Захист інформації та кібернетична безпека

УДК 004.056.55 DOI: 10.30748/soi.2019.157.14

О.А. Борисенко, О.В. Бережна, А.І. Новгородцев, В.В. Сердюк, М.М. Яковлев

Сумський державний університет, Суми

СИСТЕМА ПЕРЕДАЧІ ТА ВІДОБРАЖЕННЯ ІНФОРМАЦІЇ ІЗ ЗАХИСТОМ ЧИСЛОВИХ ДАНИХ

Стаття вирішує практичну задачу побудови цифрових систем передачі та відображення інформації із захистом числових даних від несанкціонованого доступу та помилок, які передаються багаторозрядними десятковими числами, з цифрами, що подані в двійково-десятковій формі. Секретність чисел, що передаються, досягається для кожного розряду числа за допомогою окремого шифру підстановок зі своїм ключем і ключа шифру перестановок для всіх розрядів десяткового числа. Завадостійкість при цьому забезпечується застосуванням рівноважних кодових комбінацій для кодування двійково-десяткових цифр і використанням надлишковості їх кодових зображень у вигляді 6 заборонених комбінацій.

Ключові слова: *система передачі інформації, несанкціонований доступ, перестановки, шифрувальні таблиці, завадостійкість, рівноважний код.*

Вступ

Робота направлена на вирішення практичної задачі, побудови цифрової системи передачі та відображення інформації із захистом числових даних від несанкціонованого доступу та помилок. Практично немає жодного виробничого процесу, де б не застосовувалися системи передачі інформації, які поряд з загальною інформацією не передавали б ще і інформацію в вигляді числових даних. Вони часто подаються багаторозрядними десятковими числами, цифри яких мають двійково-десяткову форму і тому кодуються 4 бітами. Числа після передачі, як правило, ще і відображаються на індикаторах, для того, щоб оператор міг отримати та прийняти відповідне керуюче рішення.

Такі 4-розрядні двійково-десяткові числа використовуються, наприклад, в системах збору даних з датчиків тепла, електроенергії, води. В більш складних сферах виробництва вони можуть використовуватися в далекомірах, частотомірах, фазометрах і тому подібних пристроях. Передача та відображення числових даних відбувається навіть при вимірюванні цифровими пристроями тривалості одиночних імпульсів, їх фронтів і зрізів, або зрушень між ними. Точність і швидкість таких вимірювань значно вища, ніж при використанні осцилографів з каліброваними розгортками, розтяжками, мітками та іншими подібними аналоговими пристроями, які використовуються для підвищення точності вимірювання [1].

При цьому досить часто ставиться задача не тільки передачі та відображення багаторозрядної числової інформації, а і підвищення її секретності, тому що ця інформація може визивати також інтерес і для сторонніх осіб. Відповідно потрібен її захист від несанкціонованого доступу до неї, в тому числі і за допомогою шифрування. При цьому для підвищення стійкості шифру можна використовувати для кожного розряду десяткового багаторозрядного числа свій шифр. При цьому часто вимагається, щоб система передачі цифрових даних була захищена не тільки від несанкціонованого доступу, а і від завад, тому що числова інформація за своєю природою має мало надлишкової інформації, а тому є найменш захищена та відповідно найбільш вразлива від їх дії [2–7].

Побудова такої системи, яка передає і відображає багаторозрядну числову інформацію та одночасно захищає її від несанкціонованого доступу і завад, і є **задачею даної роботи**.

Виклад основного матеріалу

Ідея рішення. В основу рішення захисту від несанкціонованого доступу, що пропонується, покладені шифрувальні таблиці, які перетворюють набір з 10 двійково-десяткових вихідних цифр довжиною 4 біта у взяті випадково довільні перестановки цих же цифр, тобто реалізують широко розповсюджений стандартний шифр підстановок [8–10]. При цьому деякі з цих двійково-десяткових цифр можуть переходити в такі ж самі цифри. Перестановки беруться тому, що кожна цифра одного розряду, що передається, повинна відрізнятися від інших цифр, які можуть бути передані в цьому розряді. Якщо, наприклад, дві

різні цифри кодуються одною двійково-десятковою комбінацією, то на приймальному кінці буде незрозуміло, яка з цих двох цифр передається.

