УДК 621.391:004.94

[0000-0002-2046-481X] **Е. В. Фауре,** *д-р техн. наук, професор,*
[0000-0002-8632-1176] **А. Б. Скуцький,**
e-mail: a.b.skutskyi.asp21@chdtu.edu.ua
[0000-0002-1596-4123] **А. О. Лавданський,** *канд. техн. наук, доцент*
Черкаський державний технологічний університет
б-р Шевченка, 460, м. Черкаси, 18006, Україна

ІМІТАЦІЙНА МОДЕЛЬ СИСТЕМИ ПЕРЕДАВАННЯ ІНФОРМАЦІЇ З НЕРОЗДІЛЬНИМ ФАКТОРІАЛЬНИМ КОДУВАННЯМ ДАНИХ У СЕРЕДОВИЩІ SIMULINK

Роботу присвячено розробці та дослідженню імітаційної моделі системи передавання інформації з нероздільним факторіальним кодуванням даних у середовищі Simulink. Модель у передавачі реалізує формування перестановки, кодування її символів двійковим рівномірним кодом і передавання отриманої послідовності двійковим симетричним каналом зв'язку з незалежними бітовими помилками. Приймач реалізує зворотне перетворення двійкового повідомлення в символьне. У процесі симуляції фіксується кількість правильно прийнятих і пошкоджених помилкою інформаційних повідомлень. Крім того, виконується підрахунок випадків не виявленої приймачем помилки в отриманому повідомленні. Розроблено структуру імітаційної моделі, описано етапи створення та налаштування моделі в середовищі Simulink. Отримана імітаційна модель дозволяє проводити експерименти з дослідження завадостійкості факторіального кодування даних у каналах зв'язку різної якості.

Ключові слова: *факторіальний код, перестановка, двійковий симетричний канал, імовірність помилки, моделювання.*

Вступ. Розвиток інформаційних і комунікаційних технологій невпинно впливає на сучасне життя людини. Разом з тим, відповідно до звіту [1] Державної служби спеціального зв'язку та захисту інформації України про роботу системи виявлення вразливостей і реагування на кіберінциденти та кібератаки [2] від початку війни тренд на зростання кількості кібератак зберігається. Зокрема, в ІІІ кварталі 2022 р. за допомогою засобів Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки опрацьовано 24 млрд подій. Кількість зареєстрованих і опрацьованих кіберінцидентів зросла від 64 до 115. Найпоширенішими методами кібератаки є: збір інформації зловмисником, шкідливий програмний код, втручання, порушення доступності [3]-[5]. Розвиток сучасних комп'ютерів і технологій дозволяє виконувати кібератаки на смартфоні через спеціалізоване програмне забезпечення [6] та апаратну складову. Новітні розробки відеопроцесорів дозволяють виконувати підбір паролів довжиною 8 елементів з літер нижнього та верхнього регістру, спеціальних символів і цифр методом перебору протягом 8 годин [7]. Збільшення довжини паролів накладає на користувача вимоги до збереження такого паролю не просто «в голові», а на носіях або в хмарних сховищах. Такі рішення теж вимагають захисту, шифрування та належного зберігання.

Реалізація захищеного інформаційного обміну є складовою забезпечення конфіденційності, цілісності та доступності даних в електронних комунікаційних мережах та інформаційних системах [8]. Разом з тим, процес передавання даних з обмеженим доступом каналами зв'язку передбачає одночасний захист інформації від несанкціонованого доступу та модифікації внаслідок природних чи навмисних деструктивних дій.

Підхід на основі використання нероздільного факторіального кодування даних [9]-[11] дозволяє реалізувати інтегрований захист інформації від несанкціонованого доступу та канальних помилок. Нероздільне факторіальне кодування передбачає бієктивне перетворення інформаційного повідомлення або його частини в перестановку [12] чисел $\pi = \{\pi_0, \pi_1, \ldots, \pi_{M-1}\}$ заданої довжини M. Закон перетворення учасники інформаційної взаємодії тримають у секреті. Символи перестановки кодують двійковим кодом і переда-

© Е. В. Фауре, А. Б. Скуцький, А. О. Лавданський, 2022
DOI: 10.24025/2306-4412.4.2022.273385

ють каналом зв'язку, не захищеним від підслуховування та помилок. У точці приймання виконують зворотну операцію перетворення перестановки в інформаційне повідомлення. У [10] отримано оцінку достовірності передавання перестановок, зокрема визначено ймовірність невиявленої помилки від довжини інформаційного вектора на вході кодера. Результати дослідження [13] доводять можливість використання нероздільного факторіального кодування даних у каналах з імовірністю бітової помилки, близькою до 0,5.

Для практичного використання факторіального кодування даних в інформаційних і комунікаційних системах має бути розроблений набір протоколів, які вирішують завдання синхронізації передавача й приймача, встановлення зв'язку, узгодження ключів, контролю достовірності інформації. Такі протоколи дозволять надалі використовувати їх в апаратній складовій систем захищеного передавання даних.

Разом з тим, для мінімізації часу та ресурсів розробника всі рішення в протоколах інформаційного обміну, зокрема на основі нероздільного факторіального кодування даних, першочергово мають бути відпрацьовані на відповідних комп'ютерних моделях, адже комп'ютерне моделювання в сучасному світі стало одним із невід'ємних факторів у життєвому циклі виробу.

Мета та задачі дослідження. Метою дослідження є створення імітаційної моделі системи передавання інформації з нероздільним факторіальним кодуванням даних у середовищі Simulink [14] для верифікації теоретичних показників достовірності передавання та подальшого дослідження ефективності застосованих у системі протоколів. Для досягнення поставленої мети необхідно виконати такі завдання:

- визначити структуру моделі та реалізувати її в середовищі Simulink;
- визначити перелік експериментів;
- побудувати імітаційну модель за визначеною структурою;
- реалізувати експериментальні дослідження з передавання даних каналами різної якості;
- виконати порівняння отриманих результатів з теоретичними.

Виклад основного матеріалу. Структурна схема імітаційної моделі системи передавання інформації з нероздільним факторіальним кодуванням даних має вигляд, наведений на рисунку 1.

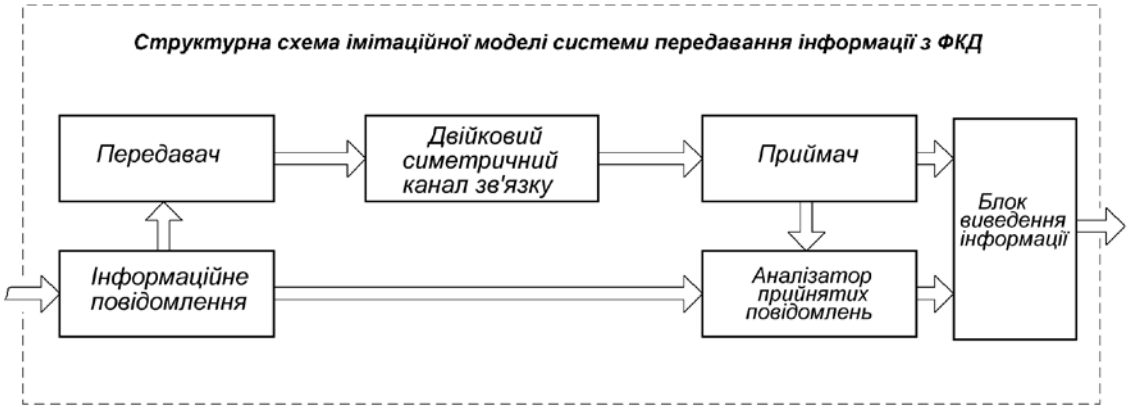

Рисунок 1. Структурна схема імітаційної моделі

Реалізація імітаційної моделі у середовищі Simulink. Розглянемо функціональні складові імітаційної моделі системи передавання перестановки двійковим симетричним каналом з визначеною ймовірністю бітової помилки (рисунок 2).

Перестановка для передавання – повідомлення, бієктивно відображене на перестановку. За довжини перестановки M потужність множини всіх перестановок дорівнює $M!$, а тому передавач може сформувати до $M!$ різних повідомлень.

Двійковий симетричний канал зв'язку (Channel) – канал передавання двійкових даних з однаковою перехідною ймовірністю p_0.

