КІБЕРНЕТИКА

УДК 51.681.3

С.Л. КРИВИЙ
Київський національний університет імені Тараса Шевченка, Київ, Україна,
e-mail: *sl.krivoi@gmail.com.*

В.М. ОПАНАСЕНКО
Інститут кібернетики ім. В.М. Глушкова НАН України, Київ, Україна,
e-mail: *opanasenkoincyb@gmail.com*.

О.О. ГРІНЕНКО
Київський національний авіаційний університет, Київ, Україна,
e-mail: *olena.hrinenko@npp.nau.edu.*

Ю.О. НОРТМАН
Київський національний університет імені Тараса Шевченка, Київ, Україна,
e-mail: *ynortman@gmail.com.*

СИМЕТРИЧНА СИСТЕМА ОБМІНУ ІНФОРМАЦІЄЮ НА ОСНОВІ ІЗОМОРФІЗМУ КІЛЕЦЬ

Анотація. Пропонуються алгоритми обміну повідомленнями між абонентами на основі властивостей скінченних асоціативно-комутативних кілець з одиницею та діофантових рівнянь над такими кільцями. Наведено алгоритми побудови скінченних кілець, адитивні групи яких повноциклічні, та алгоритми побудови ізоморфізму між кільцем k-го порядку, адитивна група якого повноциклічна, і кільцем лишків Z_k за модулем k.

Ключові слова: криптографічний протокол, ізоморфізм, кільце, алгоритм.

ВСТУП

У цій статті запропоновано алгоритми обміну повідомленнями між абонентами на основі властивостей асоціативно-комутативних кілець з одиницею та систем лінійних діофантових рівнянь над такими кільцями. Ця робота є продовженням робіт [1, 2].

НЕОБХІДНІ ОЗНАЧЕННЯ ТА ПОНЯТТЯ

Наведемо означення і поняття, які потрібні далі для викладу.

Означення 1. Універсальна алгебра $G(A,\Omega)$ називається кільцем, якщо вона є Абелевою групою стосовно додавання, групоїдом стосовно множення та для довільних її елементів $a, b, c \in A$ виконуються закони дистрибутивності:

$$a(b+c) = (ab) + (ac), \quad (a+b)c = (ac) + (bc).$$

Це означає, що Ω містить чотири операції: бінарні операції додавання і множення, унарну операцію взяття протилежного стосовно операції додавання і нульарну операцію, яка фіксує нульовий елемент Абелевої групи кільця. Нульовий елемент називається нулем кільця.