Актуальність роботи. На сучасному етапі розвитку суспільства однією з найбільших цінностей стала інформація. Важливим питанням на сьогоднішній день є захист інформації. Існує декілька напрямків та підходів до захисту інформації, і один із них це криптологія, тобто захист математичними методами. Розвиток електронно-обчислювальної техніки та математичного апарату дає зловмисникам все більше можливостей для дешифрування інформації. З плином часу до алгоритмів шифрування висуваються все більш суворі вимоги, а кожний новий запропонований метод перевіряється все більш детально на велику кількість вразливостей.

Одним із найпоширеніших методів криптографічного захисту конфіденційності інформації є блочні симетричні шифри. На сьогодні відомо багато таких шифрів, які щодня захищають велику кількість інформації. Тому питання про їхню стійкість турбує криптографічну спільноту й є як ніколи актуальним.

S-блок – нелінійне булеве перетворення, яке знайшло своє застосування в блочних шифрах для ускладнення залежності між бітами відкритого та зашифрованого текстів. Тому характеристики S-блоку дуже сильно впливають на стійкість всього шифру.

Алгоритм «Калина-2» – симетричний блочний шифр побудований за принципом SP-мережі. Нещодавно цей шифр було затверджено в якості державного стандарту шифрування України ДСТУ 7624:2014 [1]. Нелінійність забезпечує шар із шістнадцяти S-блоків, серед яких чотири різні. Автори стверджують, що вони були вибрані випадковим чином. Також нас цікавить його попередня версія 2007 під назвою «Калина» [2].

Мета та завдання роботи. Метою роботи є аналіз методів тестування криптографічних S-блоків на наявність прихованих аналітичних структур.

Для досягнення мети необхідно виконати такі завдання:

1) проаналізувати існуючі методи виявлення прихованих аналітичних структур у криптографічних S-блоках;

2) дослідити розподіли криптографічних параметрів S-блоків та побудувати на їх основі алгоритми перевірки «випадковості» генерації S-блоків;

3) перевірити пропонованими методами S-блоки двох версій алгоритму «Калина».

Об'єкт дослідження. Об'єктом дослідження є інформаційні процеси в системах криптографічного захисту.

Предмет дослідження. Предметом дослідження є методи перевірки криптографічних S-блоків на наявність прихованих структур.

Наукова новизна отриманих результатів. Запропоновано метод перевірки випадковості S-блоків на основі розподілів різниць за операцією додавання за модулем. Перевірено структуру S-блоків шифрів «Калина» та «Калина-2» на наявність внутрішніх аналітичних структур і показано, що вони були щонайменше дороблені певним аналітичним чином для підвищення стійкості до диференціального та лінійного криптоаналізу.

Практичне значення отриманих результатів. Розглянуті та запропоновані в роботі методи можна використовувати для аналізу криптографічної стійкості алгоритмів шифрування та їх окремих елементів.

Апробація результатів. Результати роботи були представлені на XIV Всеукраїнській науково-практичній конференції студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики» (м.Київ, 2016) та Міжнародній науково-практичній конференції «Інформаційні технології та комп’ютерне моделювання» (м.Івано-Франківськ – Яремче, 2016).