Шифрувальна таблиця шифрує двійково-десяткові цифри одного розряду і тим самим створює його шифр і одночасно ключ. Кількість таких таблиць очевидно буде дорівнювати факторіалу $10! = 10 \times 9 \times 8 \times \ldots \times 1 = 3628800$. Три з них в якості прикладу наведені нижче в табл. 1.

Таблиця 1

Варіанти шифрувальних таблиць

Варіант 1			Варіант 2			Варіант 3		
№	$x_1x_2x_3x_4$	$f_1f_2f_3f_4$	№	$x_1x_2x_3x_4$	$f_1f_2f_3f_4$	№	$x_1x_2x_3x_4$	$f_1f_2f_3f_4$
0	0000	0011	0	0000	0000	0	0000	0000
1	0001	0101	1	0001	0001	1	0001	0001
2	0010	0000	2	0010	0010	2	0010	0010
3	0011	1000	3	0011	0011	3	0011	0011
4	0100	0110	4	0100	0100	4	0100	0111
5	0101	0010	5	0101	1001	5	0101	1000
6	0110	0010	6	0110	1000	6	0110	1001
7	0111	0001	7	0111	0101	7	0111	0100
8	1000	1001	8	1000	0110	8	1000	0110
9	1001	0111	9	1001	0111	9	1001	0101

Всі вони можуть бути використані як шифри – ключі для 3 розрядів багаторозрядного двійково-десяткового числа. Права сторона з кожної з цих таблиць являє собою ключ довжиною в 40 біт.

Якщо вона становиться відомою, то отримати вихідні цифри з них є досить простою задачею, яка вирішується переходом кодових зображень двійково-десяткових цифр з правої сторони таблиці на ліву.

Однак для того, щоб їх знайти, необхідно для кожного кодового зображення реальної двійково-десяткової цифри з 10 можливих цифр знайти одну. Для цього потрібно при аналізі отриманого кодового зображення двійково-десяткової цифри, яке декодується, знайти її реальне значення. Наприклад, у варіанті 1 табл. 1 реальній цифрі 0000 відповідає зображення 0011. Треба довести, що реально запис 0011 передає значення 0000 десяткової цифри 0, або довести зворотне. Якраз ця задача для цифрових даних складає основну трудність, тому що, як правило, для них нема явних тестів, які б її вирішували, і тому для рішення цієї задачі треба шукати більш складні шляхи. Якщо б вдалося встановити в табл. 1 кодування цифри 0000 комбінацією 0011, наприклад за смислом, то тоді можна переходити до декодування другої цифри, яка передається по каналу зв'язку, наприклад 1000, і так далі, поки не буде встановлена відповідність значень всіх комбінацій $f_1f_2f_3f_4$ комбінаціям $x_1x_2x_3x_4$. Тільки в такому випадку можна вважати, що ключ до шифру знайдено. Можна в принципі 10 двійково-десяткових цифр для шифрування брати не з 10, а з їх загальної кількості 16, але це не міняє суть шифрування. Вона залишається незмінною.

Ефективність захисту. Ефективність захисту розряду двійково-десяткового числа напряму залежить від наявності тесту, який би розпізнавав за невеликий час дійсне значення перехопленої двійково-десяткової комбінації цифри, що передається. Якщо б такий тест був, то тоді для 10 цифр потрібно було б зробити 10 розпізнавань, і на цьому завершити дешифрування одного розряду числа. Потім аналогічно можна було б розшифрувати цифри наступного розряду числа, якщо там використовується своя шифрувальна таблиця, і так далі. Якщо розрядів, наприклад, 5, то тоді знадобиться 50 кроків дешифрування. Це невелике число і захист, що розглядається, не мав би сенсу. Однак в реальності таких тестів розпізнавання цифр або нема, або вони досить складні, і тоді захист з допомогою шифрувальних таблиць, що розглядаються, може дати потрібні результати, особливо якщо інформація швидко старіє.

