УДК 004.056.5

МЕТОДОЛОГІЯ ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ ФАКТОРІАЛЬНОГО КОДУВАННЯ ДАНИХ

Методологія захисту інформації є основою теоретичного базису для забезпечення інформаційної безпеки в інформаційно-телекомунікаційних і комп'ютерних системах і мережах. Зважаючи на постійно розширювану комунікаційну інфраструктуру, збільшення обсягів інформації, що передаються каналами зв'язку, та появу нових, більш ефективних, методів забезпечення захисту даних від загроз, засоби реалізації яких модифікуються та вдосконалюються, розвиток та вдосконалення методологічних аспектів захисту інформації на сьогоднішній день є актуальним напрямком досліджень.

Одним із засобів забезпечення інформаційної безпеки в комп'ютерних мережах є тунельовані протоколи для різних рівнів моделі OSI. Під час передавання інформації тунельованими протоколами одночасно вирішуються декілька задач захисту інформації – забезпечення аутентифікації, конфіденційності, цілісності. Окреме вирішення цих задач пов'язане з застосуванням різних математичних методів і алгоритмів, а також послідовною обробкою інформації, що призводить до збільшення навантаження на засоби перетворення інформації та підвищення вимог до їх швидкодії, збільшення введеної надлишковості і, як наслідок, до зменшення відносної швидкості передавання. Ці обставини актуалізують проблему забезпечення захисту інформації під час її зберігання та передавання в комп'ютерних системах і мережах за рахунок інтеграції методів канального кодування та комп'ютерної криптографії, що реалізують сумісний захист переданих даних від помилок каналу зв'язку, а також несанкціонованої модифікації та/або несанкціонованого доступу.

На сьогоднішній день розроблено методи роздільного факторіального кодування інформації [1]–[7], які за рахунок реалізації єдиної процедури завадостійкого кодування та захисту від нав'язування хибних даних шляхом використання перестановки в якості перевірної частини кодового слова дозволяють

забезпечити контроль цілісності інформації та підвищити її достовірність під час передавання в телекомунікаційних і комп'ютерних системах і мережах в умовах обмежень пропускної здатності каналів зв'язку.

Відомі методи нероздільного факторіального кодування інформації [4], [8]–[14], які за рахунок реалізації єдиної процедури завадостійкого кодування та шифрування шляхом бієктивного перетворення інформаційної послідовності в перестановку чисел заданого порядку, параметри якого тримаються в таємниці, дозволяють забезпечити захист інформації від помилок каналу зв'язку, несанкціонованого доступу та підвищити її достовірність під час передавання в телекомунікаційних і комп'ютерних системах і мережах в умовах обмежень пропускної здатності каналів зв'язку.

Разом із тим, на сьогоднішній день відсутня методологія захисту інформації на основі факторіального кодування даних. Її створення дозволить отримати єдину стратегію розробки та використання методів факторіального кодування для інтегрованого захисту інформації від помилок каналу зв'язку, а також несанкціонованого доступу та/або модифікації.

Створена методологія (рис. 1) базується на методах роздільного та нероздільного факторіального кодування [1]–[14] інформації та містить наступні етапи:

1) формування множини загроз під час передавання інформації каналами зв'язку;
2) формування вимог до параметрів кодування та кількісних показників захищеності інформації;
3) вибір методу факторіального кодування інформації;
4) вибір параметрів і розрахунок показників факторіального кодування інформації;
5) вибір методу формування ключових послідовностей;
6) реалізація методу формування ключових послідовностей для факторіального кодування інформації;
7) реалізація методу факторіального кодування інформації.

Опишемо більш детально кожен з етапів запропонованої методології.

