АНОТАЦІЯ

У роботі розглянуто алгоритм і уразливості стандарту JSON Web Token. Він є стандартом RFC 7519, відповідальним за створення так званих токенів аутентифікації, що використовує в якості основи формат JSON. Даний стандарт застосовується при передачі аутентифікаційних даних в веб програмах.

Токени мають на меті заміну таких способів аутентифікації, як куки, дозволяючи підвищити рівень безпеки при процедурах авторизації на сайтах та інших платформах. Але ця технологія має декілька вразливостей, які мають корені не тільки в конкретних реалізаціях бібліотек, але й в самому алгоритмі цього стандарта.

Ключові слова: авторизація, аутентифікація, фреймворк, симетричний алгоритм, ключ шифрування, відкритий канал, закритий канал.

Розмір пояснювальної записки – 80 сторінок, 10 зображень, 1 додаток

ABSTRACT

The paper considers the algorithm and vulnerabilities of the JSON Web Token standard. It is an RFC 7519 standard that is responsible for creating so-called authentication tokens that uses the JSON format as the basis. This standard applies to the transmission of authentication data in web applications.

Tokens are intended to replace authentication methods such as cookies, allowing for increased security in authorization procedures on sites and other platforms. But this technology has several vulnerabilities that have roots in not only specific implementations of libraries, but also in the algorithm itself of this standard.

Keywords: Authorization, Authentication, Framework, Symmetric Algorithm, Encryption Key, Open Channel, Closed Channel.

The size of the explanatory note - 80 pages, 10 of images, 1 application