Крім того, є можливість зашифрувати порядок передачі цифр розрядів в десятковому числі. Зазвичай вони йдуть від старших розрядів до молодших. Але можна цей порядок і поміняти. Якщо, наприклад, передаються 5-розрядні двійково-десяткові десяткові числа, то порядок розрядів може змінюватися $5! = 120$ варіантами. Можна також два 5-розрядні двійково-десяткові числа передати одноча-

сно змішаними і тоді буде отримано 10! = 3628800 варіантів, або три таких числа, що збільшить кількість варіантів дешифрування до 15!. Тобто відомим методом шифрування підстановок і перестановок можна отримати для даної задачі передачі числової інформації досить стійкий шифр [8–10].

Завадостійкість шифру. Підвищення завадостійкості цифр, що передаються, може відбуватися за рахунок використання 6 надлишкових станів в двійковій-десяткових числах, а також додаткового завадостійкого кодування, наприклад на парність, або непарність. Але є ще одна можливість отримати завадостійкий шифр – це використати рівноважний код з 2 одиницями та довжиною 5, в якому є 10 кодових комбінацій. В такому випадку табл. 1 для варіанта 1 прийме наступний вигляд (табл. 2).

Таблиця 2

Завадостійке кодування

Завадостійкий код			Завадостійкий код		
№	$x_1x_2x_3x_4$	$f_1f_2f_3f_4$	№	$x_1x_2x_3x_4$	$f_1f_2f_3f_4$
0	0000	00011	5	0101	01100
1	0001	00101	6	0110	10001
2	0010	00110	7	0111	10010
3	0011	01001	8	1000	10100
4	0100	01010	9	1001	11000

Даний рівноважний код легко знаходить помилки підсумовуванням кількості одиниць в кодових словах. Якщо їх більше або менше 2, то це є ознакою помилки, а якщо 2, то це ознака відсутності помилки. Крім того, наявність шифрування в вигляді перестановок дозволяє зберігати та передавати ключі в системі з надійним їх захистом інформації від завад, що теж важливо, коли ключі часто змінюються. Перестановки по своїй природі мають досить значну надлишковість і відповідно можуть не тільки виявляти помилки, а і виправляти деякі з них [5–6]. Тому вони мають достатньо високу ефективність при їх використанні в телекомунікаційних системах, особливо, якщо взяти до уваги можливість їх побудови з допомогою факторіальних чисел [5–6; 11–12].

Схема системи передачі та відображення однієї двійково-десяткової цифри. В даній роботі розробляється система передачі та відображення однієї двійково-десяткової цифри. Передача та відображення інших двійково-десяткових цифр, які створюють додаткові розряди в десятковому числі, для кожної з них проходить паралельно за схемою, яка розроблена для одного розряду десяткового числа. Відповідно можна організувати паралельну передачу та відображення будь-якої кількості двійково-десяткових цифр з одночасним їх висвітленням на індикаторах. Хоча не виключається передача двійково-десяткових цифр, які належать багато розрядному числу, послідовно одна за другою з їх висвітленням на одному індикаторі. Такий варіант системи більш економний, але потребує додаткового запам’ятовування цифр, які відображаються.

Структурна схема системи передачі та відображення однієї двійково-десяткової цифри надана на рис. 1.

Її блоки поділяються на блоки сторони, що передає дані, та блоки сторони, що сприймає ці дані. Відповідно до наведених позначень система, що розглядається, містить на стороні, яка передає дані, генератор тактових імпульсів (ГТІ), дільник частоти (ДЧ), систему керування (СК), буферну запам’ятовуючу схему (БЗС), шифратор (Ш), лінію зв’язку (ЛЗ). На прийомній стороні знаходиться: блок виправлення помилок (БВП), перетворювач кодів (ПК) чотирьох розрядних кодових комбінацій в семирозрядні кодові комбінації, індикатор (І).

Система працює наступним чином. На вхід буферної запам'ятовуючої схеми (БЗС) приходить і запам’ятовується двійково-десяткова цифра X_1, X_2, X_3, X_4, яка складається з 4-х розрядів. Вона відповідає десятковій цифрі, яка повинна бути передана по ЛЗ і відображена на індикаторі.