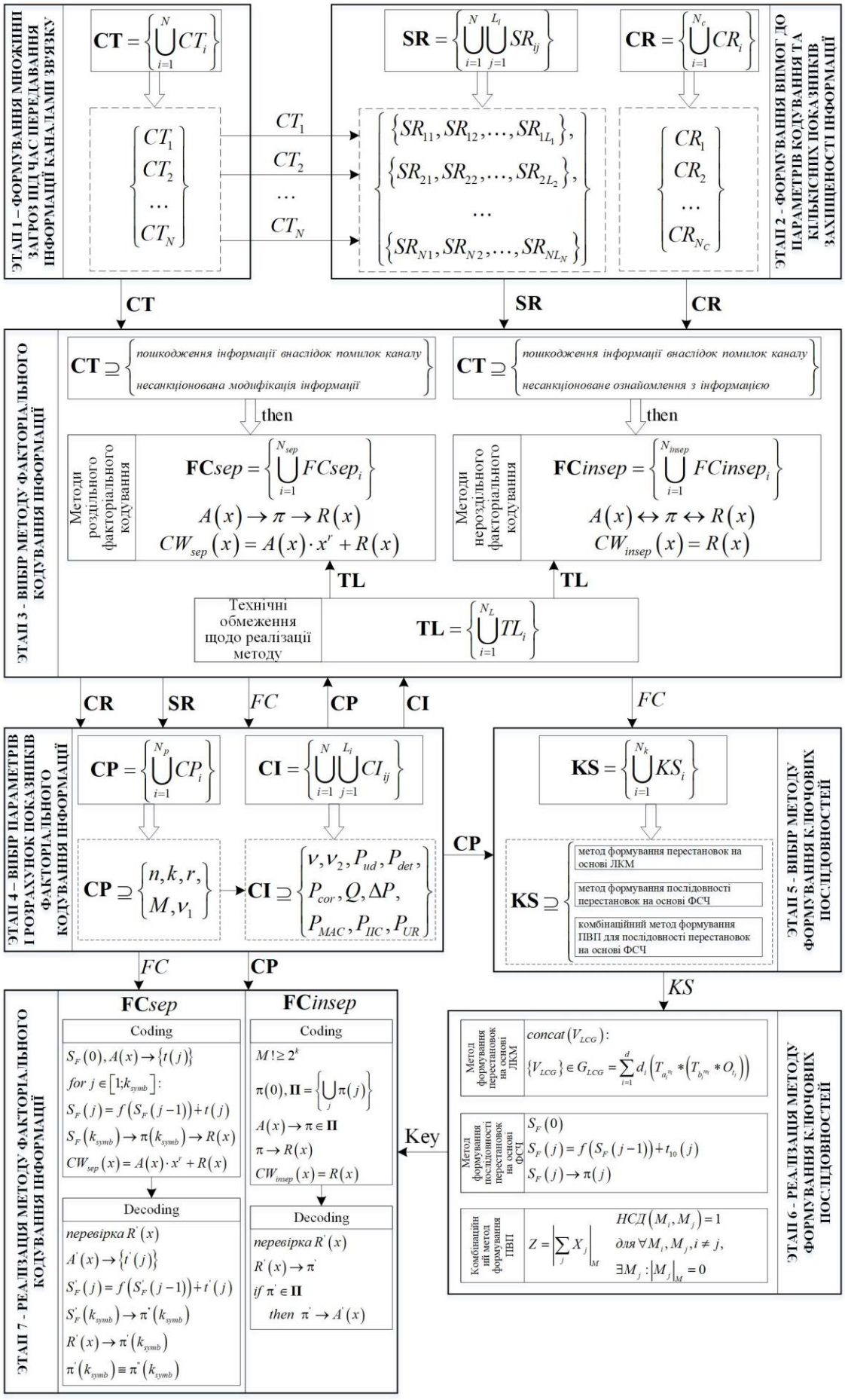

Рис. 1. Методологія захисту інформації на основі факторіального кодування даних

Етап 1. Формування множини загроз під час передавання інформації каналами зв'язку.

На першому етапі реалізації запропонованої методології користувачу необхідно визначити всі можливі загрози, які виникають під час транспортування інформації каналами зв'язку в телекомунікаційних і комп'ютерних системах і мережах. У результаті реалізації цього етапу формується множина загроз $\mathbf{CT} = \left\{ \bigcup_{i=1}^{N} CT_i \right\} = \{CT_1, CT_2, \ldots, CT_N\}$, де N – кількість можливих загроз, визначених користувачем. Прикладом загроз можуть бути наступні: $CT_1 =$«*Пошкодження інформації внаслідок помилок каналу*», $CT_2 =$«*Несанкціонована модифікація (НСМ) інформації криптоаналітиком*», $CT_3 =$«*Несанкціоноване ознайомлення з інформацією*» (несанкціонований доступ (НСД) до інформації), $CT_4 =$«*Витік інформації відхідними ланцюгами*» тощо.

Етап 2. Формування вимог до параметрів кодування та кількісних показників захищеності інформації.

