2 Забазпечення комп'ютерної безпеки в інформаційних системах

УДК 691.321

МЕТОДИКА ПЕРЕВІРКИ НЕЗАЛЕЖНОСТІ СТАТИСТИЧНИХ ТЕСТІВ ПРИ НЕВІДОМИХ СТАТИСТИЧНИХ ВЛАСТИВОСТЯХ ГЕНЕРАТОРА ПОСЛІДОВНОСТЕЙ

Леонід Скрипник, Людмила Ковальчук, Віктор Бездітний*.
*Інститут спеціального зв'язку та захисту інформації НТУУ «КПІ», *ТОВ «НВФ «УНІС»*

Анотація: **Розглядається проблема побудови набору з незалежних статистичних тестів для оцінки криптографічних якостей генераторів випадкових послідовностей. Узагальнені отримані раніше результати.**
Summary: **The problem of building of sets of independent statistical tests for estimating of cryptographic qualities of random sequences and random number generators is considered and previous results are generalized.**
Ключові слова: **Статистичний тест, незалежність.**

І Вступ

Сфера застосування генераторів послідовностей випадкових величин (далі – ГПВВ) є надзвичайно широкою. Крім захисту інформації, можна назвати такі області застосування, як космічний зв'язок, коди, що виявляють та виправляють помилки, інші. В даній статті будуть розглянуті застосування, що відносяться до сфери захисту інформації [1, 2].

Реалізація майже кожного криптографічного механізму, як у симетричній, так і в асиметричній криптографії, вимагає наявності ГПВВ, що має певні властивості. Послідовності, отримані з такого генератора, використовуються в усіх процедурах захисту інформації: шифруванні, цифрового підпису, обміну ключами, для перевірки якості інших генераторів [1, 2].

Необхідною умовою стійкості криптосистеми є наявність певних криптографічних властивостей у генератора, що використовується для генерації її параметрів та ключових даних. У зв'язку з цим перед розробником або користувачем будь-якої криптосистеми постають питання як про оцінку якості генератора, так і про оцінку якості його окремих послідовностей.

Основним методом перевірки якості генератора є застосування до нього певних статистичних критеріїв. Існує досить багато наборів таких критеріїв, найбільш популярним серед них є [3] та [4]. Тести, що входять до цих наборів, перевіряють різні властивості вихідних послідовностей: рівноймовірність, розподіл серій, максимальну довжину серії, відсутність міжсимвольних залежностей, інші. Однак при цьому гостро постає питання про побудову такого набору, що містить лише незалежні тести. Дане обмеження пояснюється принаймні двома причинами: необхідністю зменшення часу тестування та необхідністю обчислення загальної помилки першого роду при прийнятті гіпотези про випадковість послідовності.

Означення незалежності статистичних тестів було введено раніше авторами даної роботи в [5], також у численних роботах було показано зручність його практичного застосування та розроблено відповідні методики перевірки незалежності тестів. Однак розроблені методики спирались на використання наступного припущення: імовірність того, що дана послідовність проходить відповідний статистичний тест, дорівнює рівню значимості цього тесту. Дане припущення вимагає, як мінімум, використання таких генераторів, що є нерозрізнювальні від ідеальних. Як такий генератор, наприклад, може використовуватись генератор, прописаний у додатку А до ДСТУ 4145-2002. Крім того, дана методика не може застосовуватись у багатьох випадках для тестів, що будуються з використанням комбінаторних міркувань (наприклад, тест серій максимальної довжини). Для деяких таких тестів ймовірність помилки першого роду не дорівнює імовірності проходження тесту послідовністю, а є лише її верхньою оцінкою. Тому на практиці дане припущення може виявитись обтяжливим.

В роботі запропоновано методику перевірки незалежності статистичних тестів з використанням ГПВВ з невідомими статистичними характеристиками.

II Базові поняття та позначення

Нехай $A = \{a_1, ..., a_m\}$ – деякий алфавіт, (Ω, P) – деякий імовірнісний простір, $x^{(i)} : \Omega \to A$, $i \geq 1$ – однаково розподілені випадкові величини, що розглядаються як виходи деякого ГПВВ, який і задає їх імовірнісний розподіл на A; $X = (x^{(1)}, ..., x^{(l)})$ – скінчена послідовність даних випадкових величин (випадковий вектор, або випадковий елемент на A^l). Нехай також T – деякий статистичний тест, призначений для перевірки криптографічних якостей послідовностей, $T : A^* \to \{0, 1\}$, де під A^* розуміємо всі можливі послідовності елементів з A довільної (скінченої) довжини.

