Бабич, О.Д. Кувшинов, О.П. Лежнюк, С.П. Лівенцев // К. : КВІУЗ, 2001. - 150 с.

2. Хмельницький Ю.В. Забезпечення вірогідної передачі інформації при впливі перешкод в телекомунікаційних мережах / Ю.В Хмельницький, Г.Б.Жиров, Н.В. Кульпак // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2018. – Вип. № 59. – С. 161-170.

3. Хмельницький Ю.В Методи та засоби забезпечення завадостійкої передачі інформації в телекомунікаційних мережах / Ю.В Хмельницький, О.А. Каблуков, Л.О. Ряба, Л.В. Солодєєва, А.О. Ткач // Збірник наукових праць Військового інституту Київського нац. університету імені Тараса Шевченка. - К.: ВІКНУ, 2019. - № 64. – 133-144 с.

Оцінка ефективності роботи генератора криптоключів підвищеної ентропії для системи клієнт-банк

Чешун В.М., Чорненький В.І.[1], Яцків В.В.[2]
Хмельницький національний університет [1]
Західноукраїнський національний університет[2]

Після виконаної розробки засобів реалізації алгоритму роботи системи клієнт-банк із застосуванням генераторів криптоключів підвищеної ентропії, важливим етапом стає апробація здатності засобів, що реалізують алгоритм, виконувати передбачені функції відповідно до наявних вимог.

Розроблені алгоритм і засоби орієнтовані на накопичення пулу ентропії від джерел з передачею даних в систему клієнт–банк. Парадокс оцінки ентропії полягає в тому, що вона потребує зазначення того, наскільки непередбачувана послідовність. Якби можна було зробити абсолютний доказ непередбачуваності, то за визначенням послідовність була б передбачуваною.

Слід зазначити, що далеко не всі гіпотези про підвищену ентропію застосовуваних джерел і отримуваних на їх базі даних проходять перевірку на відповідність вимогам випадковості значень, тому черговою задачею дослідження постає оцінка якості отримуваного від джерел ентропії пулу тестами на випадковість.

Перевірка якості генерованих різними методами чисел на випадковість є однією із найактуальніших і найскладніших задач при розробці і впровадженні генераторів псевдовипадкових чисел.

Актуальність задачі зумовила до активного пошуку її розв’язку, а складність – до відсутності єдиного універсального рішення.

Як наслідок, на сьогоднішній день розроблено велику кількість методів перевірки якості послідовностей псевдовипадкових чисел, що

базуються на різних принципах [1, 2]:

- графічні тести;
- евристичні тести;
- статистичні тести.

Графічні тести [1] відображують властивості послідовностей графічними залежностями (графіками або просторовими моделями: гістограма розподілу елементів послідовності, розподіл на площині, графіки перевірки на монотонність), з аналізу яких робляться висновки щодо характеристик досліджуваних послідовностей.

Евристичні тести [2] формують відносну оцінку кількох версій генераторів, висновок дається за результатами порівняння або за гіпотезами оцінювання.

Статистичні тести [1, 2] вишукують в послідовностях повторювану складову і дають оцінки якості генератора за її статистичними властивостями.

Згідно [1], статистичні тести на основі оціночних критеріїв роблять висновки про ступінь близькості властивостей аналізованої і істинно випадкової послідовності. На відміну від графічних і евристичних тестів, де результати інтерпретуються користувачами або базуються на випадкових вибірках (тест днів народження, мавпячий тест тощо), в результаті чого можливі відмінності в трактуванні результатів, статистичні тести характеризуються тим, що вони видають чисельну характеристику, яка дозволяє однозначно сказати, пройдений тест чи ні.

З цього слідує перевага статистичних тестів відносно графічних і евристичних.

До категорії статистичних тестів можна віднести наступні популярні тести [1, 2, 3, 4, 5]:

– тести Кнута – один з перших наборів статистичних тестів, запропонований Д. Кнутом в 1969. Тести обчислюють значення статистики, воно порівнюється з табличними результатами. Залежно від ймовірності появи отриманої статистики робиться висновок про її якість. Перевага тестів – мала кількість і швидкі алгоритми виконання. Недолік – невизначеність трактування результатів.