На другому етапі на основі сформованої множини загроз **CT** визначаються вимоги до параметрів кодування **CR** та гранично допустимі кількісні показники захищеності інформації **SR**. До множини параметрів коду можуть входити наступні: довжина кодового слова – n, довжина інформаційної частини кодового слова – k, довжина перевірної частини кодового слова – r, швидкість коду – $\nu_1 = \frac{k}{n}$ тощо. Для кожної можливої загрози CT_i, $i \in [1, N]$, може формуватися множина показників захищеності $\mathbf{SR}_i = \left\{ \bigcup_{j=1}^{L_i} SR_{ij} \right\} = \left\{ SR_{i1}, SR_{i2}, \ldots, SR_{iL_i} \right\}$, де L_i – кількість можливих показників для i-ї загрози. Наприклад, для загрози $CT_1 =$«*Пошкодження інформації внаслідок помилок каналу*» множина вимог може мати вигляд: $SR_{11} =$«$\nu \geq 0.85$», $SR_{12} =$«$P_{ud} \leq 10^{-7}$», $SR_{13} =$«$p_{0eq} \leq 10^{-9}$», $SR_{14} =$«$\Delta P \geq 5 дБ$» тощо, де ν – відносна швидкість передавання, P_{ud} – імовірність не виявленої декодером помилки, p_{0eq} – еквівалентна бітова помилка внаслідок застосування завадостійкого

кодування; ΔP – енергетичний виграш. У результаті реалізації другого етапу запропонованої методології формується множина вимог до параметрів кодування $\mathbf{CR} = \left\{ \bigcup_{i=1}^{N_c} CR_i \right\}$ і множина кількісних показників захищеності інформації $\mathbf{SR} = \left\{ \bigcup_{i=1}^{N} \bigcup_{j=1}^{L_i} SR_{ij} \right\}$.

Етап 3. Вибір методу факторіального кодування інформації.

На третьому етапі методології на основі сформованій на першому етапі множині загроз **CT** користувачем обирається метод факторіального кодування інформації. Якщо множина загроз містить загрози $CT_i =$«*Пошкодження інформації внаслідок помилок каналу*» і $CT_j =$«*НСМ інформації криптоаналітиком*», метод факторіального кодування обирається з групи з N_{sep} роздільних методів $\mathbf{FC}sep = \left\{ \bigcup_{i=1}^{N_{sep}} FCsep_i \right\}$. Якщо множина загроз містить загрози $CT_i =$«*Пошкодження інформації внаслідок помилок каналу*» і $CT_j =$«*Несанкціоноване ознайомлення з інформацією*», метод факторіального кодування обирається з групи з N_{insep} нероздільних методів $\mathbf{FC}insep = \left\{ \bigcup_{i=1}^{N_{insep}} FCinsep_i \right\}$. Якщо ж множина загроз містить загрози $CT_i =$«*Пошкодження інформації внаслідок помилок каналу*», $CT_j =$«*НСМ інформації криптоаналітиком*» і $CT_l =$«*Несанкціоноване ознайомлення з інформацією*», користувач може як комбінувати роздільні та нероздільні методи факторіального кодування, так і використовувати метод роздільного факторіального кодування з поєднанням з іншим методом криптографічного закриття інформації, наприклад, методом двоконтурного криптографічного перетворення.

Методи роздільного факторіального кодування інформації **FC***sep* [1]–[7] передбачають перетворення інформаційної частини $A(x)$, що поступає на вхід кодера, в перестановку чисел π, яка після кодування двійковим кодом $\left(R(x)\right)$

додається до інформаційної частини, формуючи кодове слово $CW_{sep}(x) = A(x) \cdot x^r + R(x)$, де r – кількість двійкових розрядів у перевірній частині $R(x)$.

Методи нероздільного факторіального кодування інформації **FC***insep* [4], [8]–[14] передбачають бієктивне перетворення інформаційної послідовності $A(x)$, що поступає на вхід кодера, в перестановку чисел π, яка після кодування двійковим кодом $(R(x))$ передається каналом зв'язку. Таким чином, кодове слово для методів нероздільного факторіального кодування $CW_{insep}(x) = R(x)$.

Порядок перестановки M визначається сформованими на другому етапі вимогами. У будь-якому разі для методів нероздільного факторіального кодування $M! \geq 2^k$, де k – кількість біт у інформаційній послідовності, що поступає на вхід кодера.