Означення 1. Послідовність випадкових величин $X = (x^{(1)}, ..., x^{(l)})$ будемо називати випадковою, якщо $x^{(1)}, ..., x^{(l)}$ – незалежні випадкові величини, що мають рівноімовірний розподіл на A. Генератор, виходи якого утворюють випадкову послідовність, будемо називати генератором випадкових послідовностей (ГВП).

Зауваження 2. При фіксованому $\omega \in \Omega$ вектор $X(\omega) = (x^{(1)}(\omega), ..., x^{(l)}(\omega)) \in A^l$ є реалізацією послідовності випадкових величин $(x^{(1)}, ..., x^{(l)})$. Зокрема, аргумент статистичного тесту T можна розглядати як деяку реалізацію $X(\omega)$ послідовності випадкових величин X. Якщо $T(X(\omega)) = 1$, то кажуть «дана послідовність пройшла статистичний тест T», і за результатами тестування приймається гіпотеза H_0: «дана послідовність є реалізацією випадкової послідовності» (це основна гіпотеза тесту). Якщо $T(X(\omega)) = 0$, то приймається гіпотеза H_1, що є альтернативною до H_0.

Надалі будемо використовувати позначення X_i, $i \geq 1$, для послідовностей випадкових величин деякої фіксованої довжини l (достатньої для тестування), а позначення x_i, $i \geq 1$ – для їх реалізацій (які є елементами A^l).

Будемо вважати, що ГПВВ, виходами якого є послідовності X_i, $i \geq 1$, має наступні властивості:

(P1): ГПВВ є стаціонарним джерелом послідовностей випадкових величин (далі – ПВВ);

(P2): послідовності X_i, $i \geq 1$ можна обрати так, що вони будуть незалежними випадковими елементами на A^l.

При виконанні даних умов ПВВ X_i, $i \geq 1$ є незалежними однаково розподіленими елементами на A^l.

III Означення незалежності статистичних тестів

Нехай T_1 і T_2 – деякі статистичні тести із заданими рівнями значимості α_1 та α_2 відповідно; випадкові величини ξ_1 та ξ_2 – індикатори того, що деяка ПВВ X пройшла тести T_1 та T_2, відповідно:

$$\xi_1 = \mathbf{1}\{\text{X пройшла тест } T_1\},$$
$$\xi_2 = \mathbf{1}\{\text{X пройшла тест } T_2\}.$$

Зауваження 3. Іншими словами, ξ_1 (ξ_2) – це індикатор того, що в результаті тестування реалізації ПВВ X тестом T_1 (T_2) буде прийнята основна гіпотеза тесту.

Означення 4. Тести T_1 та T_2 назвемо незалежними (при заданих рівнях значимості α_1 та α_2), якщо індикатори ξ_1 та ξ_2 є незалежними випадковими величинами.

За даним означенням незалежність тестів означає, що результат застосування тесту T_1 для послідовності не залежить від результату застосування тесту T_2. Умова незалежності величин ξ_1 та ξ_2 є більш слабкою, ніж умова незалежності статистик тестів.

Позначимо через ζ_1 та ζ_2 статистики, які обчислюються в тестах T_1 та T_2, а через K_1 та K_2 критичні області тестів, відповідно.

Тоді розподіл величин ξ_1 та ξ_2 наступний:

$$P\{\xi_1 = 1\} = P\{\zeta_1 \notin K_1\}, P\{\xi_1 = 0\} = P\{\zeta_1 \in K_1\},$$
$$P\{\xi_2 = 1\} = P\{\zeta_2 \notin K_2, P\{\xi_2 = 0\} = P\{\zeta_2 \in K_2\}.$$

Тому для незалежності ξ_1, ξ_2 необхідно і достатньо, щоб були незалежними події $\{\zeta_1 \in K_1\}$ та $\{\zeta_2 \in K_2\}$. Тобто незалежність тестів еквівалентна незалежності подій, що полягають у попаданні статистик у критичні області.

Аналогічно можна визначити незалежність довільної кількості статистичних тестів.

Означення 5. Тести з набору $T=\{T_j\}_{1 \leq j \leq N}$ із заданими рівнями значимості $\{\alpha_j\}_{1 \leq j \leq N}$ назвемо незалежними, якщо незалежні в сукупності відповідні індикатори.

Оскільки не є можливим строго довести залежність або незалежність ξ_1 та ξ_2 як випадкових величин, то гіпотезу про їх незалежність будемо перевіряти статистичними методами.

