УДК 004.9 **doi: 10.26906/SUNZ.2023.122**

О. О. Можаєв[1], Ф.Ф. Сухина[2], В. С. Башилов[2]

[1] Харківський національний університет внутрішніх справ, Харків, Україна
[2] Харківський національний університет радіоелектроніки, Харків, Україна

МЕТОД ВИЯВЛЕННЯ ВТРУЧАННЯ В КОМП'ЮТЕРНІ СИСТЕМИ ЕЛЕКТРОННОГО ОБІГУ ДОКУМЕНТІВ

Анотація. Актуальність. Наш час характеризується стрімким зростанням кількості та якості різноманітних комп'ютерних систем. Значна кількість з них належить до комп'ютерних систем електронного обігу даними. Такий обіг потребує використання надійних систем захисту, що не завжди має місто у реальному житті. Цей факт вимагає удосконалення існуючих та розробку нових методів виявлення фактів не достовірного функціонування таких комп'ютерних систем. **Метою даної роботи** є розробка методу виявлення втручання в комп'ютерні системи електронного обігу документів**. Об'єктом дослідження** є процес функціонування комп'ютерних систем електронного обігу документами. **Предметом дослідження** є методи та алгоритми виявлення втручання в комп'ютерні системи. **Результати.** У даній роботі запропоновано метод виявлення втручання в комп'ютерні системи електронного обігу документів. Для виявлення втручання в комп'ютерні системи використано принципи алгоритму кодування за Хеммінгом. Даний метод може бути частиною може бути частиною системи методів виявлення втручання в комп'ютерні системи електронного обігу документів, яку в свою чергу можна використати для функціонування різноманітних в комп'ютерних систем критичного застосування. **Висновок.** Розроблений метод виявлення втручання в комп'ютерні системи електронного обігу документів планується використовувати у подальшому для забезпечення якості та надійності функціонування комп'ютерних систем електронного обігу документів.

Ключові слова: комп'ютерні системи, електронний обіг документів, алгоритм кодування, електронний цифровий підпис, криптографія, хеш-коди.

Вступ

Розвиток суспільства визначається рівнем домінування інформаційного середовища. Інформація стала невід'ємною складовою функціонування всіх суспільних установ і життя людини зокрема. Швидкий розвиток і впровадження сучасних інформаційно-комунікаційних технологій став причиною глобальної трансформації індустріального суспільства в інформаційне. Все більша частина інформації зберігається і передається в електронному вигляді. Технічний прогрес, обумовлений розвитком інформаційного суспільства передбачає використання технологій електронного обміну даними. Для управління економікою, державою, силовими структурами все більше використовуються різноманітні комп'ютерні системи. Перехід до електронного документообігу, насамперед, пов'язаний з низкою переваг його використання. Електронний документообіг дозволяє суттєво спростити роботу по формуванню, збереженні та відправці важливої інформації [1–3] та потребує створення спеціалізованих комп'ютерних систем електронного обігу документів. Це породжує значну кількість часткових проблем та задач, які пов'язані зі специфікою електронного обміну даними.

Еволюція інформаційного суспільства сприяє автоматизації людської діяльності, зокрема широкому впровадженню електронних документів (ЕД), систем електронного документообігу та електронного цифрового підпису (ЕЦП). Це очевидно на прикладі комп'ютеризації управлінської сфери. Електронний документообіг – це сукупність процесів створення, опрацювання, відправлення, передавання, одержання, зберігання, використання та знищення ЕД, які виконуються із застосуванням перевірки цілісності, і в разі необхідності, – з підтвердженням факту одержання таких документів [4–7].

Використання ЕД отримало широке розповсюдження в таких сферах людської діяльності, як освіта, медицина, державне управління та інших. Але з розвитком сучасних інформаційно-технічних можливостей виникають нові ризики та загрози, що призводять до некоректного функціонування системи електронного документообігу, зниження надійності, а також значних матеріальних втрат. Тому, використання електронного документообігу обов'язково має супроводжуватися надійною системою захисту [8].

