Міністерство освіти і науки України
Харківський національний університет імені В. Н. Каразіна

О. О. Кузнецов
М. О. Полуяненко
О. О. Полуяненко

ОГЛЯД СУЧАСНИХ АЛГОРИТМІВ ГЕШУВАННЯ У БЛОКЧЕЙН-СИСТЕМАХ

КОНСПЕКТ ЛЕКЦІЙ

з дисципліни
«Технології блокчейн»

для студентів
спеціальності 125 «Кібербезпека»

Харків – 2021

УДК 004.031.43
К 89

Рецензенти:

О. В. Лемешко – доктор технічних наук, професор, завідувач кафедри інфокомунікаційної інженерії імені В. В. Поповського Харківського національного університету радіоелектроніки;

О. Г. Толстолузька – доктор технічних наук, старший науковий співробітник, професор кафедри теоретичної та прикладної системотехніки факультету комп'ютерних наук Харківського національного університету імені В. Н. Каразіна.

Затверджено до друку рішенням Науково-методичної ради
Харківського національного університету імені В. Н. Каразіна
(протокол № 5 від 10 червня 2021 року)

Кузнецов О. О.

К 89 Огляд сучасних алгоритмів гешування у блокчейн-системах : конспект лекцій з дисципліни «Технології блокчейн» для студентів спеціальності 125 «Кібербезпека» / О. О. Кузнецов, М. О. Полуяненко, О. О. Полуяненко. – Харків : ХНУ імені В. Н. Каразіна, 2021. – 140 с.

Важливою складовою сучасних інформаційних технологій та комп'ютерних систем є криптографічні методи та засоби захисту інформації. П'ята частина «Огляд сучасних алгоритмів гешування у блокчейн-системах» конспектів лекцій для студентів факультету комп'ютерних наук за спеціальністю «Кібербезпека» присвячена дослідженню сучасних криптографічних примітивів для їх застосування в децентралізованих системах блокчейн. Зокрема досліджуються властивості різних сімейств криптографічних геш-функцій, аналізуються різні шляхи їхньої побудови та вивчається сучасний стан у галузі стандартизації та практичного застосування криптографічних функцій гешування для побудови розподілених інформаційних систем типу блокчейн. Розглянуті у даній частині конспекту лекції алгоритми криптографічного гешування застосовуються у понад 90 % існуючих проектів децентралізованих систем за технологією блокчейн. До цього опису долучено також національний алгоритм криптографічного гешування «Купина», який стандартизовано у національному стандарті.

УДК 004.031.43

Навчальне видання

Кузнецов Олександр Олександрович
Полуяненко Микола Олександрович
Полуяненко Ольга Олександрівна

**ОГЛЯД СУЧАСНИХ АЛГОРИТМІВ
ГЕШУВАННЯ У БЛОКЧЕЙН-СИСТЕМАХ**

Конспект лекцій з дисципліни «Технології блокчейн»
для студентів спеціальності 125 «Кібербезпека»

Коректор *О. В. Анцибора*
Комп'ютерне верстання *В. В. Савінкова*
Макет обкладинки *І. М. Дончик*

Формат 60 х 84/16. Ум. друк. арк. 8,30. Наклад 50 пр. Зам. № 211/21.

Видавець і виготовлювач
Харківський національний університет імені В. Н. Каразіна,
61022, м. Харків, майдан Свободи, 4.
Свідоцтво суб'єкта видавничої справи ДК № 3367 від 13.01.2009
Видавництво ХНУ імені В. Н. Каразіна
Тел. 705-24-32

ЗМІСТ