IV Допоміжні результати

Нехай $\{T_j\}_{1 \leq j \leq N}$ – статистичні тести, $\{\alpha_j\}_{1 \leq j \leq N}$ – їх рівні значимості.

Означення 6. З кожним набором тестів $T=\{T_j\}_{1\le j\le N}$ будемо пов'язувати деякий вектор $t = (t_1,..., t_N)$, $t_j \in \{0, 1\}$, $1 \le j \le N$, який будемо називати шаблоном проходження тестів $\{T_j\}_{1\le j\le N}$, а його елемент t_j – шаблоном проходження тесту T_j.

Нехай X – випадковий елемент на A^l, а випадкові величини ξ_j визначені наступним чином:

$$\xi_j(X) = \begin{cases} 1, \textit{ якщо } X \textit{ проходить тест } T; \\ 0, \textit{ якщо інакше.} \end{cases}$$

Якщо імовірнісний розподіл елемента X задається деяким ГПВВ, то тим самим визначається й імовірнісний розподіл даних випадкових величин.

Означення 7. Будемо говорити, що послідовність X проходить набір тестів $T=\{T_j\}_{1\le j\le N}$ згідно з шаблоном $t = (t_1,..., t_N)$, якщо $\forall j = \overline{1, N}$: $\xi_j(X) = t_j$.

Введемо наступні позначення:

$$\eta_j^{t_j}(X) = I\{\xi_j(X) = t_j\},\ j = \overline{1, N} \tag{1}$$

– випадкові величини; індикатори того, що ПВВ X пройшла тест T_j згідно з шаблоном t_j;

$$\eta^{t_1,...,t_N}(X) = I\{\xi_1(X) = t_1,..., \xi_N(X) = t_N\} = \prod_{j=1}^{N} I\{\xi_j(X) = t_j\} = \prod_{j=1}^{N} \eta_j^{t_j}(X) \tag{2}$$

– випадкова величина; індикатор того, що ПВВ X пройшла набір тестів T згідно з шаблоном t;

$$p_j^{t_j}(X) = P\{\xi_j(X) = t_j\} = P\{\eta_j^{t_j}(X) = 1\}, \quad j = \overline{1, N}, \tag{3}$$

$$p^{t_1,...,t_N}(X) = P\{\eta_1^{t_1}(X) = 1,..., \eta_N^{t_N}(X) = 1\}, \tag{4}$$

– імовірності відповідних подій.

Внаслідок властивостей (Р1) та (Р2) ГПВВ, $\forall i = \overline{1, n}$ величини $p_j^{t_j}(X_i)$ та $p^{t_1,...,t_N}(X_i)$ не залежать від індексу i; ці величини ми будемо позначати $p_j^{t_j}$ та $p^{t_1,...,t_N}$, відповідно.

Якщо шаблон t зафіксовано, то замість позначень

$$\eta_j^{t_j}(X_i), \quad j = \overline{1, N}, \quad i = \overline{1, n};\ \eta^{t_1,...,t_N}(X_i);\ p_j^{t_j} \text{ та } p^{t_1,...,t_N}$$

будемо використовувати, відповідно, позначення

$$\eta_j(X_i),\ j = \overline{1, N},\ i = \overline{1, n};\ \eta(X_i);\ p_j \text{ та } p.$$

Також введемо випадкові величини

$$\theta_j^{(n)} = \frac{1}{n}\sum_{i=1}^{n} \eta_j(X_i), \quad j = \overline{1, N}, \tag{5}$$

$$\theta^{(n)} = \frac{1}{n}\sum_{i=1}^{n} \eta(X_i), \tag{6}$$

– частоти проходження тесту T_j та набору тестів T, відповідно.

Зазначимо, що за умови незалежності тестів з набору T, виконується рівність

$$p = \prod_{j=1}^{N} p_j .$$

В наших позначеннях справедлива наступна теорема.

