

## ФОРМУВАННЯ ЗАСОБУ КРИПТОГРАФІЧНОЇ АУТЕНТИФІКАЦІЇ

*канд. екон. наук, проф. М.І. Главчев, канд. техн. наук, доц.  
О.І. Баленко, магістр Є.О. Буликін, НТУ "ХПИ", м. Харків*

У сучасному цифровому середовищі забезпечення надійної аутентифікації є необхідною умовою безпечної взаємодії користувачів із інформаційними системами. Робота присвячена формуванню засобу криптографічної аутентифікації, як інструменту підтвердження особи на основі криптографічних принципів. Розробка такого засобу базується на поєднанні симетричних та асиметричних алгоритмів та обміну ключами. Симетричні алгоритми забезпечують високу продуктивність, тоді як асиметричні — надійне встановлення ключів та масштабованість. Особливу увагу приділено використанню SIN-based (signature-based) аутентифікації, де користувач підписує певний виклик (challenge), що дозволяє підтвердити його особу без передачі паролів.

Важливою складовою є фазове формування коефіцієнтів автентичності: під час ідентифікації система оцінює правильність відповіді та валідність підпису, а потім підтверджує справжність користувача. Для захисту ключових компонентів застосовуються структури з відкритим ключем (PKI), які гарантують безпечне зберігання й обмін сертифікатами. Ключовим викликом є стійкість до викрадення ключів та атаки "людина посередині" (MitM), що вимагає впровадження Authenticated Key Exchange – протоколів, які одночасно встановлюють ключ та перевіряють ідентичність сторін, а саме протоколи із гарантованим прямим захистом і взаємною аутентифікацією. Фінальним компонентом пропонуваного засобу є практична реалізація на моделі, що включає сервер і клієнт у ролі учасників, обмін підписаними викликами, перевірку сертифікатів через PKI та логування результатів аутентифікації. Такий підхід підвищує безпеку та відповідає принципам масштабованості та розподіленості.

Формування засобу криптографічної аутентифікації за допомогою криптоалгоритмів, цифрових підписів, систем PKI та протоколів Authenticated Key Exchange – це шлях до створення надійних, стійких і гнучких механізмів підтвердження особи в сучасних інфосистемах..