Документообіг в державі є системою, що матеріалізує процеси збирання, перетворення, зберігання інформації, а також процеси управління: підготовку та прийняття рішень, контроль за їх виконанням [18–20]. Ефективне впровадження технологій електронного урядування неможливе без розгортання електронного документообігу із застосуванням технологій ЕЦП. Користування системою електронного обміну даними можливо лише з використанням надійних систем захисту. Проблема гарантування цілісності електронних документів є першочерговим завданням в процесі електронного документообігу. Завдання надійного захисту конфіденційних ЕД від несанкціонованого доступу, захисту інтелектуальної власності, авторських прав вирішується вже тривалий час. Проте, деякі питання розробки надійних методів забезпечення інформаційної безпеки ЕД ще потребують вирішення. У наш час великий збиток наноситься суспільству таким негативним явищем, як підробка цінних документів. Засоби виявлення підробки в традиційних документах давно і досить успішно розвиваються. Завдання виявлення фальсифікацій в електронних документах є достатньо складними і потребують великої кількості ресурсів для свого розв'язання [12–13]. Фальсифікація електронних документів може стати непоправним явищем, оскільки найменші зміни в документі можуть докорінно змінити його суть.

Електронний документообіг має важливе значення для людства і грає велику роль так, як і проблема його захисту. Однак, серед великої кількості існуючих методів захисту електронних документів жоден з них не дає повної гарантії інформаційної безпеки. Відсутність ефективних методів захисту електронних документів є джерелом постійного пошуку нових рішень, в числі яких є сучасна криптографія та стеганографія на основі використання комп'ютерних технологій. Багато праць присвячено алгоритмам побудови електронного цифрового підпису за різними схемами. Дослідження показують, що питання розробки алгоритмів побудови ЕЦП були і залишаються актуальними впродовж останніх років.

Таким чином, підсумовуючи вищесказане, можна стверджувати, що існує великий розрив між потребами в захисті електронних документів і можливостями, які можуть гарантувати існуючі методики. Тому задача створення методів виявлення та протидії фальсифікаціям електронних документів є актуальною для наукових досліджень та розробок.

Метою цієї роботи є розробка методу виявлення втручання в комп'ютерні системи електронного обігу документів

Основна частина

Достовірність передачі, обробки та зберігання електронних документів в наш час є вкрай важливим завданням. Ефективним способом вирішення даної проблеми є використання надлишкового хешування інформації. Введення надлишкової інформації в інформацію, яка передається мережею забезпечує можливість виявлення і виправлення помилок на стороні отримувача інформаційного повідомлення. Математична теорія побудови надлишкових (завадостійких) кодів зараз має великі досягнення. Проте, існує великий розрив між рівнем теоретичних досягнень теорії завадостійкого кодування і рівнем результатів практичного використання даної теорії [5–11].

Введення надлишковості дає можливість виявлення і виправлення помилок в інформації, яка передається і може бути змінена під час передачі. Однак, до цього відомі корегуючі, циклічні коди, коди Хеммінга, Ріда-Соломона, описані в дослідженнях [14–21], не придатні для вирішення проблеми виявлення фальсифікованих фрагментів інформації. Розрізняють коди, які виявляють помилки, і корегуючі коди, які ще додатково, крім виявлення помилки, виправляють її. Найпростішими способами виявлення помилок є контрольне сумування, а також перевірка на парність. Проте, вони не достатньо надійні, особливо при виникненні великої кількості помилок. Оскільки в документах зазвичай можуть фальсифікуватися цілі фрагменти інформації, тому, подібні механізми не можуть в повній мірі розв'язати проблему підробки ЕД.

Хеммінг розробив теорію лінійних блокових кодів. Він ввів і дав визначення основним параметрам блокових кодів, а також розробив кодуючий і декодуючий пристрої для своїх кодів. Для оцінки корегуючої можливості кодів Хеммінг ввів параметри кодової і мінімальної кодової відстані і показав їх залежність від довжини коду і введеної надлишковості [10]. Розглянемо детальніше використання цієї теорії для вирішення задачі забезпечення достовірності функціонування ДЕ.

Оскільки розглядається проблема підробки ЕД, при розробці методу виявлення фальсифікованих фрагментів електронного документу можна взяти за основу принципи алгоритму кодування за Хеммінгом. Код Хеммінга – самокорегуючий код, що дозволяє закодувати згідно алгоритму будь-яке інформаційне повідомлення і вразі виникнення помилки, при передачі мережею, виявити і виправити її [4]. Традиційно алгоритми кодування-декодування за Хеммінгом виявляють символьні помилки в кодових послідовностях. На відміну від традиційного алгоритму кодування за Хеммінгом, який працює з бітами, доречною є побудова алгоритму, який оперує блоками інформації, тобто фрагментами електронного документу.

Аналогічно принципам кодування за Хеммінгом, введемо надлишковість, але замість символів – додаємо блоки інформації.

