15. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірян-ня : ДСТУ 4145-2002.
16. Информационная технология. Криптографическая защита информации. Функция хэширования : ГОСТ 34.311.
17. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма : ГОСТ 34.310-95.
18. Свідоцтво про реєстрацію авторського права на твір № 31086. «Комп'ютерна програма «Бібліотека функцій криптографічних перетворень «UPGCryptoProviderBasic»» / А. О. Мелащенко, Є. О. Свиридов.
19. Інформаційні технології. ASN.1 правила кодування. Частина 1. Специфікація правил базового кодування (BER), правил канонічного кодування (CER) та правил витонченого кодування (DER) : Проект ДСТУ ISO/IEC 8825-1.
20. Інформаційні технології. Нотація абстрактного синтаксиса 1 (ASN.1) (у 4-х частинах) : ДСТУ ISO/IEC 8824-1:2002.

Article shows possible solutions of existing problems of interoperability based on signature suite GOST 34.311 + DSTU 4145 implementation, provide suggestions on profiling of GOST 34.311 + DSTU 4145 paramenters, as well as to integrate it into modern operation systems.

**Key words:** *electronic signature, cryptomodule, cryptoalgorithm*

Отримано 24.06.10

УДК 681.511.42:62-83

**В. І. Мороз**, канд. техн. наук,
**В. М. Оксентюк,** канд. техн. наук,
**І. Ф. Снітков, з**ав. лаб. НДЛ-68
Національний університет «Львівська політехніка», м. Львів

## РЕАЛІЗАЦІЯ ОПЕРАЦІЇ ДИФЕРЕНЦІЮВАННЯ У МІКРОКОНТРОЛЕРАХ

У статті пропонується спосіб реалізації цифрового диференціатора для мікропроцесорних і мікроконтролерних систем, який робить його працездатним в широкому діапазоні кроків дискретизації за наявності зовнішніх завад.

**Ключові слова:** *дискретні системи, мікроконтролер, цифрові регулятори, цифровий диференціатор.*

**Постановка проблеми.** Широке розповсюдження цифрової техніки змусило зосередити увагу на особливостях реалізації програмного забезпечення таких систем — необхідності роботи з дискретизованими в часі та квантованими за рівнем даними. При цьому не врахо-

вується, що існуюче математичне забезпечення у більшості випадків передбачає обчислення з нескінченною точністю.

Однією з проблем під час розробки систем керування є технічна реалізація операції диференціювання сигналів, яка значно ускладнюється за наявності в реальних сигналах системи керування високочастотних завад і шумів, що, як правило, складно і не завжди ефективно усуваються фільтрацією. Додатково ускладнюють ситуацію шуми квантування за рівнем, які з'являються в сигналі після проходження через аналогово-цифровий перетворювач (АЦП). Приклад такого сигналу, який отриманий комп'ютерною системою в лабораторних умовах і квантований за рівнем платою вводу/виводу типу ADA-1292 з 12-розрядним АЦП з кроком 10 мс, показано на рис. 1.

**Аналіз останніх досліджень і публікацій.** Широко використовуваний цифровий диференціатор, що реалізований за відомим алгоритмом скінченних різниць першого порядку $\frac{dx}{dt} \approx \frac{x_i - x_{i-1}}{h}$ [1, с. 316; 2; 3], формує задовільний сигнал похідної для незашумленого сигналу (рис. 2), але в реальному випадку (рис. 1) утворює непридатну для системи керування похідну корисного сигналу, що для кроку дискретизації 10 мс проілюстровано на рис. 3. Причиною його незадовільної роботи є як обмежена розрядність даних внаслідок операції квантування та реалізації обчислень, так і наявність високочастотних завад, які підсилюються внаслідок операції диференціювання.

