УДК 004.056

МЕТОД АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ КОМП'ЮТЕРНОЇ МЕРЕЖІ З ПРИВ'ЯЗКОЮ ДО ПАРАМЕТРІВ РОБОЧОЇ СТАНЦІЇ

Ю. В. Баришев, асистент; К. І. Кривешко, студент
Вінницький національний технічний університет
yuriy.baryshev@gmail.com

Автентифікація користувачів комп'ютерної мережі передбачає передавання даних мережею, що, у більшості випадків дозволяє зловмисникам перехоплювати дані, що пересилаються. В даний час найпоширенішими методами автентифікації користувачів комп'ютерних мереж є такі:

- відправлення пароля у відкритому вигляді на сервер, де відбувається перевірка збігу з існуючими в спеціалізованій базі даних паролями;
- використання хеш-функцій – на сервер відправляється не сам пароль, а його хеш-значення. При цьому отримане хеш-значення порівнюється сервером з хеш-значеннями в спеціалізованій базі даних.

В обох випадках, зловмисник, перехопивши пароль або його хеш-значення, має змогу здійснити вхід у систему від імені легального користувача, з будь-якого комп'ютера. Це обумовлює актуальність досліджень, направлених на обмеження кількості комп'ютерів, з яких відбувається автентифікація користувачів.

Авторами пропонується метод автентифікації користувачів, який полягає в обмежені кількості робочих станцій, з яких можна здійснити вхід у систему за рахунок хешування параметрів робочих станцій при автентифікації користувачів. Даний метод схематично наведено на рис. 1.

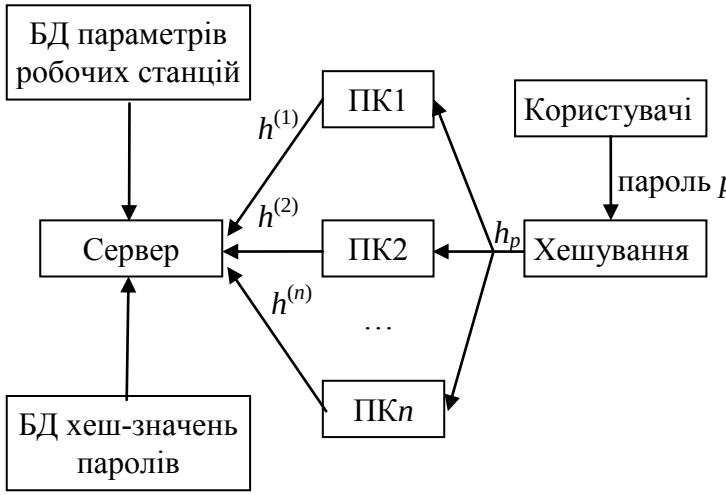

Рисунок 1 – Схематичне зображення автентифікації користувача комп'ютерної мережі

Запропонований метод автентифікації передбачає виконання таких дій:

- введення користувачем паролю p та обчислення хеш-значення цього паролю $h_p = f(h_0, p)$, де $f(\cdot)$ – хеш-функція, h_0 – вектор ініціалізації;

- хешування значень параметрів робочої станції, з якої відбувається автентифікація $h = f(h_p, PC)$;

- пересилання h до сервера;

- порівняння сервером хеш-значення h з еталонним, визначених на основі спеціалізованих баз даних.

"Прив'язка" користувачів до робочих станцій дозволяє не лише здійснити автентифікацію довірених користувачів, але й визначити множину довірених робочих станцій. Отже, зловмиснику для успішної автентифікації необхідно не лише знати пароль (хеш-значення пароля) легального користувача, але й отримати доступ до довіреної робочої станції.