Іщук К. О., здобувач,
Покотило О. А., ст. викладач,
Щур Н. О., ст. викладач
Державний університет «Житомирська політехніка»

ДОСЛІДЖЕННЯ ФУНКЦІОНАЛУ, ЕФЕКТИВНОСТІ ТА БЕЗПЕКИ КРИПТОГРАФІЧНИХ БІБЛІОТЕК У СЕРЕДОВИЩІ JAVASCRIPT

Криптографічні бібліотеки в середовищі JavaScript виступають як ключовий елемент забезпечення безпеки. Вони дозволяють забезпечити захист конфіденційної інформації, такої як паролі, особисті дані, фінансові транзакції, а також допомагають здійснювати безпечну передачу даних через мережу шляхом їх шифрування перед відправкою та розшифрування при отриманні, що унеможливлює перехоплення та злам доступу до них. Актуальність та важливість теми криптографічних бібліотек у JavaScript у сфері безпеки не може бути недооцінена. Вони є необхідними для перевірки цілісності та аутентифікації користувачів, а їх використання зменшує ризик зламу системи або зловживання даними.

Метою даного дослідження є аналіз ключових аспектів основних криптографічних бібліотек в середовищі JavaScript з подальшим порівнянням їх характеристик задля визначення оптимального рішення для використання в практичних розробках.

До найбільш відомих криптографічних бібліотек відносять CryptoJS [1], Forge [2], SJCL (Stanford JavaScript Crypto Library) [3], SubtleCrypto (Web Crypto API) [4], libsodium.js [5]. Результат їх порівняння за основними критеріями наведено в табл.1.

Результати дослідження вищенаведених криптографічних бібліотек демонструють їх основні відмінності. CryptoJS, хоча і підтримує багато алгоритмів, використовує застарілі методи шифрування, що може вплинути на безпеку та ефективність у сучасних сценаріях. Forge і SJCL забезпечують високий рівень безпеки та підтримки сучасних стандартів, проте Forge потребує багатьох ресурсних витрат у зв'язку з великим обсягом, тоді як SJCL може не враховувати деякі новіші розробки в галузі криптографії.

SubtleCrypto, яка вбудована у браузери через Web Crypto API, має високу безпеку та дозволяє використовувати сучасні алгоритми, але її функціонал може бути обмежений залежно від браузеру. libsodium.js виділяється високою безпекою та ефективністю завдяки сучасним алгоритмам та швидкодії, але можуть бути питання по швидкості завантаження веб-додатків.

Таблиця 1

Порівняльна характеристика криптографічних бібліотек у середовищі JavaScript

Критерій	***CryptoJS***	***Forge***	***SJCL***	***SubtleCrypto***	***libsodium.js***
Алгоритми шифрування	*AES, DES, Triple DES, інші*	*AES, DES, Triple DES, інші*	*AES, DES, RC4*	*AES, DES, RSA, інші*	*AES, ChaCha20, інші*
Хеш-функції	*MD5, SHA-1, SHA-256, інші*	*MD5, SHA-1, SHA-256, інші*	*SHA-1, SHA-256*	*SHA-1, SHA-256, інші*	*SHA-256, SHA-512, інші*
Підтримка RSA	+	+	-	+	+
Підтримка ECC	-	+	-	+	+
Web Crypto API сумісність	-	-	-	+	-
Розмір	*Близько 300-400 КВ (зжатий вигляд)*	*Близько 200-300 КВ*	*Близько 100-200 КВ*	*Залежить від браузера*	*Близько 200-300 КВ*
Підтримка / спільнота	*Малоактивна*	*Активна*	*Обмежена*	*Активна*	*Активна*
Ліцензія	*BSD, MIT*	*BSD*	*BSD*	*MIT*	*ISC*
Ефективність	*Середня*	*Висока*	*Середня*	*Висока*	*Висока*
Безпека	*Низька*	*Висока*	*Висока*	*Висока*	*Дуже висока*

Враховуючи отримані результати, визначення оптимального рішення для практичних розробок буде залежати від конкретних потреб. Для веб-додатків, де важлива вбудована підтримка браузерів, кросплатформених платформ, мобільних додатків та інших обмежених середовищ, де важливий обсяг завантаження, кращим вибором буде SubtleCrypto. У випадку розробки додатків, які вимагають високого рівня безпеки, доцільно зупинити вибір на libsodium.js або SJCL.

Використання криптографічних бібліотек у JavaScript є важливим кроком для забезпечення безпеки в інтернет-просторі, і їхня правильна інтеграція є важливою частиною розробки безпечних та надійних веб-застосунків.

Список використаної літератури

1. CryptoJS. URL: https://cryptojs.gitbook.io/docs/
2. Forge. GitHub Pages. URL: https://digitalbazaar.github.io/forge/
3. Stanford Javascript Crypto Library (SJCL). URL: https://crypto.stanford.edu/sjcl/
4. Web Crypto API – Web APIs. URL: https://developer.mozilla.org/en-US/docs/Web/API
5. Libsodium documentation: Introduction. URL: https://libsodium.gitbook.io/doc/