Передавач (serial transmitter) – виконує послідовне, побітове передавання перестановки в двійковий симетричний канал зв'язку.

© Е. В. Фауре, А. Б. Скуцький, А. О. Лавданський, 2022
DOI: 10.24025/2306-4412.4.2022.273385

Вхідні сигнали: pData – перестановка-повідомлення; CLK – сигнал тактування. Вихідні сигнали: sTx – біти інформаційного повідомлення, які надходять до каналу зв'язку; TxOk – сигнал завершення передавання всіх елементів перестановки в канал зв'язку. Сигнал формується після передавання останнього біту інформаційного повідомлення.

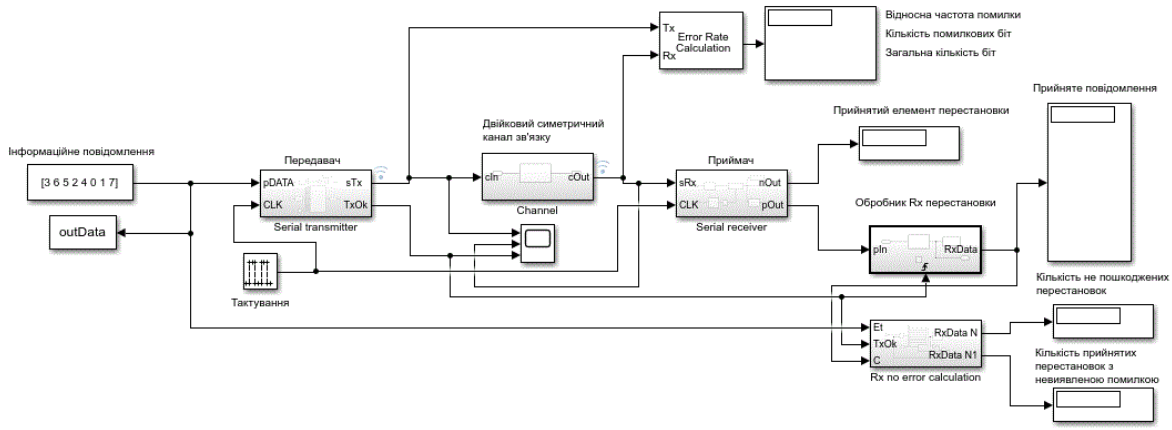

Рисунок 2. Модель системи передавання перестановки каналом зв'язку

Приймач (serial reciever) – виконує послідовне, побітове приймання перестановки з каналу зв'язку. Вхідні сигнали: sRx – перестановка-повідомлення, яка послідовно надходить з каналу зв'язку; CLK – сигнал тактування. Вихідні сигнали: nOut – елемент перестановки, отриманий приймачем; pOut – перестановка, отримана приймачем.

Обробник Rx перестановки – приводить отриману з двійкового симетричного каналу зв'язку перестановку до початкового вигляду. Наприклад, у результаті передавання перестановки (формула (1))

$$\pi = \{\pi_0, \pi_1, \ldots, \pi_{M-1}\}, \qquad (1)$$

передавачем у двійковий симетричний канал *приймач* отримує символи перестановки у зворотній послідовності – $\pi = \{\pi_M, \pi_{M-1}, \ldots, \pi_0\}$.

Лічильник прийнятих перестановок (Rx no error calculation) – рахує кількість перестановок, що співпадають з відправленими, а також фіксує кількість перестановок з невиявленою помилкою. Вхідні сигнали: Et – еталонне значення переданої перестановки (*перестановка для передавання)*; C – отримана приймачем перестановка; TxOk – сигнал завершення передавання всіх елементів перестановки в канал зв'язку. Вихідні сигнали: Rx Data N – кількість непошкоджених перестановок, Rx Data N 1 – кількість перестановок з невиявленою помилкою.

Лічильник неправильно прийнятих бітів (Error Rate Calculation) – рахує кількість помилкових бітів на виході двійкового симетричного каналу зв'язку. Вхідні сигнали: Tx – сигнал з виходу приймача, ідентичний sTx; Rx – сигнал на виході каналу (вході приймача), ідентичний cOut, sRx.

Блок тактування – формує сигнал CLK для функціонування моделі.

Дисплеї відображення даних та *осцилограф* – слугують для виводу проміжних і остаточних результатів моделювання.

Налаштування імітаційної моделі. Розглянемо головні налаштування імітаційної моделі системи передавання перестановки двійковим симетричним каналом зв'язку за довжини перестановки $M = 8$. Для рівномірного кодування символів перестановки кодова комбінація кожного символу містить три біти.

Налаштування моделі містяться в меню MODELING → Model setting (рисунок 3).

Основні налаштування (рисунок 3):

- simulation (stop time) – кінцевий час для зупинки симуляції, значення обраховується за формулою

$$Stop\,time = \left(\frac{1}{f_{txrx}} \cdot M \cdot l_r\right) \cdot N + \frac{1}{f_{txrx}}, \qquad (2)$$

де f_{txrx} – частота передавання (у роботі прийнято $f_{txrx} = 10^3\ Гц$);

© Е. В. Фауре, А. Б. Скуцький, А. О. Лавданський, 2022
DOI: 10.24025/2306-4412.4.2022.273385

M – довжина перестановки (у роботі прийнято $M = 8$);

l_r – кількість бітів для кодування одного елемента перестановки, $\lceil \log_2 M \rceil = 3$;

N – кількість тестових передавань перестановки;

$\frac{1}{f_{txrx}}$ – час для оцінки отримання даних;

- solver selection (type: fixed-step) – фіксований крок симуляції;
- solver selection (solver: discrete) – дискретний обробник моделі;
- fundamental sample time – мінімальний проміжок часу в режимі симуляції. Для передавання з частотою f_{txrx} цей параметр має бути в два рази вищий – $2 \cdot f_{txrx}$.

Приклад налаштування блоку тактування зображено нижче (рисунок 4).

