перших. Можливість генерації «зворотних» копій ПВП GMW без якої зміни в інформації, що знаходиться в регістрах цього пристрою, обумовлена властивістю ПВП, які будуються на основі різницевих множин [5]. У відповідність з цією властивістю перетворення, що міняє порядок проходження всіх елементів початкової ПВП, окрім першого, на протилежний, приводить до утворення ПВП з того ж класу, але відмінної від початкової.

Висновок. Пропонований пристрій для генерації ПВП GMW, який дозволяє роботу регістрів у реверсному режимі, дає можливість додаткового отримання ще 80 форм ПВП.

Список літератури

1. *Головань В.Г., Казакова Н.Ф.* Послідовність GMW на основі слідів полів Галуа / Захист інформації. – К.: ДУІКТ. – Спец. випуск (40), 2008. – С.95-100.

2. *Сукачев Э.А., Казакова Н.Ф.*, Чуприна А.А. Синтез сигнальных функций для цифровой радиосвязи // Матер. III Міжнар. наук.-практ. конф. «Наукові дослідження – теорія та експеримент-2007», 14-16 травня 2007 р., Полтава: Інтер-Графіка, 2007. – Т.7. – С.54-57.

3. *Кренгель Е.И.* О числе псевдослучайных последовательностей Гордона, Милза, Вёлча. – Техника средств связи, Сер. ТРС, вып. 3, 1979.

4. *Golomb S.W.* Shift register sequences. – AEGEAN PARK PRESS, Laguna Hills, California, 1982.

5. *Кренгель Е.*И. Исследование и разработка новых классов псевдослучайных последовательностей и устройств их генерации для систем с кодовым разделением каналов. – Дис. канд. техн. наук: 05.12.13: Москва. – М.: РГБ. – 2000 (Из фондов Российской государственной библиотеки).

УДК 621.396.946; 621.391.001.12

О.О. Скопа, В.І. Гура
Міжнародний гуманітарний університет

СИНТЕЗ ПОХІДНИХ СИСТЕМ СИГНАЛІВ НА ОСНОВІ ПВП GMW, ЩО ВОЛОДІЮТЬ ВЛАСТИВОСТЯМИ ОРТОГОНАЛЬНОСТІ

Сучасний період розвитку широкосмугових систем зв'язку супроводжується бурхливим зростанням числа робіт, присвячених пошуку нових систем ортогональних сигналів, використовуваних в цих системах для розширення спектру і каналостворення [1]. Системи ортогональних сигналів будуються на основі ансамблів ортогональних кодових псевдовипадкових послідовностей, основними вимогами до яких є [2]:

1) великий ансамбль послідовностей, що формуються за допомогою єдиного алгоритму;

2) хороші кореляційні властивості послідовностей ансамблю;

3) збалансованість структури;

4) велика лінійна складність або непередбачуваність символів послідовностей.

В даний час в системах зв'язку з CDMA широкого поширення набули ортогональні системи сигналів на основі циркулянтних матриць Адамара і системи функцій Уолша, які є матрицями Адамара порядку 2^N. Відомо [3], що системи ортогональних сигналів на основі матриць Адамара, в цілому характеризуються поганими авто- і взаємокореляціними функціями (АКФ і ВКФ відповідно), що приводить до зростання міжканальних інтерференційних перешкод в приймачі. Тому на практиці з метою зменшення рівня інтерференційних перешкод доцільніше використовувати похідні ортогональні системи сигналів [4, 5], що мають відносно кращі взаємнокореляційні характеристики. Нагадаємо, що похідний сигнал синтезується в результаті посимвольного перемножування двох сигналів. Відповідно система, складена з множини похідних сигналів, називається *похідною*. Серед похідних систем сигналів великого поширення набули системи, що будуються таким чином:

Як перший співмножник береться деяка ортогональна система сигналів, послідовності якої не задовольняють вимогам на кореляцію, проте володіють певними перевагами з погляду простоти їх формування і обробки. Це так звана *початкова система сигналів*. Потім як другий співмножник вибирається базисний широкосмуговий сигнал з відносно малими біч-