в кореляційному спектрі в точності рівне числу класів суміжності. Воно може бути і меншим як, наприклад, у разі трирівневих *m*-послідовностей.

Висновок. Для дослідження взаємокореляційних властивостей послідовностей, побудованих на основі різницевих множин типу Адамра, розроблений метод ізоморфних коефіцієнтів, який дозволяє істотно прискорити їх розрахунок на ЕОМ і, отже, побудову ФМ-систем з заданими кореляційними властивостями. Перспективним шляхом подальших досліджень є аналіз застосування запропонованого методу для дослідження взаємокореляційних властивостей послідовностей, які не є різницевими множинами типу Адамра.

Список літератури

1. *Кренгель Е, И.* Метод исследования корреляционных функций периодических последовательностей. – Техника средств связи, сер. ТРС, вып.3, 1980.

2. *Свердлик М.Б.* Оптимальные дискретные сигналы. – М.: Советское радио, 1975.

3. *Виноградов И. М.* Основы теории чисел. – М.: Наука, 1972.

4. *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 519.72:621.391.037.372; 621.396.946

К.Б. Нікіфоренко
ДП «Київський коледж зв'язку»
Н.М. Согіна
ДАТ КБ «Дніпровське»

ДИФЕРЕНЦІЮВАННЯ ВИМОГ, ЩО ПРЕД'ЯВЛЯЮТЬСЯ ДО ГЕНЕРАТОРІВ ПВП, ВИКОРИСТОВУВАНИХ В СТІЛЬНИКОВИХ СИСТЕМАХ ЗВ'ЯЗКУ

Основні положення, які торкаються декомпозиції вимог, що пред'являються до датчиків випадкових і псевдовипадкових чисел, на основі класифікації спеціальних даних, приведені [1...4]. В зазначених джерелах також можна знайти вимоги і до генераторів псевдовипадкових кодових послідовностей (ПВП), які побудовані на основі зазначених датчиків. Проте, слід зазначити, що в згаданих роботах аналіз і систематизація вимог виконані стосовно такої області техніки, як криптографічні методи захисту інформації в технічних системах. Разом з тим сформульовані вимоги достатньо легко переносяться на інші сфери, у тому числі і на алгоритми і пристрої генерації ПВП для систем зв'язку з кодовим розділенням каналів. Численні дослідження, наприклад [5...8], показують, що побудова хороших генераторів випадкових (ВП) і ПВП є не простим завданням. У системах зв'язку з кодовим розділенням каналів, ПВП, як вже наголошувалося, є основою для побудови підсистем управління ключовими структурами, одним з основних завдань якої є формування спеціальних даних.

Різноманітність вирішуваних за допомогою ПВП завдань (для синхронізації роботи крайових пристроїв радіотракту, для ідентифікації абонентських терміналів, безпосередньо для передачі корисної інформації, а також криптозахисту даних) вимагає сумісного застосування в єдиній системі відмінних за природою алгоритмів. Це, у свою чергу, приводить до використання різних спеціальних даних. Очевидно, що алгоритм формування ПВП за умовчанням має на увазі його скритність і високу криптозахищеність. З урахуванням цього для кожного криптографічного перетворення (тобто формування ПВП) потрібні характерні спе-

ціальні дані і, т.ч., засоби формування цих даних дещо розрізнятимуться і задовольнятимуть не співпадаючим між собою вимогам. Це все говорить про те, що система управління ключовими структурами повинна забезпечити формування різних спеціальних даних одночасно. Стосовно даних питань до них віднесемо:

– Двійкові вектора: послідовності біт обмеженої довжини – можуть генеруватися як генератором випадкових, так і псевдовипадкових чисел;

– Шифрувальні гамми: псевдовипадкові двійкові (або m-ічні) послідовності з великим періодом і статистичними характеристиками, близькими до випадкових;

– Прості числа: вибираються випадковим чином з множини простих чисел заданої розрядності і задовольняють ряду вимог, описаних [8...10]*;*

– Первісні елементи: вибираються випадковим чином з множини первісних елементів заданого простого числа.

У [3] є ще ряд вимог до ВП і ПВП, проте вони мають специфіку, направлену на створення криптографічних алгоритмів і тут не приводяться. Т.ч. видно, що, не дивлячись на широкий спектр спеціальних даних, в основі процесу їх формування лежить використання генераторів ВП і ПВП.

Природно, що ПВП практично ніколи не використовуються як спеціальні дані в чистому вигляді, а піддаються певним перетворенням. У зв'язку з цим вимоги, що пред'являються до генераторів ПВП, розбиті на три рівні залежно від ступеня наближення ПВП до власне спеціальних даних.

На самому нижньому рівні розміщені генератори ВП і ПВП. На цьому рівні їх ефективність характеризується множиною показників $W=\{w_1, w_2, ..., w_m\}$. Вимоги, що пред'являються до генераторів на цьому рівні, а також множина показників W в [3] названі *базовими*, оскільки вони не залежать від того, для яких алгоритмів використовуватимуться генератори.