Теорема 8. Нехай задано деяке $0 < \gamma < 1$ та $\varepsilon > 0$. Якщо тести з набору T незалежні в сенсі означення 5 та

$$n \ge \max\left\{ 9 \cdot \left(\frac{N}{2\varepsilon} \Phi^{-1}\left(1 - \frac{1-\gamma}{4N}\right)\right)^2, 9 \cdot \left(\Phi^{-1}\left(\frac{3+\gamma}{4}\right) / \varepsilon \right)^2 \right\}, \tag{7}$$

де $\Phi(\bullet)$ – функція стандартного нормального розподілу,

то справедлива наступна рівність:

$$P\{\rho^{(n)} \in (\rho_1 - \varepsilon/3, \rho_2 + \varepsilon/3)\} \ge \gamma,$$

де

$$\rho^{(n)} = \prod_{j=1}^{N} \theta_j^{(n)} = \frac{1}{n^N} \prod_{j=1}^{N} \sum_{i=1}^{n} \eta_i^{(j)}, \tag{8}$$

$$\rho_1 = \frac{n}{t^2+n}\left(\theta^{(n)} + \frac{t^2}{2n} - t\sqrt{\frac{\theta^{(n)}(1-\theta^{(n)})}{n} + \left(\frac{t}{2n}\right)^2} \right), \tag{9}$$

$$\rho_2 = \frac{n}{t^2+n}\left(\theta^{(n)} + \frac{t^2}{2n} + t\sqrt{\frac{\theta^{(n)}(1-\theta^{(n)})}{n} + \left(\frac{t}{2n}\right)^2} \right), \tag{10}$$

$$\mathrm{t} = \Phi^{-1}\left(\frac{3+\gamma}{4}\right).$$

При цьому довжина інтервалу $(\rho_1 - \varepsilon/3, \rho_2 + \varepsilon/3)$ не більша за ε.

Доведення.

Доведення буде проводитись у три етапи.

I. Побудуємо довірчий інтервал (ρ_1, ρ_2), який з надійністю $0 < \gamma_1 < 1$ покриває оцінюване значення ймовірності p . Тоді, згідно з [6], якщо

$$\rho_1 = \frac{n}{t^2+n}\left(\theta^{(n)} + \frac{t^2}{2n} - t\sqrt{\frac{\theta^{(n)}(1-\theta^{(n)})}{n} + \left(\frac{t}{2n}\right)^2} \right),$$

та

$$\rho_2 = \frac{n}{t^2+n}\left(\theta^{(n)} + \frac{t^2}{2n} + t\sqrt{\frac{\theta^{(n)}(1-\theta^{(n)})}{n} + \left(\frac{t}{2n}\right)^2} \right),$$

де

$$\mathrm{t} = \Phi^{-1}\left(\frac{1+\gamma_1}{2}\right),$$

то $\mathrm{P}\{ p \in (\rho_1, \rho_2) \} \geq \gamma_1$.

Зауваження 9.

1) При досить великих значеннях n (n>>t) можна використовувати наближені значення:

$$\rho_1 = \theta^{(n)} - t\sqrt{\frac{\theta^{(n)}(1-\theta^{(n)})}{n}}, \tag{11}$$

$$\rho_2 = \theta^{(n)} + t\sqrt{\frac{\theta^{(n)}(1-\theta^{(n)})}{n}}. \tag{12}$$

На практиці, як правило, виникає саме така ситуація (n>1000).

2) Якщо потрібно, щоб довжина довірчого інтервалу була не більшою за деяке наперед задане $\varepsilon_1 > 0$, то кількість послідовностей n можна обрати з наступних міркувань:

$$\rho_2 - \rho_1 = 2t\sqrt{\frac{\theta^{(n)}(1-\theta^{(n)})}{n}} \leq 2t\sqrt{\frac{1}{4n}} = \frac{t}{\sqrt{n}} \leq \varepsilon_1,$$

звідки

$$\mathrm{n} \geq \left(\Phi^{-1}\left(\frac{1+\gamma_1}{2}\right) / \varepsilon_1 \right)^2.$$

II. Далі, нехай задано $0 < \gamma_2 < 1$ та $\varepsilon_2 > 0$. Покажемо, що

$$\rho^{(n)} = \prod_{j=1}^{N} \theta_j^{(n)} \xrightarrow{\mathrm{P}} \prod_{j=1}^{N} p_j \ , n \to \infty.$$

Позначимо події

$$B_j = \{|\theta_j^{(n)} - p_j| < \varepsilon_2/N\},\ 1 \le j \le N,$$

$$C = \left\{ \left| \prod_{j=1}^{N} p_j - \prod_{j=1}^{N} \theta_j^{(n)} \right| < \varepsilon_2 \right\}.$$

Для фіксованого $1 \le j \le N$ послідовність випадкових величин $\theta_j^{(n)}$ збігається за ймовірністю до значення p_j, коли n прямує до нескінченості (див. [7]):

$$\theta_j^{(n)} \xrightarrow{\text{P}} p_j,\ n \to \infty.$$

Тоді при

$$n \ge \left(\frac{N}{2\varepsilon_2} \Phi^{-1}\left(1 - \frac{1-\gamma_2}{2N}\right) \right)^2$$