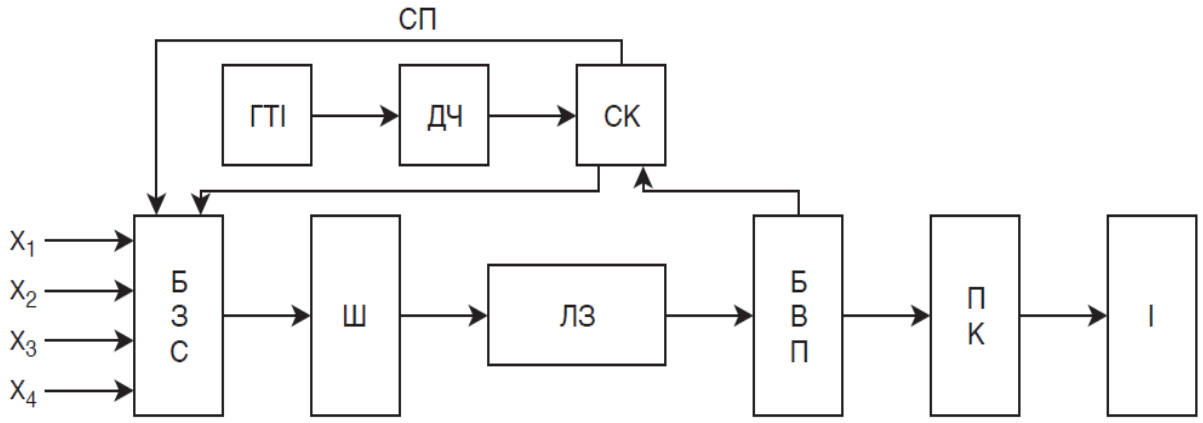

Рис. 1. Система передачі та відображення однієї двійково-десяткової цифри

Ці цифри в шифрувальних таблицях обираються випадково, шляхом довільних перестановок 10 вихідних цифр. Таким чином, чотирьохрозрядна двійково-десяткова цифра з БЗС в незмінному вигляді подається на шифратор, який перетворює її в чотирьохрозрядне двійкове слово, яке, як правило, не відповідає вхідній цифрі. Після цього отримане на виході шифратора слово подається на лінію зв'язку (ЛЗ), де воно може спотворюватися під дією завад, перетворюючись в інше чотирьохрозрядне слово. Якщо, це спотворене чотирьохрозрядне слово по своєму числовому значенню не буде відноситися до слів, які зазначені в таблиці шифру, то воно визначається блоком виправлення помилок (БВП) як заборонене.

Відповідно цей блок видає сигнал на схему керування (СК) про те, що виникла помилка. З схеми керування надходить сигнал на БЗС і відбувається повторна відправка вхідної цифри в лінію зв'язку (ЛЗ). Якщо знову виникає помилка, то знову відбувається відправка вхідної цифри. Це може продовжуватися до трьох повторів передачі кодової комбінації по ЛЗ. Якщо після третього повтору знову з'являється помилка, то СК виробляє сигнал "Аварія", і система зупиняється.

Після того, як БВП сприйняв сигнал як правильний, він по сигналу зі СК відправляє його на перетворювач кодів (ПК), який замість чотирьох двійкових розрядів виробляє сім, які потім надходять на індикатор, для того, щоб висвітити його сегменти і тим самим відобразити відповідну цифру. Цифра, яка відображається на індикаторі, повинна відповідати двійково-десятковій цифрі, яка знімається з БЗС. Цю відповідність реалізує ПК. Він може бути реалізований на постійному запам'ятовуючому пристрої, на адресні входи якого подаються зашифровані слова, а з комірок пам'яті знімаються дешифровані семирозрядні кодові слова, які перетворюються індикатором в зображення відповідних цифр. Подача на БЗС символів для індикації відбувається із заданою частотою, тобто вони періодично змінюються.

Система, що розглядається, може бути на практиці реалізована на одній мікросхемі ПЛІС і тому має невеликі габарити і відносно дешева та надійна. Її використання може швидко дати бажаний ефект і тому швидко окупитися.

Висновки

Система, що пропонується, має практичну направленість для задач передачі та відображення числової інформації, які є практично на кожному виробництві. Тому вона досить поширена. Введення в цю систему захисту інформації від несанкціонованого доступу і завад робить її більш прийнятною для сьогоденних умов, коли скритність і завадостійкість інформації є важливою вимогою сучасного виробництва. Запропонована система захисту десяткових чисел в вигляді двійково-десяткових шифрувальних таблиць проста, швидкодіюча та недорога, але в той же час може бути досить надійною. Її використання забезпечить надійну скритність і завадостійкість при передачі та відображенні числової інформації для багатьох випадків її впровадження в практику.

