АНАЛІЗ СУЧАСНИХ АЛГОРИТМІВ І МЕТОДІВ АУТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ

канд. техн. наук, доц. В.С. Бреславець, ст. викл. І.Л. Яценко, магістр А.С. Васильєва, Національний технічний університет "Харківський політехнічний інститут", м. Харків

В останні десятиліття значне зростання продуктивності обчислювальних засобів, розвиток телекомунікаційних систем і технологій передачі, обробки та зберігання даних стимулювали активне перенесення все більшого числа економічних процесів в електронну сферу. Для забезпечення інформаційної безпеки, одним з важливих завдань є використання новітніх методів та засобів зберігання інформації для того щоб бути впевненими в захищеності даних. Для цього час від часу треба оновлювати алгоритми шифрування даних. Тому перед комерційними платформами постає тяжкий виклик забезпечити якісне та надійне обслуговування своїх клієнтів.

Більшість комерційних платформ мають мільйони зареєстрованих користувачів, і перехешування всіх паролів користувачів може зайняти деякий час від кількох днів до декількох місяців. Під час цього процесу сайт не буде працювати, доки всі користувачі не оновлять паролі до нового алгоритму хешування.

У зв`язку з цим був розроблений модуль, який дозволить оновити користувачів до нового хешу набагато швидше. Система відповідає сучасним вимогам безпеки [1 – 4].

Список літератури: 1. *Шаньгин В.Ф.* Защита компьютерной информации. Эффективные методы и средства / *В.Ф. Шаньгин* – М.: ДМК Пресс, 2010. – 544 с. **2.** *Хамидуллин Р.Р.* Методы и средства защиты компьютерной информации / *Хамидуллин Р.Р., Бригаднов И.А., Мороз А.В.* – СПб.: СЗТУ, 2005. – 178 с. **3.** Cost of Computer Crime. Режим доступу: http://www.citadel-information.com/library2/4/2004-fbi-csi-surveys.pdf. **4.** *Чэн Ш.-К.* Принципы проектирования систем защиты информации / *Ш.-К. Чэн.* – М.: Мир, 1994. – 204 с.