УДК 004.056

РОЗРОБКА МОДУЛЬНОЇ СИСТЕМИ ДВОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ НА ОСНОВІ ПАРОЛЮ ТА ОДНОРАЗОВОГО КОДУ

М.І. Главчев[1], ***Є.О. Буликін[2]***

[1] *професор кафедри комп'ютерної інженерії та програмування, канд. екон. наук, НТУ «ХПІ», Харків, Україна*

2 магістрант кафедри комп'ютерної інженерії та програмування, НТУ «ХПІ», Харків, Україна

maksym.glavchev@khpi.edu.ua

В умовах зростання кіберзагроз, захист облікових записів користувачів є критично важливим завданням. Класична парольна автентифікація не забезпечує достатнього рівня безпеки, що робить системи вразливими до атак перебору та компрометації. Впровадження другого фактора автентифікації значно підвищує надійність, однак вимагає розробки рішень, які були б не тільки безпечними, але й швидкими, гнучкими та легко інтегрованими в існуючі веб-додатки. Сучасні підходи до двофакторної автентифікації включають використання апаратних токенів, біометричних даних та програмних генераторів кодів (TOTP). Хоча ці методи є ефективними, їх інтеграція може бути складною та ресурсомісткою. Багато готових рішень є монолітними, що ускладнює їхню модифікацію та адаптацію до специфічних вимог проєкту, зокрема, до заміни криптографічних алгоритмів без повної перебудови системи.

Розроблено програмний модуль двофакторної автентифікації з модульною архітектурою. Першим фактором є традиційна парольна схема. Другий фактор реалізовано через надсилання одноразового коду підтвердження на електронну пошту користувача за допомогою SMTP протоколу. Для генерації коду використовується криптографічний метод, що включає salt-рядок та ідентифікатор користувача, які додаються до хешу на основі алгоритму SHA-1. Перевагою архітектури є її компонентна структура, що дозволяє в майбутньому легко замінювати криптоалгоритми на більш сучасні та продуктивні. Взаємодія з базою даних здійснюється через EntityFramework, що забезпечує високу швидкість обробки запитів.

Проведене тестування та експлуатація розробленого програмного модуля підтвердили його повну відповідність поставленим задачам. Система успішно виконує автентифікацію суб'єктів, відповідаючи ключовим критеріям швидкості, надійності та мобільності (гнучкості архітектури). Обраний алгоритм SHA-1 забезпечив оптимальний баланс між стійкістю до атак та продуктивністю, а модульний підхід гарантує довгострокову актуальність та легкість модернізації рішення.

Список літератури:

1 Корченко О. Г., Бєгун А. В. Аналіз стійкості криптографічних хеш-функцій сімейства SHA до атак знаходження колізій // Захист інформації. – 2019. – Т. 21, № 4. – С. 220-228. DOI: https://doi.org/10.18372/2410-7840.21.14253

2 Швидкий М. А., Поліщук Є. С. Методи та засоби реалізації багатофакторної автентифікації у веб-додатках // Вісник Національного технічного університету "ХПІ". Серія: Нові рішення в сучасних технологіях. – 2021. – № 1(7). – С. 58-63. DOI: https://doi.org/10.20998/2413-4295.2021.01.08

3. Главчев М.І. Формування засобу криптографічної аутентифікації/МІ Главчев, ОІ Баленко, ЄО Буликін / Проблеми інформатики та моделювання (ПІМ–2025) : тези 25-ї міжнар. наук.-техн. конф., 25-28 вересня 2025 р. / наук. ред. Леонов С. Ю. ; Нац. акад. наук України [та ін.]. – Харків : НТУ "ХПІ", 2025.. – С.33, https://repository.kpi.kharkov.ua/handle/KhPI-Press/93467