Список літератури

1. Измерительные преобразователи систем оптической диагностики с многофункциональными одноэлементными фотоприемниками / Р.И. Воробей, О.К. Гусев, А.И. Свистун, А.К. Тявловский, К.Л. Тявловский, Л.И. Шадурская // Приборы и методы измерений. – 2018. – Т. 9, № 3. – С. 215-226.

2. Borysenko Olexiy A. Chapter 7: Description and applications of binomial numeral systems complex / Olexiy A. Borysenko, Vyacheslav V. Kalashnikov // Security and noise immunity of telecommunication systems: new solutions to the codes and signals design problem: Collective monograph. Edited by Sergey G. Rassomahin and Alexandr A. Kuznetsov. – ASC Academic Publishing, Minden, Nevada, USA, 2017. – P. 147-159.

3. Chapter 3: Representation of cascade codes in the frequency domain / Alexandr A. Kuznetsov, Roman V. Serhiienko, Dmytro I. Prokopovych-Tkachenko, Bakhytzhan S. Akhmetov // Security and noise immunity of telecommunication systems: new solutions to the codes and signals design problem: Collective monograph. Edited by Sergey G. Rassomahin and Alexandr A. Kuznetsov. – ASC Academic Publishing, Minden, Nevada, USA, 2017. – P. 71-101.

4. Kuznetsov Alexandr A. Chapter 4: The methodology of evaluating the energy gains from coding in channels with grouping errors / Alexandr A. Kuznetsov, Sergii V. Ksvun, Yuriy I. Gorbenko // Security and noise immunity of telecommunication systems: new solutions to the codes and signals design problem: Collective monograph. Edited by Sergey G. Rassomahin and Alexandr A. Kuznetsov. – ASC Academic Publishing, Minden, Nevada, USA, 2017. – P. 102-119.

5. Горячев А.Е. Обнаружение ошибок в перестановках / А.Е. Горячев // Вісник СумДУ. Технічні науки. – 2009. – №3. – С. 169-174.

6. Борисенко А.А. Обнаружение и исправление ошибок в перестановках / А.А. Борисенко, А.Е. Горячев, Е.Л. Онанченко // Міжнародна науково-практична конференція "Інформаційні технології та комп'ютерна інженерія". – Вінниця: ВНТУ, 2010. – С. 348-349.

7. Chapter 11: A Generalized Criterion of Efficiency for Telecommunication Systems / Alexei A. Borisenko, Vyacheslav V. Kalashnikov, Nataliya I. Kalashnykova, Alexey E. Goryachev; M. Favorskaya and Lakhmi Jain (Eds.) // Computer Vision in Advanced Control Systems Using Conventional and Intelligent Paradigms (Springer Series: Intelligent Systems Reference Library, ISSN 1868-4394). – Springer-Verlag, Alemania, 2014. – Vol. 1. – P. 353-373.

8. Шеннон К. Работы по теории информации и кибернетике / К. Шеннон. – М.: Иностранная литература, 1963. – 832 с.

9. Столлингс В. Криптография и защита сетей: принципы и практика, 2-е изд. / В. Столлингс. – М.: Вильямс, 2001. – 672 с.

10. Криптография: скоростные шифры // А.А. Молдовян, Н.А. Молдовян, Н.Д. Гуц, Б.В. Изотов. – СПб.: БХВ-Петербург, 2002. – 244 с.

11. Generation of Permutations Based Upon Factorial Numbers / A.A. Borisenko, V.V. Kalashnikov, I.A. Kulik, A.E. Goryachev // Eighth International Conference on Intelligent Systems Design and Applications. – Kaohiung, Taiwan, 2008. – P. 57-61.

12. Факториальные числа в задачах защиты информации / А. Борисенко, А. Горячев, В. Сердюк, М. Ермаков // Безпека інформації. – 2018. – Т. 24, № 3. – *С.* 169-174.