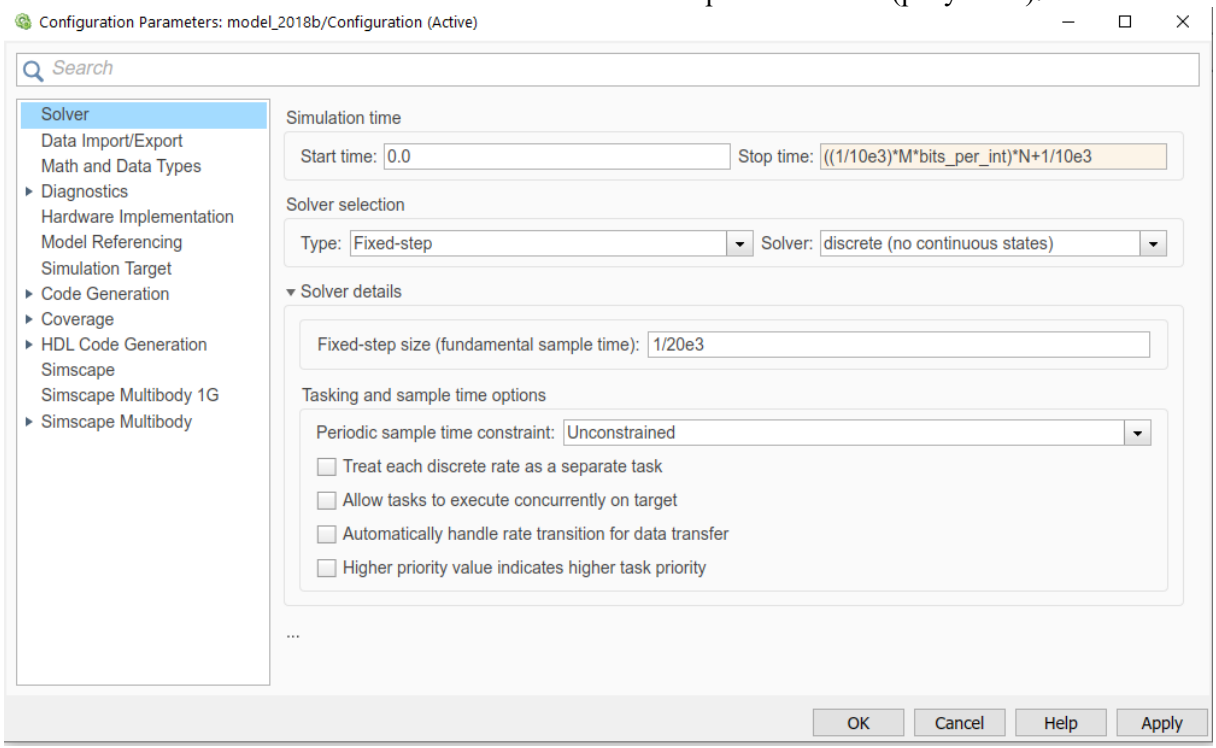

Рисунок 3. Параметри симуляції моделі

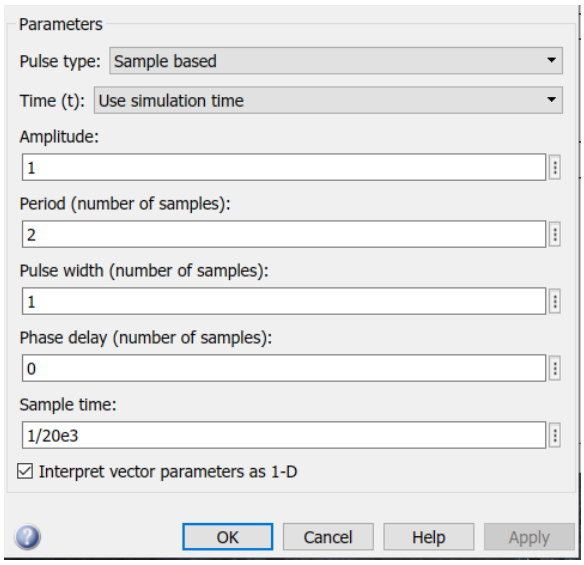

Рисунок 4. Налаштування блоку тактування

© Е. В. Фауре, А. Б. Скуцький, А. О. Лавданський, 2022
DOI: 10.24025/2306-4412.4.2022.273385

Підсистеми імітаційної моделі. *Передавач (serial transmitter)* виконує послідовне, побітове передавання даних. Передавач містить (рисунок 5): блок перетворення даних (integer to bit converter), лічильник тактування (counter), мультиплексор, блок перетворення даних (boolean), блок формування затримки сигналу (delay), блок відображення (display), блок порівняння (compare to constant), вхідні та вихідні порти.

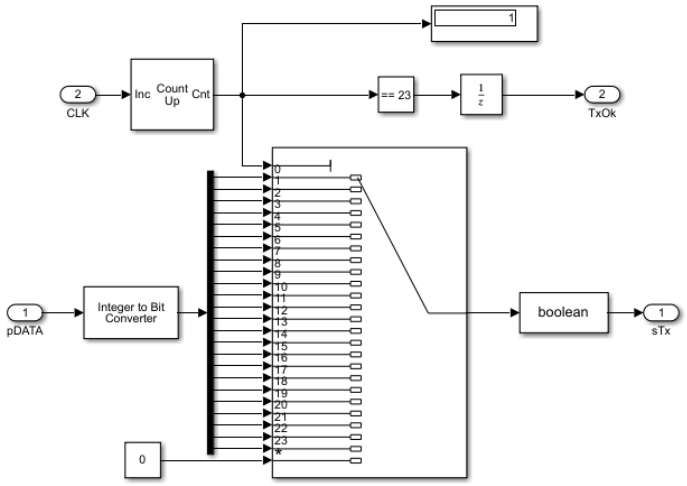

Рисунок 5. Передавач (serial transmitter)

Підсистема отримує сигнал тактування ззовні через порт CLK на лічильник (налаштування лічильника представлено на рисунку 6). На вхідний порт pDATA надходить перестановка для передавання. За визначених M і l_r кількість біт n, відповідно, тактових імпульсів для передавання однієї перестановки становить

$$n = M \cdot l_r = 8 \cdot 3 = 24. \quad (3)$$

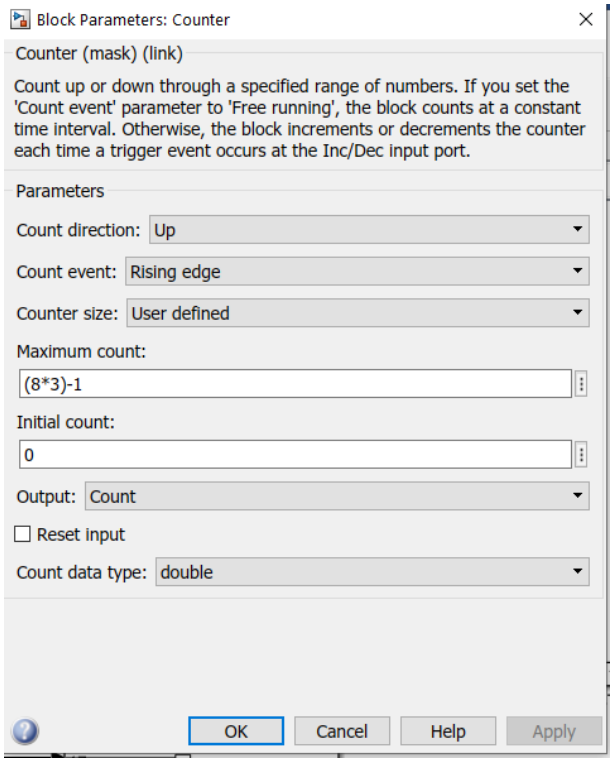

Рисунок 6. Налаштування блоку лічильника

© Е. В. Фауре, А. Б. Скуцький, А. О. Лавданський, 2022
DOI: 10.24025/2306-4412.4.2022.273385

Перестановка надходить на блок перетворювача *integer to bit*, де кожний елемент перестановки перетворюється в двійковий вигляд із заданою довжиною кодової комбінації l_r (рисунок 7).

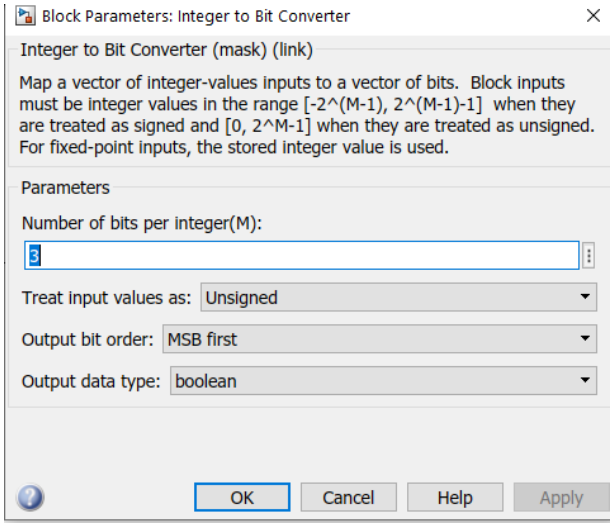

Рисунок 7. Налаштування блоку integer to bit

Послідовність біт перестановки надходить через шину до мультиплексора на 24 входи. Вихід лічильника з'єднано з адресним входом мультиплексора. Залежно від кількості обрахованих імпульсів лічильником кожен із входів мультиплектора з'єднується з його виходом. Сигнал даних з мультиплексора побітово передається на вихідний порт sTx під дією сигналу тактування. Вихідний сигнал TxOk формується після передавання останнього, 24-го (для $l_r = 3$, див. формулу (2)) біту на вихідний порт sTx.

Приймач (serial reciever) отримує бітову послідовність, передану каналом зв'язку, декодує її та формує вихідне інформаційне повідомлення. Приймач містить (рисунок 8): *n*-бітовий запам'ятовувальний пристрій (*serial-in parallel-out bits*), детектор елемента перестановки, підсистему перетворення двійкового представлення в десяткове (*convert to int*), блок формування перестановки (рисунок 9), порти вхідних і вихідних даних.

