Об’єктом дослідження виступає сімейство блокових шифрів легковагової криптографії SIMECK. Предметом дослідження є рівень захищеності сімейства блокових шифрів до диференціального криптоаналізу SIMECK. Методами дослідження є побудова шифру SIMECK зі змінними параметрами та застосування методів диференціального криптоаналізу щодо даної реалізації. Наукова новизна одержаних результатів. Дане сімейство шифрів SIMECK є маловивченим, оскільки було нещодавно створене. В даній роботі були застосовані методи диференціального криптоаналізу, які до цього часу використовувалися для сімейства SIMON, на основі якого побудований даний шифр, але не були реалізовані для шифру

SIMECK. LIGHTWEIGHT КРИПТОГРАФИЯ, SIMON, SPECK, SIMECK, ДИФЕРЕНЦІАЛЬНИЙ КРИПТОАНАЛІЗ.