

ОЦІНЮВАННЯ АЛГОРИТМІВ ТА АРХІТЕКТУРИ АНОНІМНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ СПІЛКУВАННЯ

НІКУЛІНА О.М., ЗАХАРОВ М.В., САВЧЕНКО Д.В.

*Національний технічний університет
«Харківський політехнічний інститут», м. Харків*

Дослідження направлене на оцінювання анонімності методів протидії несанкціонованій розкриття ідентичності суб'єктів у комунікаційних системах. Мета цієї доповіді – описати як певні моделі та методи анонімних комунікацій впливають на рівень конфіденційності у процесі обміну інформації, а також описати деякі деталі протоколу комунікації. Актуальність теми даної роботи обумовлена необхідністю створення систем і протоколів для пересилання, обміну даними без несанкціонованого втручання сторонніх суб'єктів у цей комунікаційний процес. Система, що досліджується, являється децентралізованою одноранговою системою для обміну миттєвими повідомленнями. Система використовує розподілену хеш-таблицю на базі протоколу Kademlia для зберігання повідомлень; важливою особливістю системи являється відсутність наявності незашифрованої інформації о відправниках і отримувачах у пакетах повідомлень. Для оцінювання ступеня анонімності d використано метод інформаційної ентропії. Для тестування рівня анонімності інформаційної системи, у якості експерименту, необхідно було відворити атаку, в якій зломисник з набору анонімності кількості N намагається виявити відправників повідомлень, знаючи підмножину некорумпованих або невиявлених користувачів кількістю S . Модель атаки: атакувач спроможний прослуховувати повідомлення N користувачів, де деяка кількість анонімного набору користувачів N унікальна для кожної тестової конфігурації. При кожному відправленому повідомленню атакувач випадково визначає відправників повідомлення з множини невиявлених і некорумпованих користувачів.

Тести здійснено на трьох тестових конфігураціях, де розмір анонімного набору $N = 100$ (загальної кількості користувачів), а набір можливих невиявлених відправників для кожного середовища $S = 10$, $S = 20$ і $S = 30$. Для кожного тестового сценарію здійснено 500 відправлень повідомлень. Нижче у таблиці 1 зазначено результати тестування, де S мало значення 10, 20 і 30 користувачів.

Таблиця 1 – Результати тестування

S , кількість некорумпованих користувачів	Точність ідентифікації користувача	d , ступінь анонімності
10	11,34%	0,5
20	5,26%	0,65
30	3,44%	0,73

Згідно з отриманими результатами можна зробити висновок, що вірогідність компрометації конфіденційності користувачів знижується зі зростанням ступеню анонімності системи та кількістю некорумпованих користувачів.