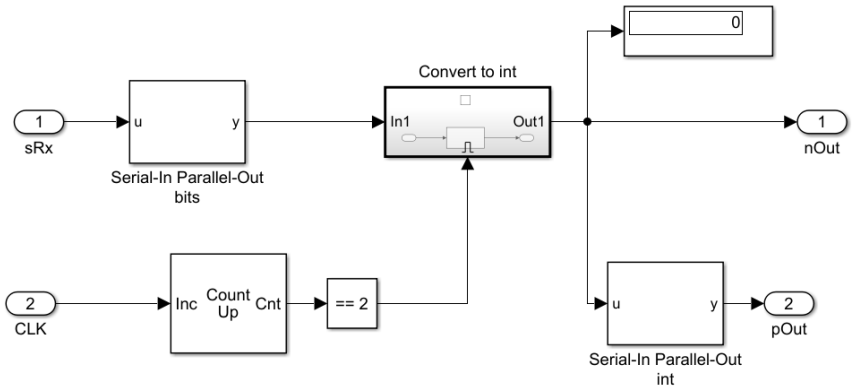

Рисунок 8. Приймач (serial reciever)

© Е. В. Фауре, А. Б. Скуцький, А. О. Лавданський, 2022
DOI: 10.24025/2306-4412.4.2022.273385

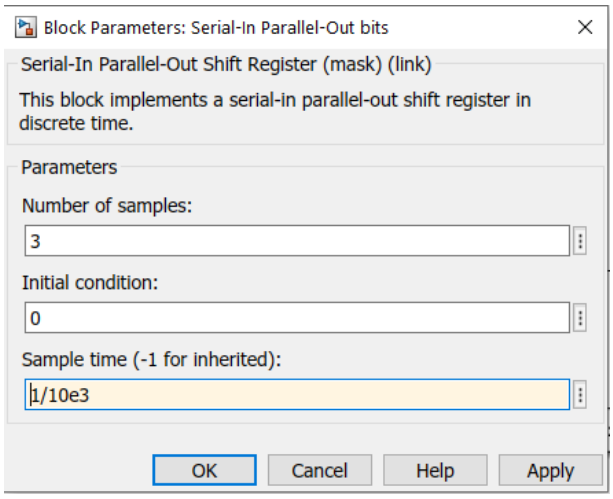

Рисунок 9. Налаштування блоку формування перестановки

Сигнал тактування CLK та дані sRx потрапляють на *n*-бітовий запам'ятовувальний пристрій. Сигнал тактування CLK також надходить до детектора елемента перестановки – лічильника. Лічильник обраховує кількість бітів, що надійшла через вхідний порт sRx, і формує сигнал дозволу перетворення даних з двійкового в десяткове представлення для підсистеми *convert to int* (рисунок 10). Налаштування блоку *bit to integer converter* представлено на рисунку 11.

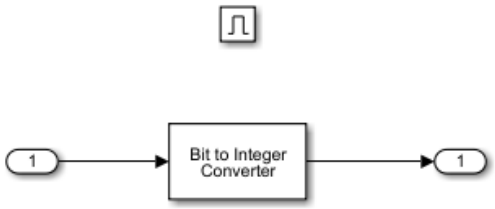

Рисунок 10. Підсистема перетворення даних з двійкового в десяткове представлення

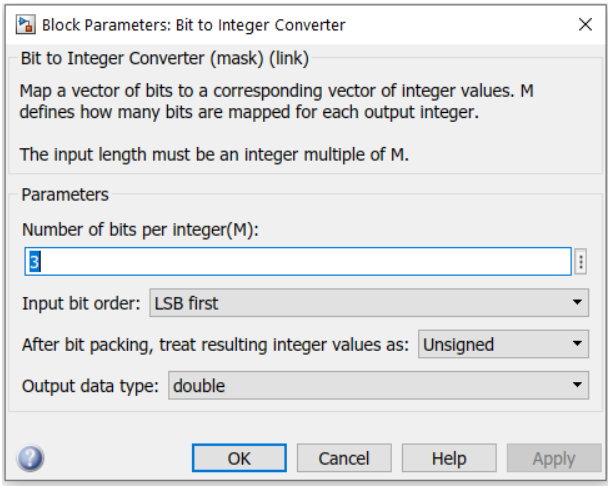

Рисунок 11. Налаштування підсистеми перетворення даних з двійкового в десяткове представлення

Обробник Rx перестановки впорядковує прийняті елементи перестановки. Отримана підсистемою перестановка приводиться до початкового вигляду за формулою (1), алгоритм упорядкування реалізовано окремою функцією MATLAB з вхідними даними *u* та вихідними *y*. Підсистема також виконує запис до зовнішнього файлу прийнятих перестановок. Підсистема є тригерною, тобто спрацьовує за сигналом TxOk.

© Е. В. Фауре, А. Б. Скуцький, А. О. Лавданський, 2022
DOI: 10.24025/2306-4412.4.2022.273385

Обробник Rx перестановки містить (рисунок 12): функцію впорядкування елементів перестановки (pResort), блок збереження даних до зовнішнього файлу inData, вхідні та вихідні порти.

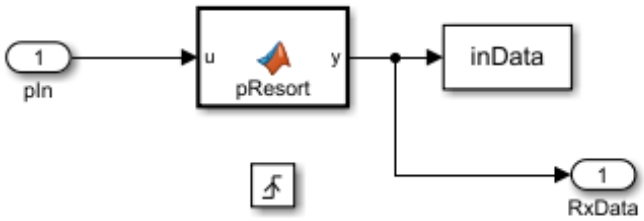

Рисунок 12. Обробник Rx перестановки

Лічильник прийнятих перестановок (Rx no error calculation) порівнює відправлену перестановку з отриманою, веде підрахунок кількості перестановок, які ідентичні вхідному інформаційному повідомленню, окремо фіксує отримані перестановки з невиявленою помилкою, які є перестановками, проте не ідентичні відправленому інформаційному повідомленню.

Лічильник містить (рисунок 13): блок порівняння, аналізатор елементів перестановок, лічильник перестановок, не пошкоджених помилкою, підсистему фіксації невиявлених пошкоджених перестановок (рисунок 14), вхідні та вихідні порти.

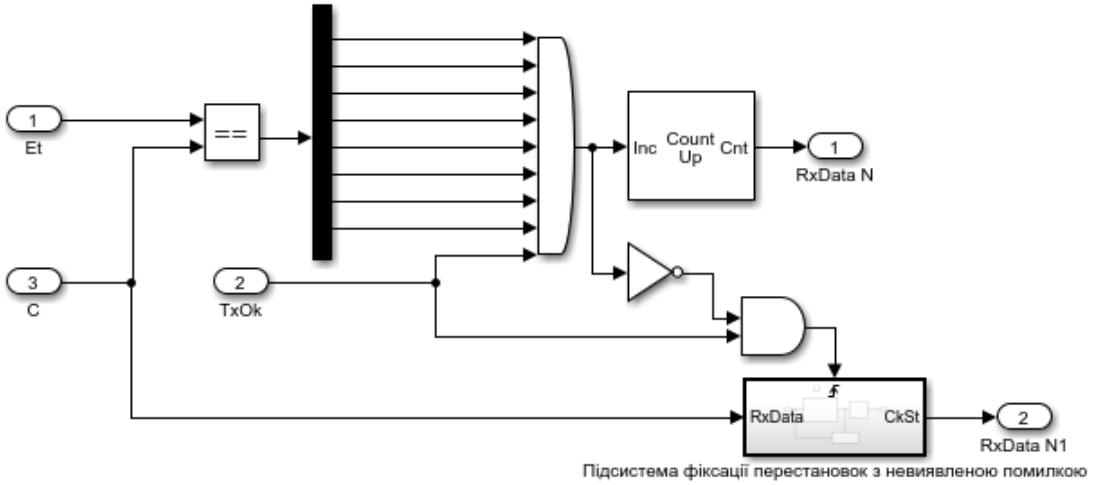

Рисунок 13. Лічильник прийнятих перестановок (Rx no error calculation)

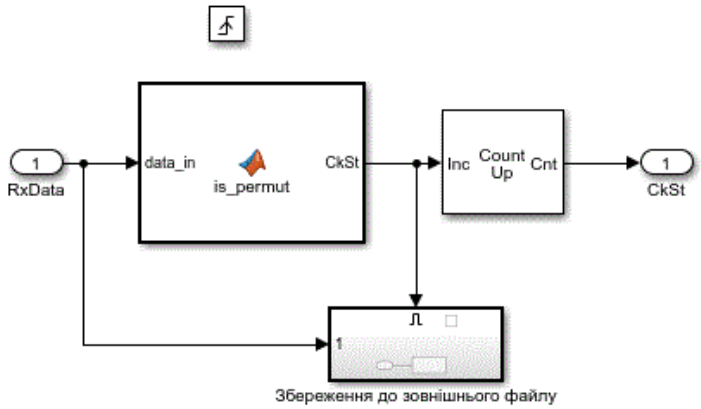

Рисунок 14. Підсистема фіксації перестановок з невиявленою помилкою

© Е. В. Фауре, А. Б. Скуцький, А. О. Лавданський, 2022
DOI: 10.24025/2306-4412.4.2022.273385