Множину можливих схем хешування блоків a_1, a_2 , a_3 ,..., a_n представити у вигляді двійкової матриці, де кожний рядок відповідає визначеній схемі хешування. При цьому виконуються наступні умови для рядків матриці:

1) відсутні нульові рядки матриці;
2) всі рядки матриці є лінійно-незалежними;
3) існує мінімальна кодові відстань між рядками матриці.

В теорії кодування для породжуючої матриці також є характерними перелічені властивості, що дає змогу використовувати правила побудови лінійних кодів для побудови систем хеш-кодів.

Система хеш-кодів – множина хеш-кодів, які отримані шляхом реалізації будь-якого алгоритму обчислення хеш-функції в порядку, визначеному спеціальною процедурою вибору записів (блоків інформації), на основі математичного апарату лінійної алгебри.

Алгоритм побудови хеш-кодів для забезпечення цілісності ЕД. Хешування вихідного блоку інформації можна представити у вигляді виразу, який є спеціальною багатовимірною не комутативною операцією хешування. Тоді, отриманий, в результаті хешування, захищений блок виглядатиме, як спеціальна багатовимірна не комутативна операція хешування інформаційних блоків електронного документу. Для пошуку всіх можливих варіантів кодів (матриць), з мінімальною кодовою відстанню між послідовностями рядків матриці, було розроблено програмне забезпечення, результати роботи якого показані в табл. 1.

Розглянемо декілька прикладів виявлення фальсифікованих фрагментів інформації на основі запропонованого методу. Як показують обчислення, між всіма кодовими послідовностями (рядками матриці) зберігається мінімальна кодова відстань, це дає можливість стверджувати, що даний код сприятиме гарантованому виправленню двохкратної помилки в блоках інформації. Схематично принцип отримання хеш-функцій показаний на рис. 1.

Таблиця 1 – **Варіанти породжуючих матриць**

№	Матриця	№	Матриця	№	Матриця	№	Матриця	№	Матриця
1	0 0 0 0 0 0 0 1 1 1 1 1 0 0 1 1 1 1 1 0	2	0 0 0 0 0 0 0 1 1 1 1 1 0 1 0 1 1 1 0 1	3	0 0 0 0 0 0 0 1 1 1 1 1 0 1 1 1 1 1 0 0	4	0 0 0 1 1 0 0 1 0 0 1 1 0 1 0 1 1 1 0 1	5	0 0 0 0 0 0 0 1 1 1 1 1 0 1 0 1 1 1 0 1
6	0 0 0 1 1 0 0 1 0 0 1 1 0 0 1 1 1 1 1 0	7	0 0 0 0 1 0 0 1 1 0 1 1 0 0 0 1 1 1 1 1	8	0 0 0 0 1 0 0 1 1 0 1 1 0 1 0 1 1 1 0 1	9	0 0 0 0 1 0 0 1 1 0 1 1 0 1 1 1 1 1 0 0	10	0 0 0 1 1 0 0 1 0 0 1 1 0 0 0 1 1 1 1 1
11	0 0 0 1 0 0 0 1 0 1 1 1 0 1 1 1 1 1 0 0	12	0 0 0 1 0 0 0 1 0 1 1 1 0 0 1 1 1 1 1 0	13	0 0 0 1 0 0 0 1 0 1 1 1 0 0 0 1 1 1 1 1	14	0 0 0 1 0 0 0 1 0 1 1 1 0 0 1 1 1 1 1 0	15	0 0 0 1 0 0 0 1 0 1 1 1 0 1 1 1 1 1 0 0
16	0 0 0 1 0 0 0 1 0 1 1 1 0 0 0 1 1 1 1 1	17	0 0 0 0 1 0 0 1 1 0 1 1 0 1 1 1 1 1 0 0	18	0 0 0 0 1 0 0 1 1 0 1 1 0 1 0 1 1 1 0 1	19	0 0 0 0 1 0 0 1 1 0 1 1 0 0 0 1 1 1 1 1	20	0 0 0 1 1 0 0 1 0 0 1 1 0 0 1 1 1 1 1 0
21	0 0 0 1 1 0 0 1 0 0 1 1 0 1 0 1 1 1 0 1	22	0 0 0 1 1 0 0 1 0 0 1 1 0 0 0 1 1 1 1 1	23	0 0 0 0 0 0 0 1 1 1 1 1 0 1 1 1 1 1 0 0	24	0 0 1 1 1 0 0 0 0 0 1 1 0 1 1 1 1 1 0 0	25	0 0 1 0 0 0 0 0 1 1 1 1 0 0 0 1 1 1 1 1
26	0 0 1 0 0 0 0 0 1 1 1 1 0 0 1 1 1 1 1 0	27	0 0 1 0 0 0 0 0 1 1 1 1 0 1 0 1 1 1 0 1	28	0 0 1 0 1 0 0 0 1 0 1 1 0 0 0 1 1 1 1 1	29	0 0 1 0 1 0 0 0 1 0 1 1 0 0 1 1 1 1 1 0	30	0 0 1 0 1 0 0 0 1 0 1 1 0 1 1 1 1 1 1 1
31	0 0 1 1 0 0 0 0 0 0 1 1 0 0 1 1 1 1 1 1	32	0 0 1 1 0 0 0 0 0 1 1 1 0 1 0 1 1 1 0 1	33	0 0 1 1 0 0 0 0 0 1 1 1 0 1 1 1 1 1 0 0	34	0 0 1 1 0 0 0 0 0 0 1 1 0 0 1 1 1 1 1 1	35	0 0 1 1 1 0 0 0 0 1 1 1 0 1 0 1 1 1 0 1