та беручи до уваги асимптотичну нормальність випадкової величини $\theta_j^{(n)}$, як вибіркового моменту, виконується наступне:

$$\text{P}\{B_j\} \approx 2\Phi\left(\frac{\varepsilon_2}{\sigma_j \cdot N}\right) - 1 \ge 2\Phi\left(\frac{2\varepsilon_2\sqrt{n}}{N}\right) - 1 \ge 1 - \frac{1-\gamma_2}{N}.$$

Останню нерівність можна переписати так:

$$\text{P}\{\overline{B}_j\} \le 2 - 2\Phi\left(\frac{2\varepsilon_2\sqrt{n}}{N}\right) \le \frac{1-\gamma_2}{N}.$$

Оскільки

$$\left| \prod_{j=1}^{N} p_j - \prod_{j=1}^{N} \theta_j^{(n)} \right| = \left| \prod_{j=1}^{N} p_j - \prod_{j=1}^{N} \theta_j^{(n)} \pm \theta_N^{(n)} \cdot \prod_{j=1}^{N-1} p_j \right| \le$$

$$\le \left| \prod_{j=1}^{N-1} p_j \right| \left| p_N - \theta_N^{(n)} \right| + \left| \theta_N^{(n)} \right| \left| \prod_{j=1}^{N-1} p_j - \prod_{j=1}^{N-1} \theta_j^{(n)} \right| \le$$

$$\le \left| p_N - \theta_N^{(n)} \right| + \left| \prod_{j=1}^{N-1} p_j - \prod_{j=1}^{N-1} \theta_j^{(n)} \pm \theta_{N-1}^{(n)} \cdot \prod_{j=1}^{N-2} p_j \right| \le \ldots \le \sum_{j=1}^{N} \left| p_j - \theta_j^{(n)} \right| < \varepsilon_2,$$

при виконанні умов B_j, $1 \le j \le N$, то подія C є наслідком події $\text{B} = B_1\, B_2\, \ldots\, B_N$.

Тоді

$$\text{P}\{C\} \ge \text{P}\{B\} = 1 - \text{P}\{\overline{B}\} = 1 - \text{P}\{\overline{B}_1 \cup \overline{B}_2 \cup \ldots \cup \overline{B}_N\} \ge 1 - \sum_{j=1}^{N} \text{P}\{\overline{B}_j\} \ge \gamma_2.$$

Отже

$$\rho^{(n)} = \prod_{j=1}^{N} \theta_j^{(n)} \xrightarrow{\text{P}} \prod_{j=1}^{N} p_j,\ n \to \infty.$$

III. Повернемось до твердження теореми. За умови незалежності тестів з набору T справедлива рівність:

$$p = \prod_{j=1}^{N} p_j.$$

Для довільних фіксованих значень $0 < \gamma < 1$ та $\varepsilon > 0$ скористаємось результатами пунктів **I** та **II**, поклавши $\gamma_1 = 1/2 + \gamma/2$, $\varepsilon_1 = \varepsilon/3$ та $\gamma_2 = 1/2 + \gamma/2$, $\varepsilon_2 = \varepsilon/3$. Тоді

$$\text{P}\{p \in (\rho_1, \rho_2)\} \ge \gamma_1 = 1/2 + \gamma/2,$$

$$\text{P}\{\rho^{(n)} \in (p - \varepsilon/3, p + \varepsilon/3)\} = \text{P}\left\{ \left| \prod_{j=1}^{N} p_j - \prod_{j=1}^{N} \theta_j^{(n)} \right| < \varepsilon/3 \right\} \ge \gamma_2 = 1/2 + \gamma/2,$$

при

$$n \geq \max\left\{9 \cdot \left(\frac{N}{2\varepsilon}\Phi^{-1}\left(1-\frac{1-\gamma}{4N}\right)\right)^2, 9 \cdot \left(\Phi^{-1}\left(\frac{3+\gamma}{4}\right)/\varepsilon\right)^2\right\}.$$

Помітимо, що якщо $p \in (\rho_1, \rho_2)$ і $\rho^{(n)} \in (p - \varepsilon/3, p + \varepsilon/3)$, то

$$\rho^{(n)} \in (\rho_1 - \varepsilon/3, \rho_2 + \varepsilon/3).$$

Отже,

$$P\{\rho^{(n)} \in (\rho_1 - \varepsilon/3, \rho_2 + \varepsilon/3)\} \geq P\{p \in (\rho_1, \rho_2), \rho^{(n)} \in (p - \varepsilon/3, p + \varepsilon/3)\} \geq$$
$$\geq 1 - P\{p \in (\rho_1, \rho_2)\} - P\{\rho^{(n)} \notin (p - \varepsilon/3, p + \varepsilon/3)\} \geq \gamma.$$

Теорему доведено.