Вибір методу факторіального кодування базується також на аналізі множини технічних обмежень $\mathbf{TL} = \left\{ \bigcup_{i=1}^{N_L} TL_i \right\} = \left\{ TL_1, TL_2, \ldots, TL_{N_L} \right\}$, а також на порівнянні сформованих на другому етапі методології вимог до параметрів кодування **CR** та кількісних показників **SR** захищеності інформації з параметрами та показниками факторіального кодування, розрахованими на четвертому етапі.

Множина технічних обмежень, наприклад, може містити наступні елементи: $TL_1 =$«*Неможливість використання вирішального зворотного зв'язку*», $TL_2 =$«*Неможливість видалення прапору циклової синхронізації (delimiter) зі структури кадру*», $TL_3 =$«*Обмеження в продуктивності засобів кодування*», $TL_4 =$«*Обмеження обсязі пам'яті під час операцій кодування/декодування*» тощо.

Етап 4. Вибір параметрів і розрахунок показників факторіального кодування інформації.

Для обґрунтованого вибору та реалізації методів факторіального кодування інформації на цьому етапі на основі характеристик каналу передавання даних

визначаються основні параметри $\mathbf{CP} = \left\{ \bigcup_{i=1}^{N_c} CP_i \right\}$ та кількісні показники $\mathbf{CI} = \left\{ \bigcup_{i=1}^{N} \bigcup_{j=1}^{L_i} CI_{ij} \right\}$ досліджуваного факторіального коду з метою їх задоволення, відповідно, множині **CR** вимог до параметрів кодування та множині вимог **SR** до кількісних показників захищеності інформації, сформованих на другому етапі методології.

Етап 5. Вибір методу формування ключових послідовностей.

Для обраного на третьому етапі методології методу факторіального кодування інформації, за визначених на четвертому етапі параметрів коду, на п'ятому етапі обирається метод формування ключових послідовностей з множини з N_K можливих методів $\mathbf{KS} = \left\{ \bigcup_{i=1}^{N_K} KS_i \right\}$. Ця множина включає:

1) $KS_1 =$ «метод формування псевдовипадкової послідовності (ПВП) чисел на основі лінійного конгруентного методу, який за рахунок конкатенації в графі станів лінійного конгруентного генератора (ЛКГ) не лише відособлених непересічних циклів, а і передциклів (дерев), якщо вони в ньому містяться, дозволяє формувати ПВП рівномірно розподілених чисел (перестановку) незалежно від топології графа станів ЛКГ»;

2) $KS_2 =$ «метод формування послідовностей перестановок на основі використання факторіальної системи числення (ФСЧ), який за рахунок введення додаткового генератора випадкових чисел, символи якого підсумовуються з модифікованим синдромом попередньої перестановки та визначають синдром наступної перестановки, забезпечує формування непередбачуваної послідовності перестановок без необхідності приведення випадкового числа додаткового генератора до потрібного діапазону зі змінною верхньою межею, дозволяє уникнути порушення рівномірності розподілу перестановок та підвищити швидкість їх формування» [15], [16];

3) KS_3 = «комбінаційний метод формування ПВП з комбінаційною функцією підсумовування за модулем слів, отриманих від групи первинних генераторів рівномірно розподілених випадкових чисел як з необмеженими, так і з обмеженими періодами, а також перестановок, які циклічно повторюються» [17].

Крім вибору самого методу формування ключової послідовності, в залежності від визначеної на четвертому етапі множини **CP** обираються параметри для його реалізації.

Етап 6. Реалізація методу формування ключових послідовностей для факторіального кодування інформації.

Цей етап передбачає реалізацію обраного на попередньому етапі методу формування ключових послідовностей з визначеними параметрами.

Зазначимо, що метод формування ПВП на основі використання ЛКГ з будь-якою топологією обумовлює конкатенацію всіх вершин з множини $\{V_{LCG}\}$, що належать графу станів ЛКГ, який узагальнено може бути описаний виразом $G_{LCG} = \sum_{i=1}^{d} d_i \left(T_{a_i^{n_i}} * \left(T_{b_i^{m_i}} * O_{t_i} \right) \right)$, де d – число різних типів компонент зв'язності графа станів ЛКГ; d_i – число компонент зв'язності графа станів ЛКГ i-го типу; a_i, n_i, b_i, m_i, t_i – параметри компонент зв'язності графа станів ЛКГ i-го типу; O_n – орієнтований цикл з n вершин, T_{2^n} – кореневе дерево з $2n$ вершинами і n поверхами крім кореня, що розгалужується бінарно на поверхах $1,\ldots,n-1$.