На вхід підсистеми *Rx no error calcuation* надходять дві перестановки: перестановка для передавання (порт Et) та перестановка на виході двійкового симетричного каналу (порт C). Ці перестановки потрапляють до блоку порівняння, в якому кожний елемент перестановки оброблюється за заданою умовою

$$C\ \&Et = \left[C_M, C_{M-1}, \ldots, C_1\right] \& \\ \&\left[Et_M, Et_{M-1}, \ldots, Et_1\right] \& \left[TxOk\right] = \\ = \begin{bmatrix} \left(C_M\right) \& \left(Et_M\right), \left(C_{M-1}\right) \& \left(Et_{M-1}\right), \ldots \\ \ldots, \left(C_1\right) \& \left(Et_1\right) \end{bmatrix} \& \\ \& \left(TxOk\right). \qquad (4)$$

де $C\ \&Et$ – логічний сигнал, що потрапляє на лічильник перестановок, не пошкоджених помилкою. Сигнал формується за умови співпадання всіх елементів перестановки, отриманих приймачем, з початковими елементами вхідної перестановки;

C_M – перестановка на виході двійкового симетричного каналу зв'язку;

Et – перестановка для передавання.

У результаті аналізу заданої блоком порівняння умови (елементи повинні співпадати) формуються логічні сигнали: логічна «1», якщо елементи задовольняють умову, логічний «0», якщо елементи не задовольняють умову. Приклад функціонування блоку порівняння за формулою (4) наведено на рисунку 15.

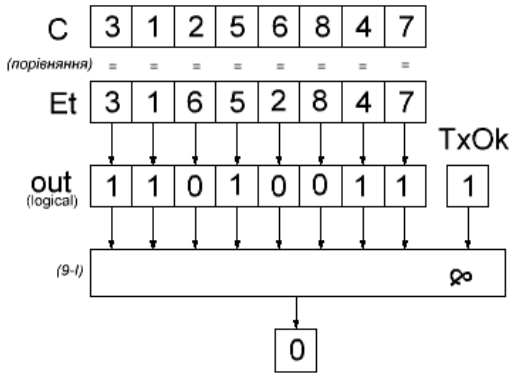

Рисунок 15. Приклад формування сигналу підрахунку кількості перестановок без канальної помилки

Опис алгоритму підрахунку перестановок, не пошкоджених помилкою. До аналізатора елементів перестановок (логічний елемент AND на 9 входів) надходить отриманий вектор логічних значень (рисунок 15, *out*). У результаті виконання логічної умови (формула (4)) та наявності сигналу передавання останнього біту поточної перестановки через порт TxOk формується сигнал лічильника про те, що перестановку з M елементів передано правильно. За умови неспівпадіння хоча б одного елемента перестановки сигнал не формується. Кількість отриманих сигналів після аналізатора елементів перестановок фіксується лічильником, а результат підрахунку виводиться на дисплей через вихідний порт RxData N.

Підсистема фіксації перестановок з невиявленою помилкою. Склад підсистеми (рисунок 14): функція *is_permut*, лічильник перестановок з невиявленою помилкою, підсистема збереження зафіксованих перестановок до зовнішнього файлу, вхідні/вихідні порти. Функція *is_permut* виконує роль аналізатора даних, отриманих з входу RxData. Функція повертає логічну одиницю, якщо вхідна послідовність є перестановкою. Кількість сформованих сигналів фіксується лічильником, значення лічильника надходить на вихідний порт RxData N1.

Підсистема фіксації перестановок з невиявленою помилкою отримує сигнал на виконання від підсистеми *Rx no error calculation* за таких умов:

– отримана перестановка через вхідний порт C не співпадає з відправленою перестановкою (вхідний порт Et);

– відбулося передавання останнього біту в канал зв'язку (сигнал TxOk).

© Е. В. Фауре, А. Б. Скуцький, А. О. Лавданський, 2022
DOI: 10.24025/2306-4412.4.2022.273385

Двійковий симетричний канал зв'язку (Channel) містить (рисунок 16): блок binary symmetric channel (BSC), вхідні та вихідні порти.

Рисунок 16. Двійковий симетричний канал зв'язку (*Channel*)

До головних налаштувань блоку BSC входять (рисунок 17): імовірність помилки (*Error probability*) від 0 до 1; початкове «зерно» (*initial seed*) використовується для генерації псевдовипадковості.

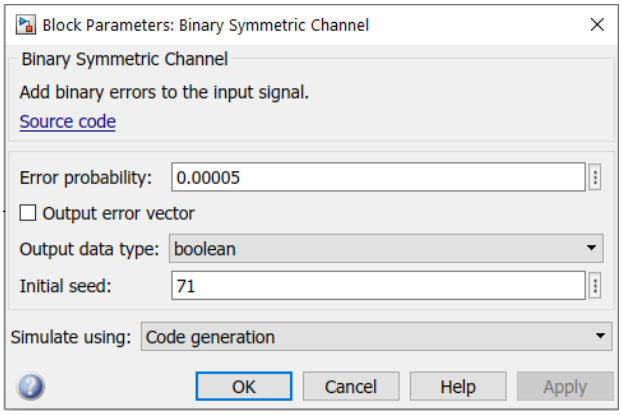

Рисунок 17. Налаштування binary symmetric channel

Результати досліджень. За створеною імітаційною моделлю системи передавання перестановок двійковим симетричним каналом за довжини перестановки $M = 8$ і рівномірного кодування її символів проведемо симуляцію передавання $N = 10000$ перестановок для каналів з різними ймовірностями бітових помилок: $p_0 = 0.05$ (експеримент № 1), $p_0 = 0.1$ (експеримент № 2), $p_0 = 0.15$ (експеримент № 3). Виконаємо аналіз отриманих результатів за допомогою інструменту Data Inspection.

Опис і результати експерименту № 1. Імовірність бітової помилки $p_0 = 0.05$, *initial seed* – 666, вхідна перестановка $\pi = [3,6,5,2,4,0,1,7]$.

Кількість перестановок, отриманих без пошкодження помилкою, дорівнює $N_{noerr}(0.05) = 2929$. Кількість перестановок з невиявленою помилкою становила $N_{ud}(0.05) = 110$. Кількість перестановок, пошкоджених помилкою та перетворених у неперестановку, дорівнює $N_{det}(0.05) = 6961$ (рисунок 18).

Дослідимо проілюстровані на рисунку 18 дані. Верхній графік демонструє сигнали на вході та на виході каналу зв'язку. Вісь абсцис позначає час симуляції. Відмінності в сигналах на вході та на виході каналу зв'язку зафіксовано на нижньому графіку. Відхилення приймає значення з множини $\{-1;1\}$. Значення «-1» означає наявність логічного нуля в отриманих даних замість логічної одиниці, «1» – наявність логічної одиниці в отриманих даних, де повинен бути логічний нуль.