– тести Diehard – набір тестів для вимірювання якості набору випадкових чисел. Набір Diehard з 14 тестів Джорджа Марсалі був першим для комплексного тестування генераторів, розроблявся декілька років і опублікований в 1995р. Тести Diehard розглядаються як один з найбільш суворих існуючих наборів тестів, але і їм притаманний ряд недоліків [Шевч]:відсутній докладний опис тестів і методика трактування результатів; параметри тестування жорстко задані, через що тести не адаптовані для перевірки послідовностей різних розмірів; більшість тестів є наближеними і засновані на результатах емпіричних випробувань, а не на статистичних

моделях;

– набір статистичних тестів Crypt-X розроблений дослідниками науково-дослідного центру з інформаційної безпеки технологічного університету Квінсленда (Австралія). Це комерційний пакет програмного забезпечення. Тести застосовуються в залежності від типу алгоритму генератора і спрямовані на тестування генераторів псевдовипадкових чисел. Підтримуються потокові шифри, блокові шифри, генератори потоку ключів. У набір включені наступні тести: частотний, на послідовність однакових бітів, лінійна складність, складність послідовності, двійкова похідна, зміна точки. Основний недолік для даної роботи – відсутність детального опису тестів та комерційна основа розповсюдження.

– тести NIST – перший крок до стандартизації набору статистичних тестів (в 1994р. в національному стандарті США «Вимоги безпеки до криптографічних модулів»). Однак вимоги і методика стандарту носили більше технологічний характер. У 1999 р фахівцями NIST (Національний інститут стандартів і технологій (ність) США), в рамках проекту AES (Advanced Encryption Standard) був розроблений набір статистичних тестів «NIST STS» (NIST Statistical Test Suite) і запропонована методика проведення статистичного тестування генераторів, орієнтованих на використання в задачах криптографічного захисту інформації, яка, на погляд багатьох фахівців в даній області, на даний момент найкращим чином відповідає потребам всіх зацікавлених сторін. Пакет NIST STS включає в себе 15 статистичних тестів, які розроблені для перевірки гіпотези про випадковість послідовностей довільної довжини. Всі тести спрямовані на виявлення різних дефектів випадковості;

– тести стандарту FIPS140 є складовою стандарту FIPS (федеральний стандарт по обробці інформації) – державного стандарту США, що описує вимоги до шифрування і пов'язаних з ним заходів безпеки IT-продуктів, які використовуються для обробки конфіденційної інформації без грифу секретності. FIPS 140-1 був випущений в 1994 році, йому на зміну прийшов стандарт FIPS 140-2 в 2001 році, а в 2019 році з’явився FIPS 140-3 – це нова версія стандарту, актуальна на сьогодні.

Це далеко не повний перелік тестів, але достатній для формування уяви про тенденції розвитку методів тестування і прийняття рішення щодо вибору одного з методів.

За результатами проведеного аналізу можна зробити висновок про доцільність вибору статистичних тестів, які найкраще себе зарекомендували і стали стандартами перевірки якості генераторів псевдовипадкових чисел.

Найновішим стандартом тестування псевдовипадкових послідовностей є стандарт FIPS 140-3, виданий у 2019 році. Новизна стандарту зумовлює відсутність його перекладів та програмних реалізацій тестерів. Тому в апробації алгоритму роботи системи клієнт-банк із

застосуванням генераторів криптоключів підвищеної ентропії застосуємо аналітичне дослідження властивостей генерованих алгоритмом даних на відповідність вимогам FIPS 140-3.

Тести стандарту FIPS140 виконуються над послідовностями довжиною 20000 біт і включають 4 тести:

- монобітний тест;
- блоковий тест (тест покеру);
- тест серій;
- тест довжин серій.

Для проведення випробувань обрано фрагмент пулу ентропії довжиною 20000 біт, сформований розробленим програмним додатком на підставі накопичення ентропії з датчиків мобільного телефону.

Монобітний тест полягає в підрахунку кількості нулів і одиниць в послідовності певної довжини. Тест вважається пройденим, якщо кількість нулів (n_0) і одиниць (n_1) лежить в діапазоні від 9654 до 10346.

За результатами статистичного аналізу тестованої послідовності отримуємо:

- n_0=9996, $9654 < n_0 < 10346$;
- n_1=10004, $9654 < n_1 < 10346$.

З отриманих результатів робимо висновок – монобітний тест успішно пройдено.

Блоковий тест (тест покеру) полягає в наступному. Потік даних довжиною 20000 біт розбивається на чотирьохрозрядні двійкові коди (5000 кодів по 4 біта кожен), після чого виводиться статистика появи кожного коду. Статистичні дані підставляються в формулу:

$$X = \frac{16}{5000} * \sum_{i=0}^{15} K_i - 5000\,, \qquad (1)$$

де K_i – кількість входжень коду зі значенням i в тестовану послідовність (для чотирьохрозрядних кодів $0 \le i \le 15$).

