Диференціальний криптоаналіз є одним з найпотужніших методів аналізу сучасних блочних шифрів. Незбалансовані узагальнені схеми Фейстеля є поширеним та ефективним напрямком для синтезу нових алгоритмів шифрування, тому оцінки стійкості до диференціального аналізу для цих схем є необхідними умовами для обґрунтування загальної надійності таких шифрів.

Метою роботи є отримання оцінок верхніх меж імовірностей існування нетривіальних диференціалів схем блочного шифрування із різною кількістю раундів. Отримання даних оцінок досягається шляхом розглядання всіх можливих диференціальних переходів під час шифрування. Ґрунтуючись на аналізі одержаних даних, фактично розв’язується задача пошуку достатньої кількості раундів для досягання заданого рівня теоретичної стійкості до атак диференціального аналізу на узагальнені схеми Фейстеля.

Дане дослідження може виступати основою для доведення доказової теоретичної стійкості довільних модифікацій узагальнених схем Фейстеля до диференціального аналізу та побудови точних аналітичних оцінок стійкості. Одержані в роботі результати можуть бути використані для обґрунтування надійності нових перспективних блочних шифрів.