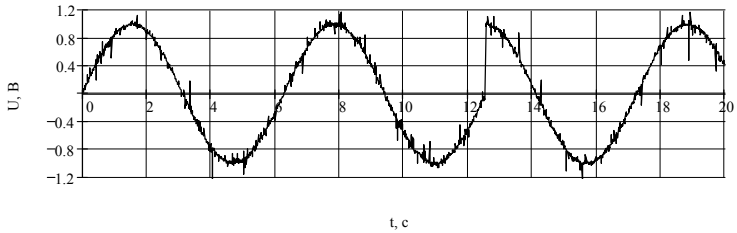


***Рис. 1.*** *Реальний сигнал на вході цифрової системи керування*

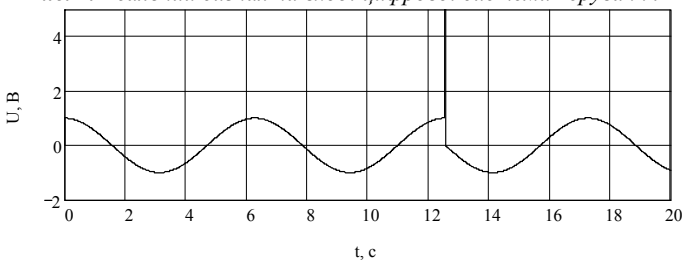


***Рис. 2.*** *Вихідний сигнал цифрового диференціатора за алгоритмом скінчених різниць для незашумленого сигналу і кроку 10 мс*

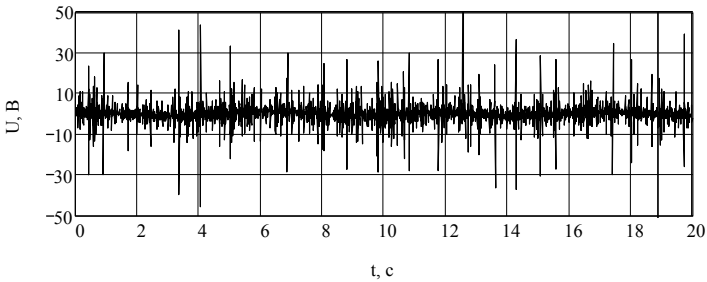


***Рис. 3.*** *Вихідний сигнал цифрового диференціатора за алгоритмом скінчених різниць для реального сигналу (рис. 1) і кроку 10 мс*

**Метою досліджень** є вивчення придатності застосування числово-аналітичного підходу [4, 5] для практичної реалізації цифрової системи керування, зокрема, операції цифрового диференціювання.

**Виклад основного матеріалу**. Зменшити вплив високочастотних завад і збурень можна шляхом їх фільтрації. Структурна схема для практичного здійснення процедури фільтрації у випадку реалізації диференціатора показана на рис. 4, а його передатна функція знаходиться шляхом простих перетворень:

$$W_d(s) = K - \frac{K}{\frac{s}{K}+1} = \frac{s}{\frac{s}{K}+1}.$$

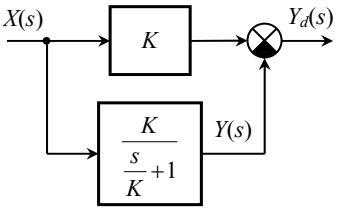


***Рис. 4.*** *Структурна схема пропонованої реалізації цифрового диференціатора*

Для реалізації аперіодичної ланки з передатною функцією $\frac{K}{s/K+1}$ з міркувань простоти і точності застосовано формулу першого порядку, запропоновану в [4, 5]. У результаті отримаємо відповідне рекурентне рівняння для обчислення дискретного вихідного сигналу цієї ланки:

$$y_{i+1} = y_i e^{-h\cdot K} + \left(1 - e^{-h\cdot K}\right)\cdot K \cdot x_i +$$

$$+\left(1 - \frac{1}{h\cdot K}\left(1 - e^{-h\cdot K}\right)\right)\cdot K \cdot (x_i - x_{i-1}).$$

Таким чином, миттєве значення вихідного сигналу $y_d$ пропонованої реалізації реального цифрового диференціатора формуватиметься виразом, що отриманий після простих перетворень:

$$y_{di+1} = K \cdot e^{-h \cdot K} \cdot x_i - \left(1 - \frac{1}{h \cdot K}\left(1 - e^{-h \cdot K}\right)\right) \cdot K \cdot (x_i - x_{i-1}) - y_i e^{-h \cdot K}.$$

Потрібно відзначити, що в системі реального часу можливе застосування лише явних форм рекурентних рівнянь, оскільки інформація про значення сигналу в i+1-ій точці ще не відома (умова фізичної реалізованості). Для порівняння з традиційним методом з використанням скінчених різниць на рис. 5 і рис. 6 показано вихідний сигнал реалізації диференціатора пропонованим способом для кроку дискретизації 10 мс і K = 5.

