Дана робота присвячена обчисленню верхніх границь диференціальних імовірностей для класу немарковських фейстель-подібних схем із певною структурою раундової функції. Верхні границі дають змогу говорити про теоретичну (доказову) стійкість шифрів даного класу до диференціального криптоаналізу. На сьогоднішній день існують десятки схем, що базуються на схемі Фейстеля або її модифікаціях. Існуючі аналітичні оцінки стійкості таких шифрів можна суттєво уточнити, якщо враховувати структуру раундових перетворень, тому задача цієї роботи полягає в отриманні ефективного методу для обчислення більш точних оцінок стійкості до диференціального криптоаналізу.

В ході роботи було узагальнено запропонований Ліамом Келіхером метод обчислення верхніх меж імовірностей диференціалів на ряд схем на основі схеми Фейстеля, L-схеми (MISTY) та R-схеми. Запропонований метод застосовано до моделей шифрів, що використовують різні лінійні перетворення та S-блоки відомих алгоритмів шифрування – національних стандартів України, США та Білорусі. Показано, що запропонований метод значно підсилює відомі аналітичні результати для немарковських шифрів. Також продемонстровано, що оцінки стійкості шифрів будуть залежати не тільки від характеристик S-блоків, але й від параметрів лінійних перетворень, які використовуються у алгоритмах шифрування.