Блоковий тест вважається пройденим, якщо розрахункове значення попадає в діапазон від 1,03 до 57,4.

В деяких джерелах [5] зазначається, що статистичні характеристики розбиття можуть змінюватися при зсуві вхідного коду, тому для якісної оцінки потрібно дослідити всі 4 варіанти розбиття з циклічним зсувом тестованого коду пулу ентропії довжиною 20000 біт (після четвертого зсуву статистичні дані будуть циклічно повторюватися з кожним зсувом).

Результати експерименту наведені в таблиці 1.

За даними експериментів (Експ. 1-4), наведеними в таблиці 1, побудовано гістограми статистичних даних кількості входжень i-го коду в послідовність даних пулу ентропії (рис. 1-4).

Таблиця 4.1 – Результати блокового тесту (4 можливих варіанти)

i	*i*-й код	Статистичні дані кількості входжень *i*-го коду в послідовність даних пулу ентропії			
		Експ. 1: зміщення 0	Експ. 2: зміщення 1	Експ. 3: зміщення 2	Експ. 4: зміщення 3
0.	0000	304	309	306	292
1.	0001	306	305	304	332
2.	0010	289	287	311	281
3.	0011	362	336	310	342
4.	0100	301	294	319	308
5.	0101	321	315	310	325
6.	0110	300	298	307	261
7.	0111	326	365	309	361
8.	1000	310	301	318	318
9.	1001	316	316	319	319
10.	1010	319	343	322	341
11.	1011	301	280	312	284
12.	1100	316	343	318	318
13.	1101	302	320	315	295
14.	1110	363	335	306	357
15.	1111	264	255	314	266

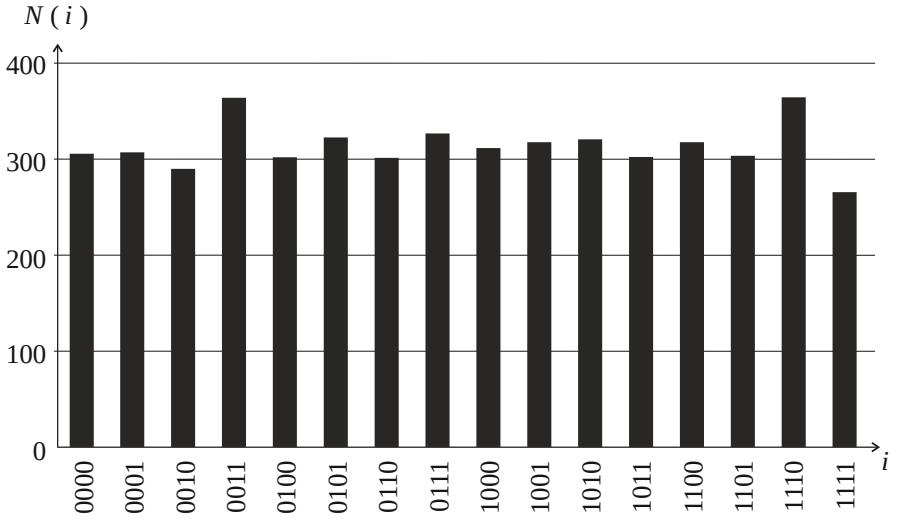

Рисунок 1 – Гістограми статистичних даних кількості входжень *i*-го коду в послідовність даних базового пулу ентропії без зміщення