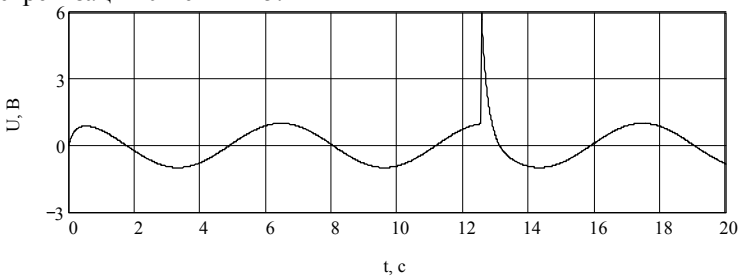


***Рис. 5.*** *Вихідний сигнал пропонованої реалізації цифрового диференціатора для аналітичного сигналу для кроку h = 10 мс і K = 5*

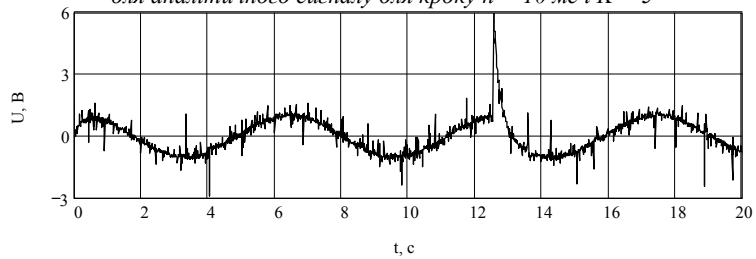


***Рис. 6.*** *Вихідний сигнал пропонованої реалізації цифрового диференціатора для реального сигналу для кроку h = 10 мс і K = 5*

Аналогічні результати для малих кроків забезпечує і використання явного (з умов фізичної реалізованості) числового методу інтегрування Адамса другого порядку: $y_{i+1} = y_i + \frac{h}{2T}\left(3x_i - x_{i-1}\right)$ для формування рекурентної формули моделі ланки $\frac{K}{s/K+1}$:

$$y_{i+1} = y_i \cdot \left(1 - \frac{3K \cdot h}{2}\right) + \frac{K \cdot h}{2} \cdot y_{i-1} + \frac{h \cdot K^2}{2} \cdot (3x_i - x_{i-1}).$$

Відмінності у поведінці різних реалізацій диференціаторів починаються зі збільшенням кроку — зростання періоду дискретизації до 0.2 с при періоді вхідної синусоїди π с (це складає приблизно 16 відліків на період) вже робить цифровий диференціатор на основі класичного числового методу непридатним через числову нестійкість, що проілюстровано на рис. 7 (використання формули числового інтегрування за Адамсом), на рис. 8 (цифровий диференціатор за схемою скінченних різниць) і на рис. 9 (пропонований варіант реалізації цифрового диференціатора).

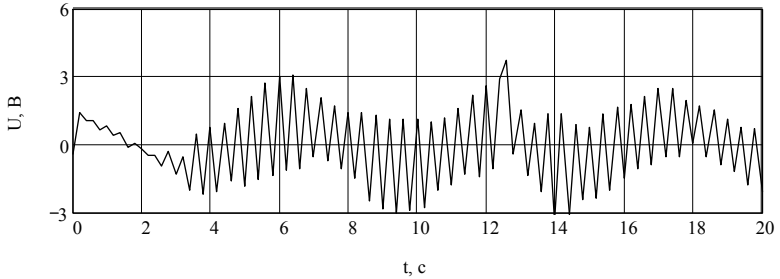


***Рис. 7.*** *Вихідний сигнал цифрового диференціатора на основі явного методу Адамса для реального сигналу і кроку* $h = 0.2$ *с та* $K = 5$

