Об’єктом дослідження є блоковий алгоритм шифрування – національний стандарт Російської Федерації ГОСТ Р 34.12-2015. Предметом дослідження є стійкість даного шифру до цілочисельного різницевого криптоаналізу. Методами дослідження є методи лінійної та абстрактної алгебри, теорії імовірностей, теорії складності алгоритмів, методи комп’ютерного та статистичного моделювання. Наукова новизна одержаних результатів. В роботі вперше одержано аналітичні оцінки практичної стійкості шифру ГОСТ Р 34.12-2015 «Кузнєчік» до цілочисельного різницевого криптоаналізу. Також побудовано статистичні розподіли оцінок, що дозволяють сприймати оцінки цих параметрів для S-блоку, зазначеного у стандарті, у контексті загальної картини, характерної для S-блоків такого розміру Практичне значення одержаних результатів. Одержані в роботі результати дозволяють обґрунтувати надійність нелінійного перетворення зазначеного у специфікації шифру «Кузнєчік». Статистичні розподіли оцінок можуть використовуватися на практиці для оцінювання стійкості до цілочисельного різницевого криптоаналізу інших шифрів, які містять 8-бітові S-блоки. Результати роботи були продемонстровані під час роботи наукової конференції «Теоретичні і прикладні проблеми фізики, математики та інформатики».

БЛОКОВІ ШИФРИ, РІЗНИЦЕВИЙ КРИПТОАНАЛІЗ, МАРКОВСЬКІ ШИФРИ, ЦІЛОЧИСЕЛЬНИЙ ДИФЕРЕНЦІАЛ, ПОБУДОВА ВЕРХНІХ ОЦІНОК ІМОВІРНОСТЕЙ.