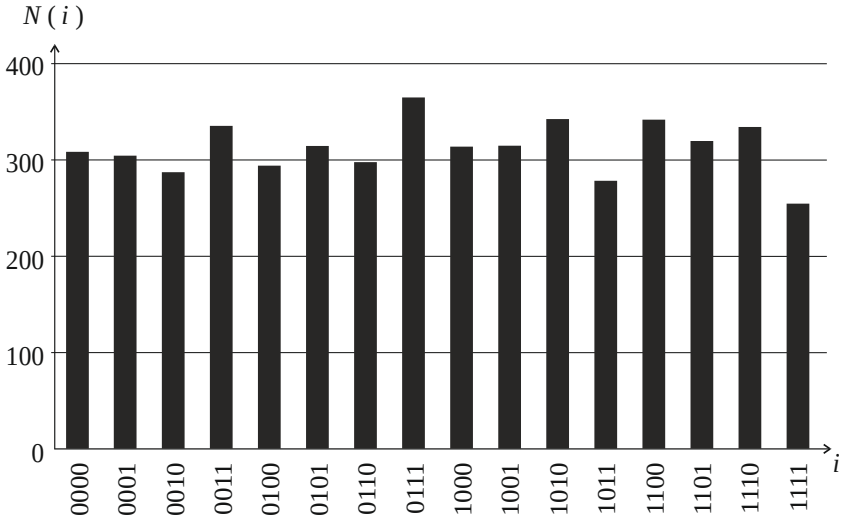

Рисунок 2 – Гістограми статистичних даних кількості входжень *i*-го коду в послідовність даних пулу ентропії зі зміщенням пулу на 1 розряд

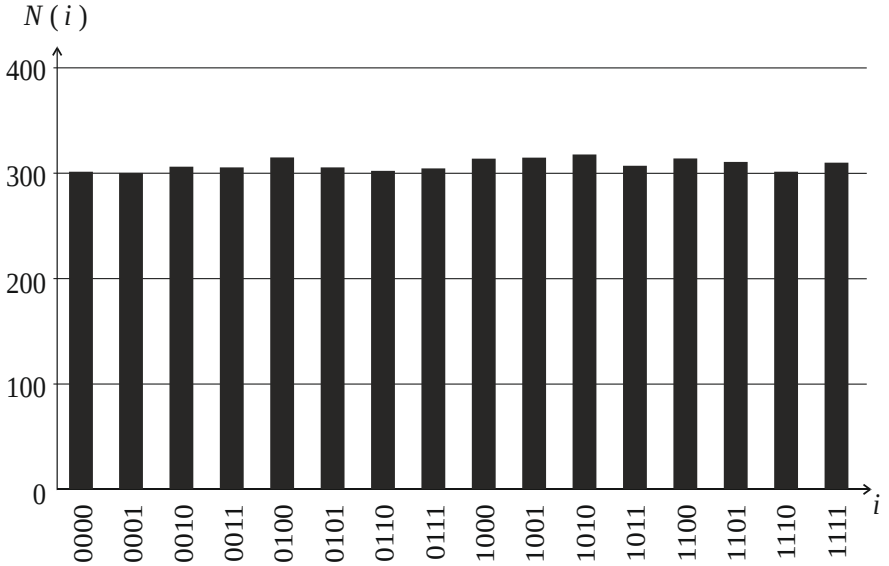

Рисунок 3 – Гістограми статистичних даних кількості входжень *i*-го коду в послідовність даних пулу ентропії зі зміщенням пулу на 2 розряди

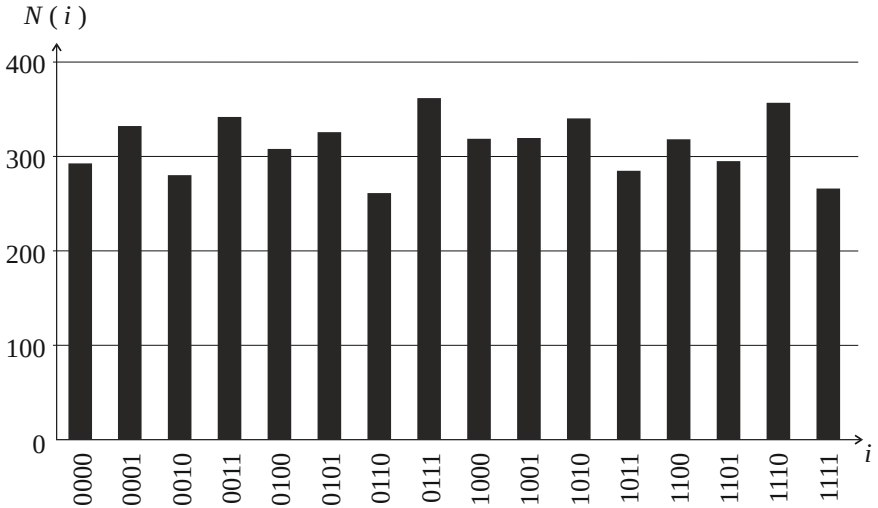

Рисунок 4 – Гістограми статистичних даних кількості входжень *i*-го коду в послідовність даних пулу ентропії зі зміщенням пулу на 3 розряди

За даними таблиці 1 маємо наступні розрахункові дані показника X_j (*j* - номер експерименту):

– експеримент 1: X_1=28.4096, 1,03 < X_1 < 57,4;
– експеримент 2: X_2=40,8512, 1,03 < X_2< 57,4;
– експеримент 3: X_3=1.4656, 1,03 < X_3 < 57,4;
– експеримент 4: X_4=44,864, 1,03 < X_4 < 57,4.