Базові показники характеризують закон розподілу формованих послідовностей, їх незалежність і випадковість, а також технічні характеристики пристроїв і програм (швидкість формування чисел, складність реалізації пристрою і т. д.). Дані показники можуть бути розроблені або сформовані на основі використання апарату математичної статистики теорії складності.

Генератори ПВП і формовані ними послідовності повинні володіти специфічною властивістю – *криптографічною стійкістю*. Криптографічна стійкість характеризує здатність алгоритмів формування ПВП протистояти криптоаналізу, направленому на розкриття закону формування ПВП.

Множина показників $S=\{s_1, s_2, ..., s_n\}$, що характеризують стійкість генератора ПВП, доцільно виділити в окрему групу і розташувати їх на наступному рівні. Тут показники характеризують непередбачуваність, структурні властивості, безпечний час, лінійну еквівалентну складність ПВП [11]. Застосування методів і засобів, які забезпечують необхідний рівень криптографічної стійкості, не повинно погіршувати базові показники. На цьому рівні відбувається деяке розділення множини показників S, оскільки для генераторів псевдовипадкових чисел різних класів оцінка криптографічної стійкості здійснюється з використанням різних показників.

Нарешті на третій рівень можна віднести множину показників, що характеризують ступінь задоволення вимог, які пред'являються умовами реалізації конкретного алгоритму. Тут доцільно виділити множини $R=\{r_1, r_2, ..., r_n\}$ показників, що відносяться до конкретного класу спеціальних даних, причому ці множини, в загальному випадку, не перетинаються. Очевидно, що для генерації таких спеціальних даних як перестановки, прості числа, первісні елементи необхідно використовувати спеціальні генератори.

Висновок. У системах зв'язку з кодовим розділенням каналів ПВП є основою для по-

будови підсистем управління ключовими структурами. Проведене диференціювання вимог до ПВП дозволяє отримати попередню оцінку вимог до таких підсистем, одним з основних завдань яких є формування спеціальних даних.

Список літератури

1. *Корчинский В.В., Филькин К.М.* О выборе первичного датчика для задач имитационного моделирования // Моделювання та інформаційні технології. Збірн. наук. праць ІПМЕ. – Вип. 42. – Львів: Львівська політехніка, 2007. – С. 81-90. Филькин К.М. Критерии выбора ансамблей псевдослучайных последовательностей для систем связи с кодовым разделением каналов // Вісник УНДІЗ / Матер. X Міжнар. наук.-практ. конф. «Еволюція транспортних мереж телекомунікацій. Проблеми побудови, розвитку та управління». – Ялта, 28-30 травня 2008 р. – С.43-45.

2. *Корчинский В.В., Филькин К.М.* Анализ моделей первичных датчиков псевдослучайных чисел / Матер. II наук.-практ. семін. молодих науковців та студентства «Сучасні телекомунікаційні та інформаційні технології», 12-14 грудня 2007 р., Київ: УНДІЗ. – С.20-24.

3. *Потий А.В., Пестерев А.К., Олейников Р.В.* Декомпозиция требований, предъявляемых к генераторам случайных и псевдослучайных чисел, на основе классификации специальных данных // Ювілейна наук.-техн. конф. «Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні», Київ, 1998.

4. *Филькин К.М.* Обобщение требований к сигналам, используемым для передачи дискретных сообщений // Матер. II звітної наук.-практ. конф. проф.-викл. складу та студентства Міжнар. гуманіт. ун-ту, 12 квітня 2007 р., Одеса: Міжнар. гуманіт. ун-т, 2007. – С.21-22.

5. *Ritter T.* The Efficient Generation of Cryptographic Confusion Sequences. – Criptologia, V. XV, No.2, 1991, p. 81-139.

6. *L'Ecuyer, Proulx R.* About Polynomial-time «unpredictable» generators [Электронный ресурс]: http//www. iro.umontreal.ca/~lecuyer

7. *Bellare M., Goldwasser S.* «Pseudo-Random» Number Generation within Criptographic Algorithms: the DSS Case. – Advances in Cryptology, CRYPTO 97, Lecture Notes in Computer Science, Springer Verlag, 1997.

8. *Schneier B.* Applied Cryptography, Second Edition. – New York, John Wiley & Sons, Inc., 1996, p.760.

9. *Горбенко И.Д., Долгов В.И., Потий А.В., Федорченко В.Н.* Анализ каналов уязвимости системы RSA // Безопасность информации, 1995, №2. – С.22-26.

10. *Горбенко И.Д., Долгов В.И., Рублинецкий В.И., Коровкин К.В.* Методы защиты информации в системах телекоммуникаций и методы их криптоанализа // Радиотехника. – Всеукр. межвед. научн.-техн. сб. – 1997, Вып. 104. – С.138-150.

11. *Simon M.K., Omura J.K., Scholtz R.A., Levit B.K.* Spread spectrum communications handbook. – McGraw-Hill, Inc., 1994.