V Методика перевірки незалежності тестів з набору тестів

Виходячи з отриманих результатів, можна запропонувати наступну загальну методику перевірки гіпотези незалежності тестів набору $\{T_j\}_{1 \leq j \leq N}$ згідно з означенням 2:

1. Вибрати значення $0 < \gamma < 1$, $\varepsilon > 0$ та n таким чином, щоб виконувалась нерівність (7).
2. Обрати шаблон $(t_1, t_2, ..., t_N)$ проходження тестів.
3. Отримати значення $\eta_i^{(j)}$, $1 \leq i \leq n$, $1 \leq j \leq N$, для цього протестувати набором тестів $\{T_j\}_{1 \leq j \leq N}$ послідовності X_i, $1 \leq i \leq n$, які згенеровані ГВП.
4. Використовуючи формули (8), (9), (10) (або, для спрощення обчислень, (8), (11), (12)) на основі значень $\eta_i^{(j)}$ підрахувати значення величини $\rho^{(n)}$ та границь довірчого інтервалу (ρ_1, ρ_2). При цьому якщо $\rho_1 < \varepsilon/3$, то покласти $\rho_1 = \varepsilon/3$; якщо $\rho_2 > 1 - \varepsilon/3$, то покласти $\rho_2 = 1 - \varepsilon/3$.
5. Якщо $\rho^{(n)} \in (\rho_1 - \varepsilon/3, \rho_2 + \varepsilon/3)$, то гіпотеза про незалежність тестів з набору тестів $\{T_j\}_{1 \leq j \leq N}$ приймається. Інакше гіпотеза відхиляється.

Помилка першого роду при цьому становить $1 - \gamma$.

Зауважимо, що (ρ_1, ρ_2) є інтервальною оцінкою ймовірності того, що послідовності пройдуть всі тести, а величина $\rho^{(n)}$ є точковою оцінкою для значення добутку ймовірностей проходження кожного тесту.

VI Висновки

Наведена методика є узагальненням раніше отриманих результатів. При виборі шаблону, який складається з усіх одиниць, вона повністю збігається з попередньою методикою. А при її застосуванні до тестів, рівень значимості яких збігається з ймовірністю їх проходження випадковою рівно ймовірною послідовністю, результати збігатимуться з результатами застосування методики з роботи [5]. Узагальнення дозволяє уникнути отримання тривіальних результатів тестування.

Література: ***1.*** *Гулак Г. Н. Різні підходи до визначення випадкових послідовностей / Г. Н. Гулак, Л. В. Ковальчук // НТЗ Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Київ, 2001. – Вип. 3. – С. 127-133.* ***2.*** *Ковальчук Л. В. О периодах выходных последовательностей некоторых псевдослучайных генераторов, построенных на основе односторонних функций / Л. В. Ковальчук // Безопасность информации в информационно-телекоммуникационных системах, III Международная научно-практическая конференція (Киев, апрель, 2000 р.): тезисы докл. – С. 56-59.* ***3.*** *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST Special Publication 800-22, Rev. 1. – 131 с.* ***4.*** *Marsaglia G. DIEHARD Statistical Tests / George Marsaglia. – Режим доступу: http://stat.fsu.edu/~geo/diehard.html. – Дата доступу: ??.??.????.* ***5.*** *Ковальчук Л. В. Перевірка незалежності статистичних тестів, призначених для оцінки криптографічних якостей ГВП. / Л. В. Ковальчук, В. Т. Бездітний; «Захист інформації», №2(29) 2006.* ***6.*** *Гмурман В. Е. Теория вероятностей и математическая статистика / В. Е. Гмурман. – М. : Высшая школа, 2003. – С. 224-226.* ***7.*** *Ивченко Г. И. Математическая статистика: учебное пособие для ВУЗов / Г. И. Ивченко, Ю. И. Медведев. – М.: Высшая школа, 1984. – С. 20-21.* ***8.*** *Ширяев А. Н. Вероятность / А. Н. Ширяев. – М.: Наука, 1989. – 640 с.*