З отриманих результатів висновок – блоковий тест успішно пройдено.

Тест серій – базується на підрахунку кількостей послідовностей (серій) однакових символів (нулів або одиниць) в послідовності. Послідовність вважається випадковою, якщо появи серій певної довжини лежить в заданих діапазонах. Послідовності довжиною більше 6 біт розглядаються як серія довжиною 6 біт. Результати виконання тесту наведені в таблиці 2 (окремо для серій одиниць і нулів). Діапазони оцінки нижньої і верхньої допустимої межі взято з [4].

Таблиця 2 – Результати тесту серій

Дані серій	Розрядність серії				
	2 біти	3 біти	4 біти	5 біти	6 біт
Нижня межа	2267	1079	502	223	90
Серії нулів	2328	1414	618	335	191
Серії одиниць	2279	1307	613	314	135
Верхня межа	2733	1421	748	402	223

З наведених в таблиці 2 результатів може бути зроблено висновок – тест серій успішно пройдено.

Заключним і одним із найпростіших є тест довжин серій. Даний тест визначає максимальну допустиму серію нулів або одиниць в послідовності Якщо послідовність випадкова, то максимальна довжина серії не повинна перевищувати 34 розряди [проц], оскільки ймовірність появи такої серії у випадковому потоці дуже низька.

Дослідження пулу ентропії показали, що довжина серії нулів l_0 і одиниць l_1 мають наступні характеристики: l_0=12, l_0<34, l_1=11, l_1<34.

З отриманих результатів робимо висновок – тест довжин серій успішно пройдено.

Оскільки тести стандарту FIPS140 включають 4 тести, кожен з яких для досліджуваного значення пулу ентропії, отриманого на підставі алгоритму роботи системи клієнт-банк із застосуванням генераторів криптоключів підвищеної ентропії, пройдено, то можна стверджувати, що тести стандарту FIPS140 в дослідженні пройдено.

Тести стандарту FIPS140 є дійсними на сьогоднішній день, але зазнають певної критики через малу кількість тестів і невелику складність деяких з них. Зокрема, наголошується на більшій складності тестів вільного доступу.

Дійсно, для реалізації тестів розроблено ряд програмних продуктів, частина яких є доступною як інтернет-ресурс:

– програма Statistica компанії StatSoft містить тести для перевірки приналежності послідовності заданому розподілу;

– програма Statistics Toolbox / Hypothesis Tests в програмі MathLab містить

– функції тестування статистичних гіпотез;

– NIST Statistical Test Suite – тестування на відповідність NIST;

– TEST-U01 – пакет статистичних емпіричних тестів, реалізований на мові ANSI C;

– CRYPT-X – містить частотний тест, тест підпослідовностей, тест перевірки лінійної складності. В комерційному варіанті має 10 тестів;

– The pLab Project – набір тестів (деталізація відсутня);

– Diehard – класичні тести Diehard (14 тестів, в тому числі тест дні народження, тест пересічні перестановки, тест ранги матриць, мавпячі тести, тест підрахунок одиничок, тест на парковку, тест на мінімальну відстань, тест випадкових сфер, тест стиснення, тест пересічних сум, тест послідовностей, тест гри в кості тощо);

– Dieharder – альтернативна реалізація тести Diehard.

Серед перелічених продуктів тестування послідовностей на випадковість найбільшу кількість тестів (15) реалізує тест NIST Statistical

Test Suite, який вважається найбільш повним статистичним тестом. Це стало підставою для вибору цього тесту.

Тест пройдено онлайн на сайті https://randomness-tests.fi.muni.cz/, настроювання програми тестування, використані для проходження тесту, наведено на рис. 5.