© Е. В. Фауре, А. Б. Скуцький, А. О. Лавданський, 2022
DOI: 10.24025/2306-4412.4.2022.273385

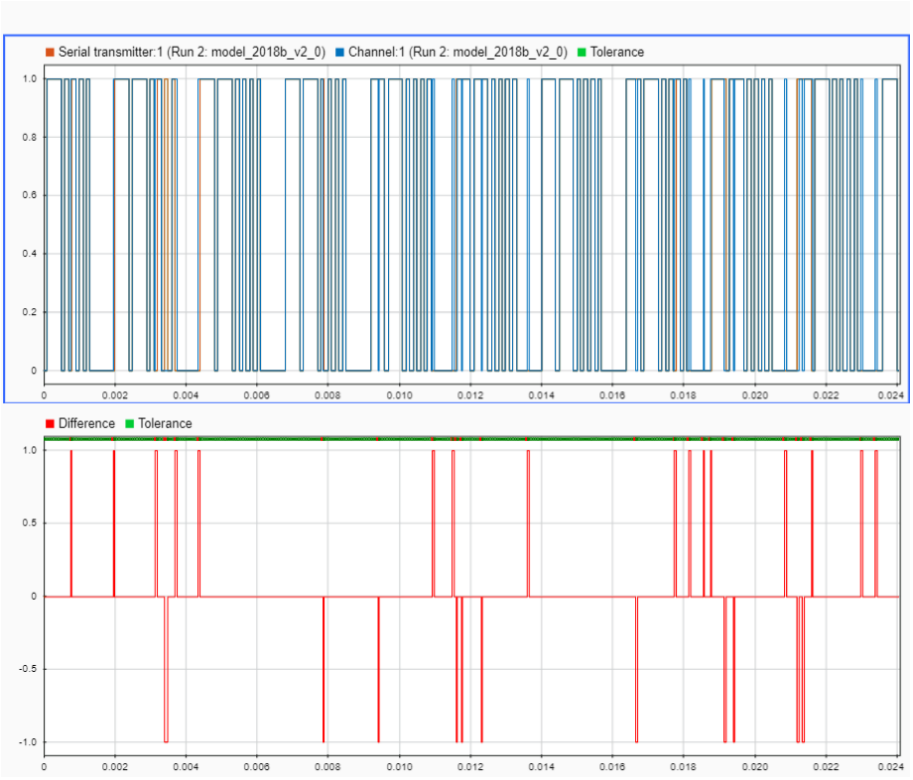

Рисунок 18. Графік Data Inspection за ймовірності бітової помилки $p_0 = 0.05$ (наведено перші 10 блоків інформаційного повідомлення)

Рисунок 19 демонструє відомості про статистичні показники передавання під час симуляції. У результаті проведення експерименту № 1 маємо: відносна частота появи бітової помилки $w(0.05) = 0.0491$, кількість помилкових бітів – $1.179 \cdot 10^4$, загальна кількість переданих і прийнятих бітів – $2.4 \cdot 10^5$.

Абсолютне відхилення значення відносної частоти появи бітової помилки від заданої в параметрах (рисунок 19) p_0 з імовірністю $\gamma = 0.95$ не повинно виходити за межі:

$$\left| w(p_0) - p_0 \right| \le \varepsilon = 1.96 \sqrt{\frac{p_0 (1 - p_0)}{N}}. \qquad (5)$$

Рисунок 19. Результати передавання бітів каналом зв'язку

Інакше кажучи, відносна частота появи бітової помилки з імовірністю $\gamma = 0.95$ повинна потрапляти у відрізок

$$p_0 - 1.96 \sqrt{\frac{p_0 (1 - p_0)}{N}} \le w(p_0) \le p_0 + 1.96 \sqrt{\frac{p_0 (1 - p_0)}{N}}. \qquad (6)$$

Для $p_0 = 0.05$ вираз (формула (6)) набуває вигляду: $0.0457 \le w(0.05) \le 0.0543$, а значення відносної частоти $w(0.05) = 0.0498$ потрапляє в цей відрізок. Відносна частота перестановок з виявленою помилкою в експерименті № 1 становила $W_{det}(0.05) = N_{det}(0.05)/N = 0.6961$. Відносна частота перестановок з невиявленою помилкою – $W_{ud}(0.05) = N_{ud}(0.05)/N = 0.0110$.

Опис і результати експерименту № 2. Імовірність бітової помилки $p_0 = 0.1$, *initial seed* – 53, вхідна перестановка

© Е. В. Фауре, А. Б. Скуцький, А. О. Лавданський, 2022
DOI: 10.24025/2306-4412.4.2022.273385

$\pi = [3,6,5,2,4,0,1,7]$. Кількість перестановок, отриманих без пошкодження помилкою, дорівнює $N_{noerr}(0.1) = 768$. Кількість перестановок з невиявленою помилкою становила $N_{ud}(0.1) = 139$. Кількість перестановок, пошкоджених помилкою та перетворених у неперестановку, дорівнює $N_{det}(0.1) = 9093$, (рисунок 20).

Для $p_0 = 0.1$ вираз (формула (6)) набуває вигляду: $0.0941 \le w(0.1) \le 0.1059$, а значення відносної частоти $w(0.1) = 0.1006$ потрапляє в цей відрізок. Відносна частота перестановок з виявленою помилкою в експерименті № 2 становила $W_{det}(0.1) = N_{det}(0.1)/N = 0.9093$. Відносна частота перестановок з невиявленою помилкою – $W_{ud}(0.1) = N_{ud}(0.1)/N = 0.0139$ (рисунок 21).

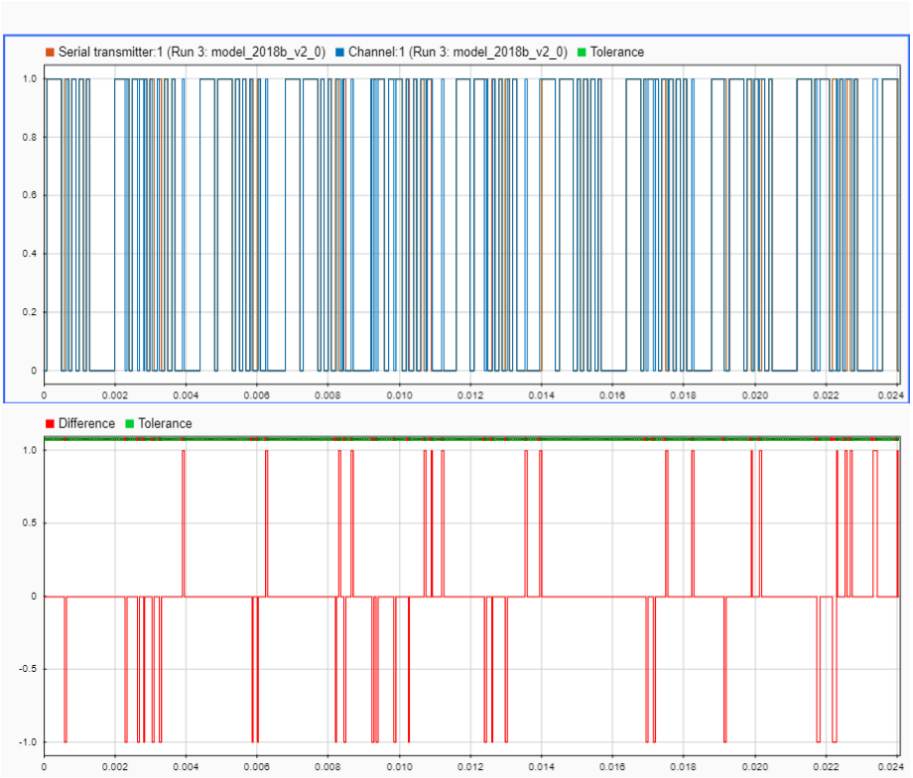

Рисунок 20. Графік Data Inspection за ймовірності бітової помилки $p_0 = 0.1$ (наведено перші 10 блоків інформаційного повідомлення)

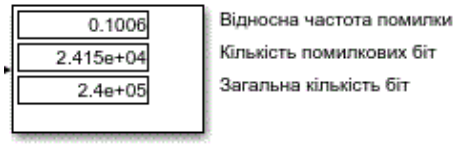

Рисунок 21. Результати передавання бітів каналом зв'язку

Опис і результати експерименту № 3. Імовірність бітової помилки $p_0 = 0.15$, *initial seed* – 74, вхідна перестановка $\pi = [3,6,5,2,4,0,1,7]$. Кількість перестановок, отриманих без пошкодження помилкою, дорівнює $N_{noerr}(0.15) = 215$. Кількість перестановок з невиявленою помилкою становила $N_{ud}(0.15) = 94$. Кількість перестановок, пошкоджених помилкою та перетворених у неперестановку, дорівнює $N_{det}(0.15) = 9691$, (рисунок 22).

Для $p_0 = 0.15$ вираз (формула (6)) набуває вигляду: $0.1430 \le w(0.15) \le 0.1570$, а значення відносної частоти $w(0.15) = 0.1499$ потрапляє в цей відрізок. Відносна частота перестановок з виявленою помилкою в експерименті № 3 становила

© Е. В. Фауре, А. Б. Скуцький, А. О. Лавданський, 2022
DOI: 10.24025/2306-4412.4.2022.273385

$W_{det}(0.15) = N_{det}(0.15)/N = 0.9691$. Відносна частота перестановок з невиявленою помилкою – $W_{ud}(0.15) = N_{ud}(0.15)/N = 0.0094$ (рисунок 23).