References

1. Vorobey, R.I., Gusev, O.K., Svistun, A.I., Tyavlovskiy, A.K., Tyavlovskiy, K.L. and Shadurskaya, L.I. (2018), ”Izmeritelnyye preobrazovateli sistem opticheskoy diagnostiki s mnogofunktsionalnymi odnoelementnymi fotopriyemnikami” [Measuring transducers of optical diagnostics systems with multi-functional single-element photodetectors], *Pribory i metody izmereniy*, 2018, Vol. 9, No. 3, pp. 215-226.

2. Borysenko, Olexiy A. and Kalashnikov, Vyacheslav V. (2017), Chapter 7: Description and applications of binomial numeral systems complex, *Security and noise immunity of telecommunication systems: new solutions to the codes and signals design problem: Collective monograph*, ASC Academic Publishing, Minden, Nevada, USA, pp. 147-159.

3. Kuznetsov, Alexandr A., Serhiienko, Roman V., Prokopovych-Tkachenko, Dmytro I. and Akhmetov, Bakhytzhan S. (2017), Chapter 3: Representation of cascade codes in the frequency domain, *Security and noise immunity of telecommunication systems: new solutions to the codes and signals design problem: Collective monograph*, ASC Academic Publishing, Minden, Nevada, USA, pp. 71-101.

4. Kuznetsov, Alexandr A., Ksvun, Sergii V. and Gorbenko, Yuriy I. (2017), Chapter 4: The methodology of evaluating the energy gains from coding in channels with grouping errors, *Security and noise immunity of telecommunication systems: new solutions to the codes and signals design problem: Collective monograph*, ASC Academic Publishing, Minden, Nevada, USA, pp. 102-119.

5. Goryachev, A.E. (2009), “Obnaruzheniye oshibok v perestanovkakh” [Detection of errors in permutations], *Visnik SumDU. Tekhnichni nauki*, No. 3, pp. 169-174.

6. Borisenko, A.A., Goryachev, A.E. and Onanchenko, E.L. (2010), “Obnaruzheniye i ispravleniye oshibok v perestanovkakh” [Detection and correction of errors in permutations], *Mizhnarodna naukovo-praktichna konferentsiya “Informatsiyni tekhnologiï ta komp’yuterna inzheneriya”*, VNTU, Vinnitsya, pp. 348-349.

7. Borisenko, Alexei A., Kalashnikov, Vyacheslav V., Kalashnykova, Nataliya I. and Goryachev, Alexey E. (2014), Chapter 11: A Generalized Criterion of Efficiency for Telecommunication Systems, *Computer Vision in Advanced Control Systems Using Conventional and Intelligent Paradigms* (Springer Series: Intelligent Systems Reference Library, ISSN 1868-4394), Springer-Verlag, Alemania, Vol. 1, pp. 353-373, available at: http://www.springer.com/series/8578.

8. Shennon, K. (1963), “*Raboty po teorii informatsii i kibernetike*” [*Works on information theory and cybernetics*], Inostrannaya literatura, Moscow, 832 p.

9. Stollings, V. (2001), “*Kriptografiya i zashchita setey: printsipy i praktika*” [*Works on information theory and cybernetics*], Viliams, Moscow, 672 p.

10. Moldovyan, A.A., Moldovyan, N.A., Guts, N.D. and Izotov, B.V. (2002), “*Kriptografiya: skorostnyye shifry*” [*Cryptography: speed ciphers*], BHV-Peterburg, Sankt Peterburg, 244 p.

11. Borisenko, A.A., Kalashnikov, V.V., Kulik, I.A. and Goryachev, A.E. (2008), “Generation of Permutations Based Upon Factorial Numbers, *Eighth International Conference on Intelligent Systems Design and Applications*, Kaohiung, Taiwan, pp. 57-61.

12. Borisenko, A., Goryachev, A., Serdyuk, V. and Ermakov, M. (2018), “Faktorialnyye chisla v zadachakh zashchity informatsii” [Factorial numbers in information security tasks], *Ukrainian Scientific Journal of Information Security,* Vol. 24, No. 3, pp. 169-174.