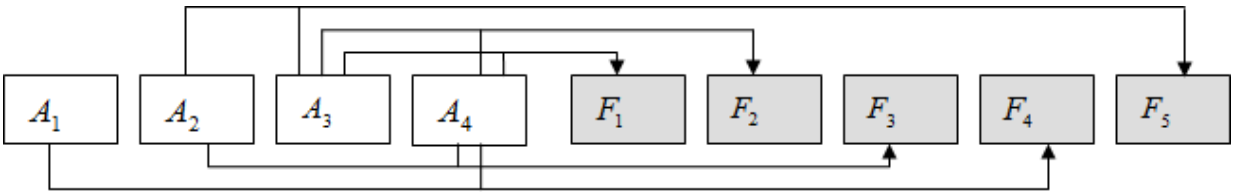

Рис. 1. Схема отримання хеш-функцій

В табл. 2 показано значення синдрому при різних комбінаціях помилок. Перевіримо правильність методу на прикладі, нехай маємо інформаційні блоки «0101», обчислимо контрольні блоки. Всі можливі комбінації помилок в інформаційних блоках показані в табл. 2.

Таблиця 2 – **Комбінації помилок в блоках електронного документу (** помилки в блоках)**

0101 11011 ⊕ * * 1001 11100 1100 00111	0101 11011 ⊕ * * 1111 00000 1010 11011	0101 11011 ⊕ * * 1100 00111 100111100	0101 11011 ⊕ * * 0011 00111 0110 11100	0101 11011 ⊕ * * 0000 00000 0101 11011
0101 11011 ⊕ * * 0110 11100 0011 00111	0101 11011 ⊕ * 1101 11001 1000 00010	0101 11011 ⊕ * 0001 11110 0100 00101	0101 11011 ⊕ * 0111 00010 0010 11001	0101 11011 ⊕ * 0100 00101 0001 11110

Розглянемо результати виявлення і виправлення помилок приведеними кодами Хеммінга в залежності від кратності помилки. Дані результати наведені в табл. 3.

Моделі запропонованих методів обчислення хеш-функції електронного документу та методів виявлення фальсифікацій були реалізовані на програмному та апаратному рівнях.

Таблиця 3 – **Виправлення помилок в блоках електронного документу (*– фальсифікований блок інформації)**

Локалізація помилки										
	Двохкратна помилка						Однократна помилка			
x_1	1 *	1 *	1 *	0	0	0	1 *	0	0	0
x_2	1 *	0	0	1 *	1 *	0	0	1 *	0	0
x_3	0	1 *	0	1 *	0	1 *	0	0	1 *	0
x_4	0	0	1 *	0	1 *	1 *	0	0	0	1 *
$f_1(x_3+x_4)$	0	1	1	1	1	0	0	0	1	1
$f_2(x_3+x_4)$	0	1	1	1	1	0	0	0	1	1
$f_3(x_2+x_4)$	1	0	1	1	0	1	0	1	0	1
$f_4(x_1+x_4)$	1	1	0	0	1	1	1	0	0	1
$f_5(x_2+x_3)$	1	1	0	0	1	1	0	1	1	0

Для розробки апаратних засобів реалізації методів контролю цілісності та виявлення фальсифікацій в електронних документах використано функціональні схеми реалізації методів обчислення хеш-функції електронного документу:

1) функціональна схема реалізації методу безключового обчислення хеш-функції на основі послідовного виконання операцій;