Рисунок 22. Графік Data Inspection за ймовірності бітової помилки $p_0 = 0.15$ (наведено перші 10 блоків інформаційного повідомлення)

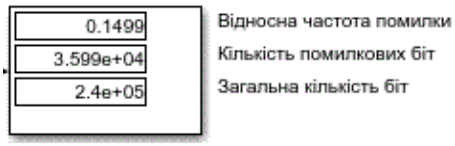

Рисунок 23. Результати передавання бітів каналом зв'язку

Обговорення результатів. Побудована імітаційна модель дозволила дослідити вплив канальної помилки на інформаційні повідомлення. У результаті проведення трьох експериментів отримано такі результати відносної частоти пошкодження перестановки та перетворення її в неперестановку (виявлення помилки в отриманій перестановці): експеримент № 1 – $W_{det}(0.05) = 0.6961$ за $p_0 = 0.05$, експеримент № 2 – $W_{det}(0.1) = 0.9093$ за $p_0 = 0.1$, експеримент № 3 – $W_{det}(0.15) = 0.9691$ за $p_0 = 0.15$.

Відносна частота не виявленої в отриманій перестановці помилки дорівнює: $W_{ud}(0.05) = 0.0110$, $W_{ud}(0.1) = 0.0139$, $W_{ud}(0.15) = 0.0094$.

Відносна частота отримання перестановки без помилок дорівнює: $W_{noerr}(0.05) = 0.2929$, $W_{noerr}(0.1) = 0.0768$, $W_{noerr}(0.15) = 0.0215$.

Імовірність отримання перестановки без помилок дорівнює

$$Q(p_0) = (1 - p_0)^{24}. \qquad (7)$$

Для $p_0 \in \{0.05, 0.1, 0.15\}$ ця ймовірність набуває значень $Q(0.05) = 0.2920$, $Q(0.1) = 0.0798$, $Q(0.15) = 0.0202$.

Абсолютне відхилення значення відносної частоти отримання перестановки без помилок від теоретично визначеної ймовірності (7) з імовірністю $\gamma = 0.95$ не повинно виходити за межі:

© Е. В. Фауре, А. Б. Скуцький, А. О. Лавданський, 2022
DOI: 10.24025/2306-4412.4.2022.273385

$$\left|W_{noerr}(p_0)-Q(p_0)\right| \le \mathrm{E} = 1.96\sqrt{\frac{Q(p_0)\left(1-Q(p_0)\right)}{N}}. \quad (8)$$

Інакше кажучи, відносна частота отримання перестановки без помилок з імовірністю $\gamma = 0.95$ повинна потрапляти у відрізок

$$\begin{cases} W_{noerr}(p_0) \ge Q(p_0) - 1.96\sqrt{\dfrac{Q(p_0)\left(1-Q(p_0)\right)}{N}}, \\ W_{noerr}(p_0) \le Q(p_0) + 1.96\sqrt{\dfrac{Q(p_0)\left(1-Q(p_0)\right)}{N}}. \end{cases} \quad (9)$$

Для $p_0 \in \{0.05, 0.1, 0.15\}$ вираз (формула (9)) отримує вигляд:

$0.2831 \le W_{noerr}(0.05) \le 0.3009$,

$0.0745 \le W_{noerr}(0.1) \le 0.0851$,

$0.0175 \le W_{noerr}(0.15) \le 0.0230$. Як видно, отримані експериментальні показники лежать у визначених межах.

Довірчий інтервал для ймовірності невиявленої помилки в перестановці за відомою відносною частотою $W_{ud}(p_0)$ з надійністю $\gamma = 0.95$

$$\begin{cases} P_{ud}(p_0) \ge W_{ud}(p_0) - 1.96\sqrt{\dfrac{W_{ud}(p_0)\left(1-W_{ud}(p_0)\right)}{N}}, \\ P_{ud}(p_0) \le W_{ud}(p_0) + 1.96\sqrt{\dfrac{W_{ud}(p_0)\left(1-W_{ud}(p_0)\right)}{N}}. \end{cases} \quad (10)$$

Таким чином, для $p_0 \in \{0.05, 0.1, 0.15\}$ і $\gamma = 0.95$ маємо:

$0.0090 \le P_{ud}(0.05) \le 0.0130$,

$0.0116 \le P_{ud}(0.1) \le 0.0162$,

$0.0075 \le P_{ud}(0.15) \le 0.0113$.

Зауважимо, що наявність невиявлених помилок в отриманих повідомленнях може призводити до аварійних ситуацій (стоп програми, некоректне розпізнавання даних) на стороні приймача. За високої ймовірності бітової помилки в каналі зв'язку отримані оцінки ймовірності невиявленої помилки факторіальним кодом з відновленням даних за перестановкою можуть не задовольняти поставленим вимогам і тому вимагати додаткових методів підвищення достовірності.

Висновки. У роботі розроблено структуру та створено модель системи передавання інформації з нероздільним факторіальним кодуванням даних, яка за рахунок реалізації процедур бієктивного перетворення інформаційного повідомлення в перестановку дозволяє дослідити вплив помилки в каналі зв'язку на достовірність отриманої інформації.

Результати експериментальних досліджень передавання інформаційного повідомлення двійковим симетричним каналом зв'язку з заданими ймовірностями бітової помилки $p_0 \in \{0.05, 0.1, 0.15\}$ свідчать про їх відповідність теоретичним показникам, що свідчить про адекватність побудованої моделі. Визначено довірчий інтервал для ймовірності невиявленої помилки в залежності від p_0.

Розроблена імітаційна модель системи передавання інформації з нероздільним факторіальним кодуванням даних дозволяє досліджувати та відпрацьовувати надалі методи підвищення достовірності та завадостійкості інформації.

Предметом подальших досліджень є розширення запропонованої моделі системи передавання інформації з нероздільним факторіальним кодуванням даних до моделі захищеного інформаційного обміну з використанням трьохетапного криптографічного протоколу на основі перестановок [15].

Список використаних джерел

[1] *Звіт про роботу системи виявлення вразливостей і реагування на кіберінциденти та кібератаки*, Оперативний центр реагування на кіберінциденти державного центру кіберзахисту державної служби спеціального зв'язку та захисту інформації України, 2022(Q3), 2022. [Електронний ресурс]. Режим доступу: https://scpc.gov.ua/api/docs/4eeb6a10-b7aa-4396-8b04-e0e4b7fca1ba/4eeb6a10-b7aa-4396-8b04-e0e4b7fca1ba.pdf

[2] *Постанова Кабінету Міністрів України № 1295, груд. 23, 2020, Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки*. [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/1295-2020-%D0%BF#Text

[3] "Статистика кібератак за чотири місяці війни". *Держспецзв'язку.* [Електронний ресурс]. Режим доступу: https://www.kmu.gov.ua/news/derzhspeczvyazku-statistika-kiberatak-za-chotiri-misyaci-vijni.

© Е. В. Фауре, А. Б. Скуцький, А. О. Лавданський, 2022
DOI: 10.24025/2306-4412.4.2022.273385

[4] "Кібератаки групи UAC-0118 – дослідження CERT-UA", *Державна служба спеціального зв'язку та захисту інформації України*. [Електронний ресурс]. Режим доступу: https://cip.gov.ua/ua/news/kiberataki-grupi-uac-0118-doslidzhennya-cert-ua

[5] "Які російські та проросійські хакери атакують Україну", *Державна служба спеціального зв'язку та захисту інформації України*. [Електронний ресурс]. Режим доступу: https://cip.gov.ua/ua/news/yaki-rosiiski-ta-prorosiiski-khakeri-atakuyut-ukrayinu

[6] "Kali Linux". [Online]. Available: https://www.kali.org/

[7] "Are your passwords in the green?" [Online]. Available: https://www.hivesystems.io/blog/are-your-passwords-in-the-green

[8] *Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України № 601, черв. 2021, Методичні рекомендації щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури.* [Електронний ресурс]. Режим доступу: https://cip.gov.ua/ua/news/nakaz-ad-2021-10-06-601

[9] Э. В. Фауре, "Факториальное кодирование с исправлением ошибок", *Радіоелектроніка, інформатика, управління*, № 3, с. 130-138, 2017. doi: 10.15588/1607-3274-2017-3-15.