Надійшла до редколегії 13.03.2019
Схвалена до друку 23.04.2019

Відомості про авторів:

Борисенко Олексій Андрійович
доктор технічних наук професор
професор Сумського державного університету,
Суми, Україна
https://orcid.org/0000-0001-7466-9135

Бережна Ольга Володимирівна
кандидат технічних наук доцент
доцент Сумського державного університету,
Суми, Україна
https://orcid.org/0000-0001-7105-1276

Information about the authors:

Oleksiy Borysenko
Doctor of Technical Sciences Professor
Professor of Sumy State University,
Sumy, Ukraine
https://orcid.org/0000-0001-7466-9135

Olga Berezhna
Candidate of Technical Sciences Associate Professor
Senior Lecturer of Sumy State University,
Sumy, Ukraine
https://orcid.org/0000-0001-7105-1276

Новгородцев Анатолій Іванович
кандидат технічних наук доцент
доцент Сумського державного університету,
Суми, Україна
https://orcid.org/0000-0003-4598-5598

Anatoly Novgorodtsev
Candidate of Technical Sciences Associate Professor
Senior Lecturer of Sumy State University,
Sumy, Ukraine
https://orcid.org/0000-0003-4598-5598

Сердюк Віктор Васильович
аспірант
Сумського державного університету,
Суми, Україна
https://orcid.org/0000-0003-1432-4519

Viktor Serdiuk
Doctoral Student
of Sumy State University,
Sumy, Ukraine
https://orcid.org/0000-0003-1432-4519

Яковлев Максиміліан Миколайович
студент
Сумського державного університету,
Суми, Україна
https://orcid.org/0000-0002-1196-4062

Maximilian Yakovlev
Student
of Sumy State University,
Sumy, Ukraine
https://orcid.org/0000-0002-1196-4062

СИСТЕМА ПЕРЕДАЧИ И ОТОБРАЖЕНИЯ ИНФОРМАЦИИ С ЗАЩИТОЙ ЧИСЛОВЫХ ДАННЫХ

А.А. Борисенко, О.В. Бережная, А.И. Новгородцев, В.В. Сердюк, М.Н. Яковлев

Статья решает практическую задачу построения цифровых систем передачи и отображения информации с защитой числовых данных от несанкционированного доступа и ошибок, которые передаются многоразрядными десятичными числами, с цифрами, представленными в двоично-десятичной форме. Секретность передаваемых чисел достигается для каждого разряда числа с помощью отдельного шифра подстановок со своим ключом и ключа шифра перестановок для всех разрядов десятичного числа. Помехоустойчивость при этом обеспечивается применением равновесных кодовых комбинаций для кодирования двоично-десятичных цифр и использованием избыточности их кодовых изображений в виде 6 запрещенных комбинаций.

Ключевые слова: *система передачи информации, несанкционированный доступ, перестановки, шифровальные таблицы, помехоустойчивость, равновесный код.*

INFORMATION TRANSMISSION AND DISPLAY SYSTEM WITH PROTECTION OF NUMERICAL DATA

O. Borisenko, O. Berezhna, A. Novgorodtsev, V. Serdiuk, M. Yakovlev

The article solves the practical task of constructing a digital system for information transmission and displaying in the form of multi-digit numbers with the protection of the numbers of each digit from unauthorized access and errors. Their numbers are in binary-decimal form and are encoded with 4 bits. The numbers after the transmission are displayed on the indicators. The simplicity of the proposed algorithms allows them to be implemented on one PLD chip. This ensures a sufficient level of reliability and performance of the device at its insignificant cost. The secrecy of the transmitted multi-bit numbers is achieved separately for each digit number using a special substitution cipher, which, in each of ten binary-decimal digits, correlates with another binary-decimal digit selected randomly. As a result, the cipher for a single digit of a multivalued number represents a randomly taken permutation of 10 binary-decimal digits. These ciphers can easily be changed if necessary, which ensures their high stability. In addition to the cipher in the form of substitutions in each level, in the multi-bit number, there are also permutations of discharges, which greatly raises the reliability of the cipher as a whole. Errors in the transmission of binary-decimal digits in encrypted form are detected using an equilibrium code and the presence of 6 forbidden combinations for each digit being transmitted. The same keys have the form of permutations of 10 digits, and therefore they have redundancy, which can be used to raise their noise immunity in storage and transmission. Therefore, in general, the system for transmitting and displaying information being developed is protected from both unauthorized access and errors.

Keywords: *information transmission system, unauthorized access, permutations, encryption tables, noise immunity, equilibrium code.*