УДК 004.415.5
С. Лупенко, Я. Андрійчук
(Тернопільський національний технічний університет імені Івана Пулюя)

РЕАЛІЗАЦІЯ ПРОТОКОЛІВ АУТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ ВЕБ-ОРІЄНТОВАНИХ КОМП'ЮТЕРНИХ СИСТЕМ

Зростання значущості різних веб-сервісів у сучасному світі очевидний: практично всі компанії, починаючи з найдрібніших і закінчуючи найбільшими мають свої сайти в Інтернеті. Безліч підприємств випускає продукцію, так чи інакше, здійснюєють свою діяльність в глобальній мережі. Постійно росте рівень залученості аудиторії в різного роду веб взаємодіях, щоденний час, який проводиться користувачами в мережі збільшується. Разом з цим росте і довіра до веб-ресурсів: збільшується кількість користувачів інтернет-банків і магазинів, користувачі часто розміщують на відповідних ресурсах конфіденційну інформацію різної цінності.

У цьому контексті важливим є вивчення криптографічних методів захисту інформації: різних видів шифрування, створення цифрових підписів і цифрових водяних знаків і т.п.

На даний момент існує велика кількість методів авторизації та аутентифікації користувача: від найпростіших – як введення логіна і пароля, до найскладніших, що включають в себе багатоетапну систему підтвердження аутентичності. Всі вони розрізняються використовуваними протоколами передачі даних, складністю реалізації, вартістю підтримки працездатності системи і т.д.

Серед значної множини протоколів, найбільш актуальними є OpenID (для перевірки облікових даних користувача (identification & authentication)), OAuth (для отримання доступу до даних), OpenID Connect (отримання базової інформації щодо профілю користувача).

Всі три протоколи дозволяють користувачеві не розголошувати свої секретні логін і пароль. Протоколи OpenID та OAuth розроблялися паралельно аж до 2014 року і об'єдналися в результаті в OpenID Connect. OpenID став провідним стандартом для забезпечення єдиного входу та ідентифікації в Інтернеті. Його формула успіху: прості JSON-веб-токени (JWT), що постачаються через потоки OAuth 2.0, призначені для веб-браузерних і мобільних додатків.

OpenID Connect досить простий для інтеграції з основними додатками, але також має функції та параметри безпеки, що відповідають вимогам підприємства.

Яка формула успіху OpenID Connect? Легко вживати ідентифікаційні токени: клієнти отримують ідентифікацію користувача, закодовану в захищеному веб-токені JSON (JWT), називаючи токен ідентифікації. JWT цінується своєю елегантністю і мобільністю, а також їхньою готовою підтримкою для широкого спектру алгоритмів підпису та шифрування. Все це робить JWT найкращим для роботи з ідентифікацією токенів.