2) функціональна схема реалізації методу безключового обчислення хеш-функції на основі паралельного виконання операцій;

3) функціональна схема реалізації вдосконаленого методу обчислення хеш-функції електронного документу на основі послідовної реалізації обчислень;

4) функціональна схема реалізації методу обчислення хеш-функції електронного документу на основі використання операцій матричного криптографічного перетворення;

5) функціональна схема реалізації методу обчислення хеш-функції електронного документу на основі паралельної реалізації обчислень з використанням операцій матричного криптографічного перетворення;

6) функціональна схема реалізації вдосконаленого методу обчислення хеш-функції електронного документу на основі паралельної реалізації обчислень з використанням операцій матричного криптографічного перетворення;

7) функціональна схема реалізації методу ключового обчислення хеш- функції електронного документу на основі аналізу фрагменту інформації.

Функціональні схеми методів виявлення фальсифікованих фрагментів електронного документу:

1) функціональна схема реалізації методу виявлення фальсифікованого фрагменту електронного документу шляхом перехресного хешування;

2) функціональна схема реалізації методу виявлення заданої кількості фальсифікованих фрагментів електронного документу на основі надлишкового хешування контрольного блоку інформації.

Висновки

В результаті проведених авторами досліджень розроблений метод виявлення втручання в комп'ютерні системи електронного обігу документів для покращення достовірності електронного документу.

У цій роботі запропоновано метод виявлення втручання в комп'ютерні системи електронного обігу документів, який використовує обчисляння хеш-функції електронного документу на основі паралельної реалізації обчислень з використанням операцій матричного криптографічного перетворення.

Даний метод може бути частиною системи методів виявлення втручання в комп'ютерні системи електронного обігу документів, яку в свою чергу можна використати для функціонування різноманітних в комп'ютерих систем критичного застосування.

У подальших дослідженнях планується розробка програмно-інструментальних засобів реалізації розробленого методу.

Список літератури

1. Shulze H. Theory and Applications of OFDM and CDMA / H. Shulze, C. Luders. − Germany: John Wiley & Sons, Ltd , 2005.– 408 p.
2. Ungerboeck G. Channel coding with multilevel/phase signal / G. Ungerboeck // IEEE Trans., 1981. – Vol. IT-28, № 1. – P. 55 – 66.
3. Verd´u S. Fifty Years of Shannon Theory / S. Verd´u // IEEE Transactions on information theory. – 1998. – Vol. 44, №6. – P. 2057 – 2078.