[10] Э. В. Фауре, "Факториальное кодирование с восстановлением данных", *Вісник Черкаського державного технологічного університету*, № 2, с. 33-39, 2016.

[11] J. Al-Aazzeh, B. Ayyoub, E. Faure, V. Shvydkyi, O. Kharin, and A. Lavdanskyi, "Telecommunication systems with multiple access based on data factorial coding", *International Journal on Communications Antenna and Propagation*, vol. 10, no. 2, pp. 102-113, 2020. doi: 10.15866/irecap.v10i2.17216.

[12] M. Bóna, *Combinatorics of Permutations*. CRC Press, 2022.

[13] E. Faure, A. Shcherba, B. Stupka, I. Voronenko, and A. Baikenov, "A method for reliable permutation transmission in short-packet communication systems', in *Information Technology for Education, Science and Technics. Lecture Notes in Computational Science and Engineering*, (in press), 2022.

[14] D. K. Chaturvedi, *Modeling and Simulation of Systems Using MATLAB® and Simulink®*. CRC press, 2017.

[15] A. Shcherba, E. Faure, and O. Lavdanska, "Three-pass cryptographic protocol based on permutations", in *2020 IEEE 2nd Int. Conf. on Advanced Trends in Information Theory (ATIT)*, 2020, pp. 281-284. doi: 10.1109/ATIT50783.2020.9349343.

References

[1] *Report on the work of the system for detecting vulnerabilities and responding to cyber incidents and cyber attacks*, Operational center for responding to cyber incidents of the state cyber protection center of the state service of special communications and information protection of Ukraine, 2022(Q3), 2022. [Online]. Available: https://scpc.gov.ua/api/docs/4eeb6a10-b7aa-4396-8b04-e0e4b7fca1ba/4eeb6a10-b7aa-4396-8b04-e0e4b7fca1ba.pdf [in Ukrainian].

[2] *Resolution of the Cabinet of Ministers of Ukraine no. 1295, Dec. 23, 2020, Some issues of ensuring the functioning of the system for detecting vulnerabilities and responding to cyber incidents and cyber attacks.* [Online]. Available: https://zakon.rada.gov.ua/laws/show/1295-2020-%D0%BF#Text [in Ukrainian].

[3] "Statistics of cyber attacks for four months of war", *Derzhspetszviazku*. [Online]. Available: https://www.kmu.gov.ua/news/derzhspeczvyazku-statistika-kiberatak-za-chotiri-misyaci-vijni [in Ukrainian].

[4] "Cyber attacks of the UAC-0118 group - CERT-UA research", *Derzhavna sluzhba spetsialnoho zviazku ta zakhystu informatsii Ukrainy.* [Online]. Available: https://cip.gov.ua/ua/news/kiberataki-grupi-uac-0118-doslidzhennya-cert-ua [in Ukrainian].

[5] "What Russian and pro-Russian hackers are attacking Ukraine", *Derzhavna sluzhba spetsialnoho zviazku ta zakhystu informatsii Ukrainy.* [Online]. Available: https://cip.gov.ua/ua/news/yaki-rosiiski-ta-prorosiiski-khakeri-atakuyut-ukrayinu [in Ukrainian].

[6] "Kali Linux". [Online]. Available: https://www.kali.org/

© Е. В. Фауре, А. Б. Скуцький, А. О. Лавданський, 2022
DOI: 10.24025/2306-4412.4.2022.273385

[7] "Are your passwords in the green?" [Online]. Available: https://www.hivesystems.io/blog/are-your-passwords-in-the-green

[8] *Order of the Administration of the State Service for Special Communications and Information Protection of Ukraine no. 601, June 2021, Methodological recommendations for increasing the level of cyber protection of critical information infrastructure.* [Online]. Available: https://cip.gov.ua/ua/news/nakaz-ad-2021-10-06-601 [in Ukrainian].

[9] E. V. Faure, "Factorial coding with error correction", *Radioelektronika, informatyka, upravlinnia*, no. 3, pp. 130-138, 2017. doi: 10.15588/1607-3274-2017-3-15 [in Russian].

[10] E. V. Faure, "Factorial coding with data recovery", *Visnyk Cherkaskogo derzhavnogo tekhnolohichnogo universytetu*, no. 2, pp. 33-39, 2016 [in Russian].

[11] J. Al-Aazzeh, B. Ayyoub, E. Faure, V. Shvydkyi, O. Kharin, and A. Lavdanskyi, "Telecommunication systems with multiple access based on data factorial coding", *International Journal on Communications Antenna and Propagation*, vol. 10, no. 2, pp. 102-113, 2020. doi: 10.15866/irecap.v10i2.17216.

[12] M. Bóna, *Combinatorics of Permutations*. CRC Press, 2022.

[13] E. Faure, A. Shcherba, B. Stupka, I. Voronenko, and A. Baikenov, "A method for reliable permutation transmission in short-packet communication systems', in *Information Technology for Education, Science and Technics. Lecture Notes in Computational Science and Engineering*, (in press), 2022.

[14] D. K. Chaturvedi, *Modeling and Simulation of Systems Using MATLAB® and Simulink®*. CRC press, 2017.

[15] A. Shcherba, E. Faure, and O. Lavdanska, "Three-pass cryptographic protocol based on permutations", in *2020 IEEE 2nd Int. Conf. on Advanced Trends in Information Theory (ATIT)*, 2020, pp. 281-284. doi: 10.1109/ATIT50783.2020.9349343.

E. V. Faure, *Dr. Sc., Professor,*
A. B. Skutskyi,
e-mail: a.b.skutskyi.asp21@chdtu.edu.ua
A. O. Lavdanskyi, *Ph. D., Associate Professor,*
Cherkasy State Technological University
Shevchenko blvd, 460, Cherkasy, 18006, Ukraine

SIMULATION MODEL FOR INFORMATION TRANSMISSION SYSTEM WITH NON-SEPARABLE DATA FACTORIAL CODING IN SIMULINK ENVIRONMENT

The work is devoted to the development and research of a simulation model, which includes the information transmission system with non-separable factorial coding of data in Simulink environment. The approach is based on the use of non-separable factorial coding of data that allows the implementation of integrated information security against unauthorized access and channel errors. Non-separable factorial coding involves the bijective transformation of an information message or its part into a permutation. The list of protocols must be developed. These protocols are aimed at solving the tasks of synchronizing transmitter and receiver, establishing communication, agreeing keys, and monitoring the information reliability for practical use of data factorial coding in information and communication systems. In order to minimize the developer's time and resources, all solutions in information exchange protocols, based on non-separable data factorial coding, should be simulated on appropriate computer models. The developed simulation model includes the transmitter that realizes the permutation formation, coding symbols with a binary uniform code, and transmission of the received sequence through a binary symmetric communication channel with independent bit errors. The receiver implements reverse conversion from a binary message into a symbolic one. In the process of simula-

© Е. В. Фауре, А. Б. Скуцький, А. О. Лавданський, 2022
DOI: 10.24025/2306-4412.4.2022.273385

tion, the quantity of information messages correctly received and damaged by an error are recorded. In addition, cases of undetected errors on the received side are counted. The structure of the simulation model has been developed, and the functional purpose of each subsystem has been determined. The stages for model construction and configuration in Simulink environment are described in details. The built simulation model allows to investigate the influence of channel error on information messages. The results of experimental studies of information message transmission through a binary symmetric communication channel with given bit error probabilities testify to their correspondence to theoretical estimates and to the adequacy of the constructed model. The obtained simulation model will make it possible to conduct experiments to study data factorial coding in communication channels of different quality. In addition, the developed model is the basis for constructing a model of secure information exchange through a three-pass cryptographic protocol based on permutations.

Keywords: *factorial code, permutation, binary symmetric channel, error probability, simulation.*

Стаття надійшла 20.11.2022
Прийнято 13.12.2022

© Е. В. Фауре, А. Б. Скуцький, А. О. Лавданський, 2022
DOI: 10.24025/2306-4412.4.2022.273385