SHA-256 В АВТОРИЗАЦІЙНИХ СИСТЕМАХ: ЗБЕРІГАННЯ ПАРОЛІВ І БЕЗПЕЧНА ІДЕНТИФІКАЦІЯ. НАЙКРАЩІ ПРАКТИКИ ТА АЛЬТЕРНАТИВИ

Чаплін А.А., Сенько А.В.
Національний технічний університет «Харківський політехнічний інститут», м. Харків

Доповідь присвячена дослідженню застосування криптографічного алгоритму SHA-256 в авторизаційних системах, з акцентом на зберігання паролів і безпечної ідентифікації користувачів. Алгоритм SHA-256 широко використовується завдяки своїй криптографічній стійкості та швидкості обчислень. Однак його застосування в авторизаційних системах вимагає дотримання певних практик, а в деяких випадках – розгляду альтернативних рішень.

Метою роботи є аналіз застосування SHA-256 для хешування паролів та ідентифікації користувачів, виявлення найкращих практик і порівняння з альтернативними алгоритмами, які розроблені для цих завдань. Розглядаються переваги та обмеження SHA-256 у контексті сучасних вимог до безпеки.

SHA-256 являє собою криптографічну хеш-функцію, що перетворює дані довільної довжини на 256-розрядний хеш із високим ступенем незворотності та стійкості до колізій. Вона широко застосовується в авторизаційних системах для безпечного зберігання паролів і генерації токенів автентифікації, наприклад, у протоколах OAuth або JWT. Проведене дослідження показало, що SHA-256 цінується за швидкість і універсальність, але для хешування паролів вимагає додаткових заходів, таких як соління і багаторазове хешування, щоб протистояти атакам brute-force. Під час аналізу було розглянуто альтернативні алгоритми, включно з Argon2, bcrypt і PBKDF2, спеціально розроблені для хешування паролів, які мають механізми сповільнення обчислень, що робить їх стійкішими до атак із використанням GPU або ASIC. Порівняння, виконане в рамках дослідження, виявило, що Argon2, завдяки ефективному використанню пам'яті, і bcrypt, з адаптивною складністю, перевершують SHA-256 у завданнях зберігання паролів, тоді як SHA-256 залишається оптимальним для завдань ідентифікації, де важлива швидкість. На основі аналізу запропоновано рекомендації: використовувати SHA-256 з посиленими заходами безпеки в наявних системах, віддавати перевагу Argon2 або bcrypt у нових розробках і забезпечувати захист хешів на рівні бази даних.

У рамках цієї роботи було реалізовано власну версію алгоритму SHA-256, оптимізовану для використання в авторизаційних системах, із застосуванням методів соління та багаторазового хешування. Також було розроблено програму для тестування алгоритму, проведено порівняльні тести з алгоритмами Argon2, bcrypt і PBKDF2, а також виконано аналіз отриманих результатів. Результати демонструють можливість ефективного застосування SHA-256 у задачах ідентифікації при дотриманні найкращих практик, але підтверджують перевагу спеціалізованих алгоритмів для хешування паролів, що підкреслює важливість вибору відповідного рішення для забезпечення безпеки сучасних систем.