Актуальність роботи

Стан захисту інформації залежить не тільки від теоретичних напрацювань і досліджень, але й також від практичного впровадження механізмів та алгоритмів в інформаційно-комунікаційні системи, в тому числі й криптографічні. Особливо актуальне питання проектування та розробки систем на початкову етапі, оскільки від нього залежить подальший стан безпеки та функціонування усіх залежних частин. Виявлення та нейтралізація слабких місць в системі, як показує багаторічний досвід, на початковому етапі функціонування будь-якої інформаційної системи вимагає найменше людських та фінансових ресурсів і зусиль. Тому, важливим є питання дослідження причин, через які можуть виникати слабкі місця в криптографічних системах та як саме ці причини впливають на стійкість, живучість та надійність системи в цілому.

З інженерної точки зору нас цікавлять саме технічні аспекти виникнення слабких місць і подальші можливості зловмисника при реалізації атак за сторонніми каналами на ті частини системи, де можуть використовуватись криптографічні механізми.

Мета і завдання дослідження

З теоретичної точки зору метою роботи є дослідження впливу помилок, які виникають при реалізації криптографічних систем на практичну стійкість цих криптосистем. З практичної точки зору важливим моментом є можливість та складність реалізації атак за сторонніми каналами, що використовують дані помилки.

Об’єкт дослідження – помилки проектування при побудові систем, що використовують криптографічні механізми

Предмет дослідження – атаки сторонніми каналами, реалізовані за допомогою помилок при проектуванні інформаційно-комунікаційних систем

Методи дослідження – в процесі дослідження реалізовувались атаки за сторонніми каналами на інформаційно-комунікаційні системи, що працюють на сучасних операційних системах.

Наукова новизна одержаних результатів

Розглянуті практичні помилки, що можуть призводити до появи слабких місць, навіть в тих місцях інформаційної системи, де використовуються сучасні стійкі з математичної точки зору криптографічні примітиви. Продемонстровано, як саме зловмисник, використовуючи, на перший погляд, незначні помилки при проектуванні та реалізації системи, може створювати загрози компрометації всієї системи. Для більшої ефективності виявлення та вивчення слабких місць в системах була розглянута сучасна платформа тестування найнебезпечніших на сьогоднішній день загроз WEB додатків, що працюють в трирівневій архітектурі інформаційно-комунікаційній системі.