4. Xiang W. 5G Mobile Communications / Xiang W., Zheng K., Xuemin Sh.; Springer International Publishing, 2016. – 690 p.
5. Svyrydov, A., Kuchuk, H., Tsiapa, O. (2018). Improving efficienty of image recognition process: Approach and case study. Proceedings of 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies, DESSERT 2018, 593-597, doi: https://doi.org/10.1109/DESSERT.2018.8409201·
6. O. Mozhaev Potential application of hardware protected symmetric authentication microcircuits to ensure the security of internet of things/P. Klimushin, T.Solianyk, T. Kolisnyk, O. Mozhaev// Advanced Information Systems. 2021. Vol. 5, No. 3, P 103-111, doi: https://doi.org/10.20998/2522-9052.2021.3.14
7. Mozhaiev M. Sustainability of Open Educational Resources in Forensic Sciences: International Experience/ Karina Palkova, Olena Agapova, Aelita Zīle, Anton Polianskyi, Khosha Vadym, Serafyma Hasparian, Mozhaiev Mykhailo// European Journal of Sustainable Development(2022), 11, 3, 71-80 ISSN: 2239-5938 Doi:10.14207/ejsd.2022.v11n3p71
8. Mozhaiev, M., (2022). Devising a procedure for defining the general criteria of abnormal behavior of a computer system based on the improved criterion of uniformity of input data samples./ Semenov, S., Mozhaiev, O., Kuchuk, N., Mozhaiev, M., Tiulieniev, S., Gnusov, Y., Yevstrat, D., Chyrva, Y., Kuchuk, H. EasternEuropean Journal of Enterprise Technologies, 6 (4 (120)), 40–49. doi: https://doi.org/10.15587/17294061.2022..
9. Гнусов Ю.В., Клімушин П.С., Колісник Т.П., Можаєв М.О. Аналіз систем моделювання мікроконтролерів з додатковими модулями криптографічного захисту інформації. Вісник Національного технічного університету «ХПІ». Серія: Системний аналіз, управління та інформаційні технології №1(3) 2020 С. 79-84
10. Mykhailo Mozhaiev, Viacheslav Davydov, Zhang Liqiang Analysis and comparative researches of methods or improving the software Advanced Information Systems, 2020 Vol. 4, No. 3, pp. 8-11, DOI: https://doi.org/doi: 10.20998/2522-9052.2020.3.18
11. Коваленко А. А., Кучук Г. А. Методи синтезу інформаційної та технічної структур системи управління об'єктом критичного застосування. Сучасні інформаційні системи. 2018. Т. 2, № 1. С. 22–27. DOI: https://doi.org/10.20998/2522-9052.2018.1.04
12. Kuchuk G., Kharchenko V., Kovalenko A., Ruchkov E. Approaches to selection of combinatorial algorithm for optimization in network traffic control of safety-critical systems. *East-West Design & Test Symposium (EWDTS)*. 2016. Pp. 1-6. doi:https://doi.org/10.1109/EWDTS.2016.7807655.
13. Kuchuk G.A. An Approach To Development Of Complex Metric For Multiservice Network Security Assessment / G.A. Kuchuk, A.A. Kovalenko, A.A. Mozhaev // Statistical Methods Of Signal and Data Processing (SMSDP – 2010): Proc. Int. Conf., October 13-14, 2010.– Kiev: NAU, RED, IEEE Ukraine section joint SP, 2010. – P. 158 – 160.
14. Mozhaiev M Method of Forensic Research on Image for Finding Touch up on the Basis of Noise Entropy/O. Kliuiev ; M. Mozhaiev ; M. Mozhaiev , O.Uhrovetskyi ,E. Simakova-Yefremian 3rd International Conference on Advanced Information and Communications Technologies (AICT) Publisher: IEEE, 2019 Lviv, Ukraine P. 76 – 79. DOI: 10.1109/AIACT.2019.8847760 (Scopus)
15. Mozhaiev M., (2017). Multiservice network security metric/ Mozhaev, O., Kuchuk, H., Kuchuk, N., Mozhaiev M., Lohvynenko, M..// 2nd International Conference on Advanced Information and Communication Technologies, AICT 2017 – Proceedings, 133-136. doi: https://doi.org/10.1109/AIACT.2017.8020083
16. . Report: Cenzic Application Vulnerability Trends Report: 2014 [Електронний ресурс] // Cenzic. – 2014. – Режим доступу до ресурсу: https://info.cenzic.com/2013-Application-Security-Trends-Report.html.
17. OWASP Secure Coding Practices Quick Reference Guide. // OWASP. – 2010. 4 OWASP Top 10 - 2017 The Ten Most Critical Web Application Security Risks, 2017.
18. The Bobby Tables Guide to SQL Injection. Archived from the original on November 7, 2017. Retrieved October 30, 2017
19. Martin Anderson. Cross-site scripting enabled on 1000 major sites – including financial sites. The Stack. 24 лютого 2016., 205с.
20. CERT Vulnerability Notes Dat abase. Software Engineering Institute. Original Release Date: 2008. – 21с.;
21. NIST Comments on Cryptanalytic Attacks on SHA-1 - NIST Information Technology Laboratory / 2006.

Received (Надійшла) 18.01.2023
Accepted for publication (Прийнята до друку) 08.03.2023

A method of detection of interference in computer systems of electronic document circulation

O. Mozhaiev, F. Sukhina, V. Bashylov

Abstract. Topicality. Our time is characterized by rapid growth in the number and quality of various computer systems. A significant number of them belong to computer systems of electronic data circulation. Such circulation requires the use of reliable protection systems, which the city does not always have in real life. This fact requires the improvement of existing and the development of new methods of detecting facts of unreliable functioning of such computer systems. **The goal of this work** is to develop a method of detecting interference in computer systems of electronic circulation of documents. **The object of research** is the process of functioning of computer systems of electronic circulation of documents. **The subject of research** are methods and algorithms for detecting interference in computer systems. **Results**. This paper proposes a method of detecting interference in computer systems of electronic document circulation. The principles of the Hamming coding algorithm were used to detect interference in computer systems. This method can be a part of a system of methods for detecting interference in computer systems of electronic document circulation, which in turn can be used for the functioning of various critical application computer systems. **Conclusion**. The developed method of detecting interference in computer systems of electronic document circulation is planned to be used in the future to ensure the quality and reliability of the functioning of computer systems of electronic document circulation.

Keywords: computer systems, electronic circulation of documents, coding algorithm, electronic digital signature, cryptography, hash codes.