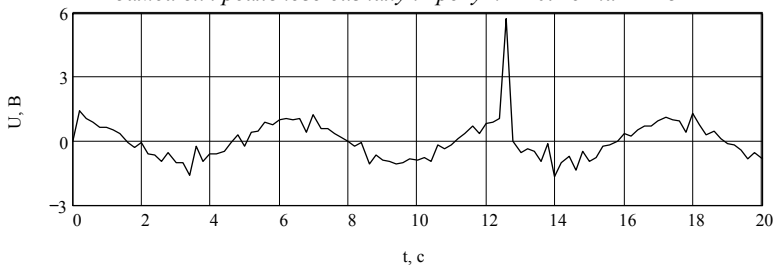


***Рис. 8.*** *Вихідний сигнал цифрового диференціатора за схемою скінчених різниць для реального сигналу і кроку* $h = 0.2$ *с*

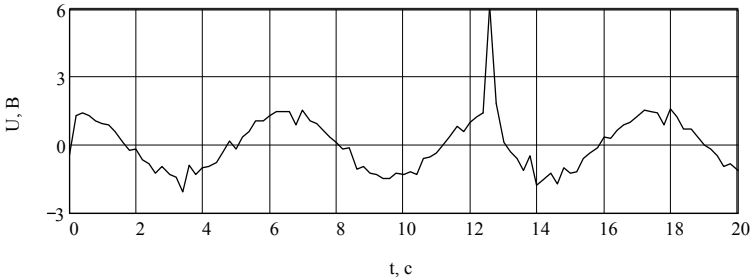


***Рис. 9.*** *Вихідний сигнал пропонованої реалізації цифрового диференціатора для реального сигналу і кроку* $h = 0.2$ *с та* $K = 5$

**Висновок.** Аналіз результатів проведених експериментальних досліджень показав, що лише реалізація цифрового диференціатора на основі розроблених рекурентних формул [4, 5] забезпечила достатню точність диференціювання для різних типів сигналу і широкого діапазону кроків дискретизації. Традиційні способи реалізації цифрового диференціатора, як показали експерименти, можуть бути використані лише за певних обмежень стосовно виду сигналу та періоду дискретизації. Ще однією перевагою застосування розробленого методу для виконання операції диференціювання в системах керування є його простота програмної реалізації: після підстановки конкретних значень у рекурентну формулу та виконання спрощень, вираз для обчислень може бути зведений до кількох арифметичних операцій множення та додавання і віднімання, що нескладно реалізується навіть у простих мікроконтролерах з обмеженою розрядністю даних.

**Список використаних джерел:**

1. Куо Б. Теория и проектирование цифровых систем управления / Б. Куо ; пер. с англ. ; под ред. проф. П. И. Попова. — М. : Машиностроение, 1986. — 448 с. (наукове видання).
2. Клиначев Н. В. Теория автоматического управления : Учебно-методический комплекс / Н. В. Клиначев. — Offline версия 2.9. Челябинск, 2003. — Режим доступу до ресурсу : http://www.vissim.nm.ru.
3. Буянкин В. М. Теория цифрового электропривода [Електронний ресурс] / В. М. Буянкин. — М. : МГТУ им. Н. Э. Баумана, 2005. — Режим доступу : http://privodi.narod.ru/1_1.files.
4. Мороз В. Ефективні рекурентні формули для комп'ютерного моделювання електромеханічних систем / В. Мороз // Вісник Національного університету "Львівська політехніка" "Електроенергетичні та електромеханічні системи". — 2007. — № 597. — С. 3—11.
5. Moroz V. Computer simulation of the electromechanical systems using convolution integral / V. Moroz // Elektrotechnika. — 14 (2009). — Uniwersytet technologiczno-przyrodniczy im. Jana 1 Jкdrzeja Њniadeckich w Bydgoszczy. Zeszyty naukowe NR 254. — P. 17—24. (ISSN 0209-0570).

The approach for digital differentiation for microcontrollers with robustness in wide range of the sampling steps is presented.

**Key words:** *digital controller, digital differentiator, digital system, microcontroller.*

Отримано17.05.10