У методі формування послідовностей перестановок на основі ФСЧ для представлення синдрому перестановки S_F [15], [16] формування наступної перестановки зводиться до модифікації її синдрому згідно з ітераційним виразом $S_F(j) = f\left(S_F(j-1)\right) \dot{+} t_{10}(j)$, де $f\left(S(j-1)\right)$ – функція від значення синдрому попередньої перестановки; $t_{10}(j)$ – випадкове число в десятковій системі числення, що позначає зсув порядкового номеру перестановки щодо номеру попередньої перестановки на відрізку $[0, M!-1]$; символ $\dot{+}$ позначає додавання чисел різних

систем числення. Випадкову величину $t_{10}(j)$ формує вбудований генератор (псевдо) випадкових чисел.

Для рівномірного розподілу дискретної випадкової величини на множині цілих чисел потужності M на виході комбінаційного генератора [17] з комбінаційною функцією підсумовування за модулем M слів від деякої кількості n незалежних первинних генераторів, кожний з яких циклічно формує перестановку на множині цілих чисел $[0, M_i - 1]$, $i = 1, 2, \ldots n$, достатньо, щоб значення M_i були попарно взаємно прості ($НСД(M_i, M_j) = 1$ для $\forall M_i, M_j$, $i \neq j$) і одне зі значень M_i було кратне M $\left(\exists M_j : |M_j|_M = 0\right)$ [18].

Етап 7. Реалізація методу факторіального кодування інформації.

Сьомий етап передбачає реалізацію обраного на етапі 3 методу факторіального кодування інформації на основі визначених параметрів (етап 4), а також вибору методу формування ключових послідовностей (етап 5) і його реалізації (етап 6).

Ядро процедури реалізації будь-якого методу роздільного факторіального кодування інформації **FC***sep* [1]–[7] включає наступні етапи:

1) інформаційна послідовність $A(x)$, що надходить на вхід кодера, розбивається на укрупнені символи множини $\{t(j)\}$, $j \in [1; k_{symb}]$, де k_{symb} – кількість укрупнених символів;

2) отримана послідовність символів $\{t(j)\}$ прихованим чином на основі перетворення $S_F(j) = f(S_F(j-1)) \dot{+} t(j)$ за заданого $S_F(0)$ визначає $S_F(k_{symb})$;

3) отриманий синдром $S_F(k_{symb})$ перетворюється в перестановку $\pi(k_{symb})$, яка після кодування її символів двійковим кодом формує перевірну частину $R(x)$;

4) формується кодове слово $CW_{sep}(x) = A(x) \cdot x^r + R(x)$.

Процес декодування роздільного факторіального коду містить етапи:

1) перевірна частина $R^{'}(x)$ отриманого з каналу кодового слова перевіряється на відповідність перестановці. Якщо ця перевірка не проходить, формується сигнал перезапиту спотвореного блоку. В іншому випадку:

2) за інформаційною частиною отриманого з каналу кодового слова $A^{'}(x)$ за тими ж етапами, які реалізуються під час кодування, визначається перевірна перестановка $\pi^{''}(k_{symb})$. Якщо обчислена $\pi^{''}(k_{symb})$ та прийнята $\pi^{'}(k_{symb})$ перестановки співпадають, блок даних видається користувачу.

Методи нероздільного факторіального кодування **FC***insep* [4], [8]–[14] бієктивно перетворюють інформаційну послідовність $A(x)$, що надходить на вхід кодера, в перестановку π, що належить множині дозволених перестановок $\mathbf{\Pi} = \left\{ \bigcup_{j} \pi(j) \right\}$ з заданими властивостями. Після кодування символів перестановки двійковим кодом вона видається в канал: $CW_{insep}(x) = R(x)$.

Декодування нероздільного факторіального коду передбачає перевірку отриманого з каналу зв'язку кодового слова $\pi^{'}$ на належність до множини $\mathbf{\Pi}$ та наступне зворотне перетворення в інформаційну послідовність $\pi^{'} \to A^{'}(x)$.