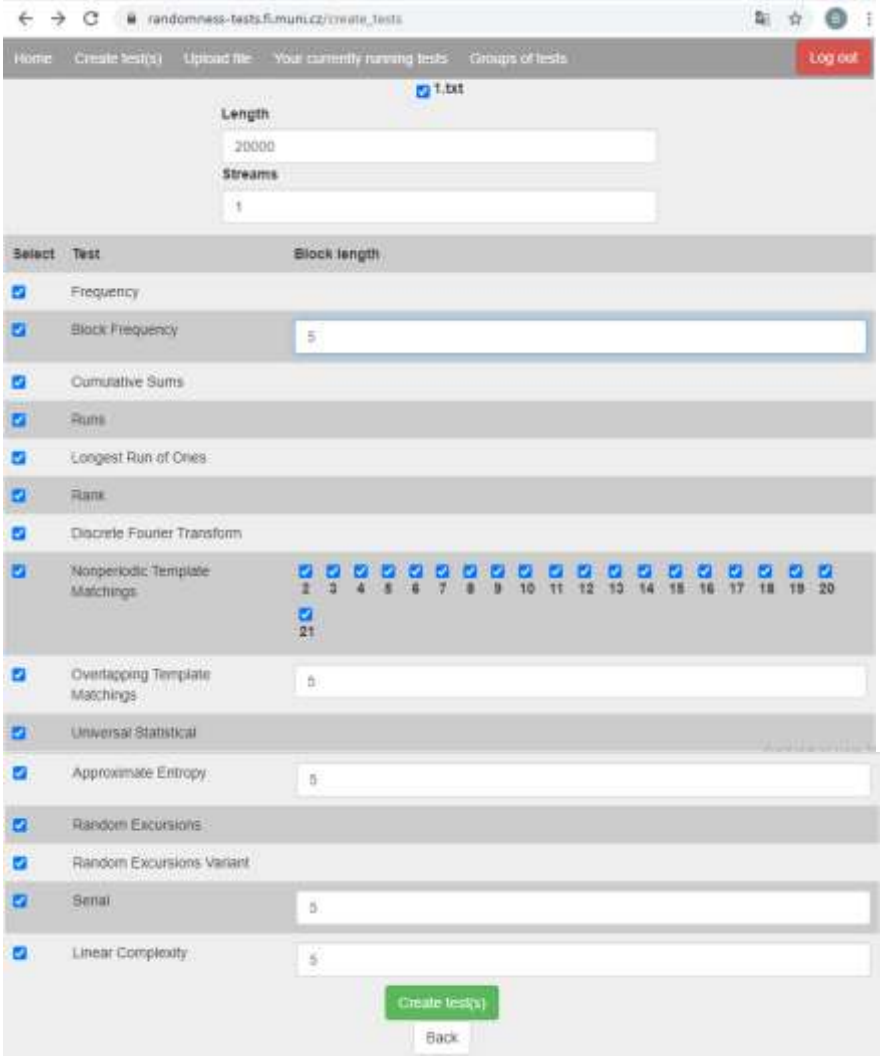

Рисунок 5 – Настройки програми проходження тесту на випадковість за стандартом тестування NIST STS

З рисунку 5 видно, що кількість різновидів тестів 15, але частина тестів дозволяє настроювання параметрів довжин серій або інших параметрів, що дозволяє значно посилити якість тестування і достовірність висновку.

Загалом результати випробувань пулу ентропії на випадковість складалися загалом з 209 тестів. Всі тести успішно пройдено, що свідчить про досягнення очікуваного результату при розробці і апробації алгоритму роботи системи клієнт-банк із застосуванням генераторів криптоключів підвищеної ентропії та засобів його реалізації.

Перелік посилань

4. Григорьев А. Ю. Методы тестирования генераторов случайных и псевдослучайных последовательностей / Григорьев А. Ю. // Ученые записки УлГУ. Сер. Математика и информационные технологии. – 2017. – № 1. – С. 22-28.

5. Слеповичев И.И. Генераторы псевдослучайных чисел / И.И. Слеповичев Саратов: СГУ, 2017. – 118 с.

6. Шевченко Д.Н. Методика тестирования и использования генераторов псевдослучайных последовательностей / Д.Н. Шевченко, С.В. Кривенков // Проблемы физики, математики и техники, № 2 (19), 2014

7. Проценко А.Г. Тестирование генераторов псевдослучайных чисел систем программирования на основе стандарта FIPS140-1 / А.Г. Проценко, И.В. Лысенко // Системи обробки інформації, 2010, випуск 2 (83) 130-132.

8. Шелест М. Є. Експериментальне дослідження методу генерування тритових псевдовипадкових послідовностей для криптографічних застосувань / М. Є. Шелест, С. О. Гнатюк, Т. О. Жмурко, В. М. Кінзерявий, Х. І. Юбузова // Захист інформації. - 2017. - Т. 19, № 1. - С. 67-79.