Розроблена методологія захисту інформації на основі факторіального кодування даних дозволяє формалізувати процес створення ефективних засобів забезпечення захисту інформації під час її зберігання та передавання в телекомунікаційних і комп'ютерних системах і мережах за рахунок інтеграції методів канального кодування та комп'ютерної криптографії, що реалізують сумісний захист переданих даних від помилок каналу зв'язку, а також несанкціонованої модифікації та/або несанкціонованого доступу.

Література

[1] Э. В. Фауре, В. В. Швыдкий, и А. И. Щерба, "Контроль целостности информации на основе факториальной системы счисления", *Journal of Baku Engineering University. Mathematics and computer science*, т. 1, № 1, с. 3–13, 2017.

[2] Э. В. Фауре, В. В. Швыдкий, и В. А. Щерба, "Метод формирования имитовставки на основе перестановок", *Захист інформації*, т. 16, № 4, с. 340, 2015.

[3] Э. В. Фауре, В. В. Швыдкий, и В. А. Щерба, "Комбинированное факториальное кодирование и его свойства", *Радіоелектроніка, інформатика, управління*, № 3, с. 80–86, 2016.

[4] Э. В. Фауре, "Факториальное кодирование с несколькими контрольными суммами", *Вісник Житомирського державного технологічного університету. Серія: Технічні науки*, № 3 (78), с. 104–113, 2016.

[5] В. М. Рудницький, Е. В. Фауре, В. В. Швидкий, і А. І. Щерба, "Спосіб контролю цілісності інформації", патент України №107655, 24.06.2016.

[6] В. М. Рудницький, Е. В. Фауре, В. В. Швидкий, і А. І. Щерба, "Спосіб комбінованого кодування інформації", патент України №107657, 24.06.2016.

[7] Е. В. Фауре, В. В. Швидкий, і А. І. Щерба, "Спосіб формування імітовставки", патент України №106669, 10.05.2016.

[8] Э. В. Фауре, "Факториальное кодирование с восстановлением данных", *Вісник Черкаського державного технологічного університету. Серія: Технічні науки*, т. 1, № 2, с. 33–39, 2016.

[9] Э. В. Фауре, "Метод повышения эффективности факториального кодирования с восстановлением данных", *Вісник Черкаського державного технологічного університету. Серія: Технічні науки*, № 4, с. 57–61, 2016.

[10] E. V. Faure, A. I. Shcherba, and A. A. Kharin, "Factorial code with a given number of inversions", *Radio Electronics, Computer Science, Control*, no. 2, pp. 143–153, 2018.

[11] Е. В. Фауре, "Факториальное кодирование с исправлением ошибок", *Радіоелектроніка, інформатика, управління*, № 3, с. 130–138, 2017.

[12] Э. В. Фауре, "Факториальное кодирование с исправлением ошибок. Теоретическое обоснование и примеры реализации", в *Наукоемкие технологии в инфокоммуникациях: обработка информации, кибербезопасность, информационная борьба : монография*, В. М. Безрук и В. В. Баранник, Ред. Харьков: Лидер, 2017, с. 291–323.

[13] Е. В. Фауре, О. О. Харін, В. В. Швидкий, і А. І. Щерба, "Спосіб факторіального кодування з відновленням даних", патент України №117004, 12.06.2017.

[14] Е. В. Фауре, О. О. Харін, В. В. Швидкий, і А. І. Щерба, "Спосіб факторіального кодування з виявленням і виправленням помилок", патент України №121361, 11.12.2017.

[15] Э. В. Фауре, В. В. Швыдкий, и А. И. Щерба, "Метод формирования воспроизводимой непредсказуемой последовательности перестановок", *Безпека інформації*, т. 20, № 3, с. 253–258, 2014.

[16] Е. В. Фауре, В. В. Швидкий, і А. І. Щерба, "Спосіб формування випадкової послідовності перестановок", патент України №106668, 10.05.2016.

[17] А. А. Лавданский и Э. В. Фауре, "Комбинационный метод формирования последовательности псевдослучайных чисел", в *Системний аналіз та інформаційні технології: матеріали 16-ї Міжнародної науково-технічної конференції SAIT-2014, Київ, 26-30 травня 2014 р.*, К., 2014, с. 403–404.

[18] Э. В. Фауре, "Закон распределения дискретной случайной величины на выходе комбинационного генератора", *Безпека інформації*, т. 20, № 2, с. 153–158, 2014.