

ВИКОРИСТАННЯ ПОСТКВАНТОВОЇ КРИПТОГРАФІЇ В СУЧАСНИХ ВЕБ-ЗАСТОСУНКАХ

Зі швидким розвитком квантових обчислень постає проблема безпеки сучасних криптографічних алгоритмів, які використовуються для захисту даних у веб-застосунках. Традиційні алгоритми, такі як RSA та ECC (еліптичні криві), можуть бути скомпрометовані квантовими комп'ютерами, які мають здатність розв'язувати задачі факторизації та дискретного логарифмування за допомогою алгоритму Шора. У зв'язку з цим, веб-застосунки, які обробляють конфіденційну інформацію, повинні впроваджувати постквантові криптографічні алгоритми, що базуються на задачах, стійких до атак квантових комп'ютерів (наприклад, криптографія на основі решіток, кодів або багатозмінних поліномів). Тому, тема є актуальною [1].

Для забезпечення безпеки веб-застосунків у постквантову еру необхідно адаптувати сучасні криптографічні протоколи, такі як TLS/SSL, до використання постквантових алгоритмів. Це включає оновлення стандартів шифрування, підписів та обміну ключами. Наприклад, NIST вже проводить конкурс на стандартизацію постквантових алгоритмів, і веб-розробники повинні готуватися до їх впровадження [2].

Попри значний потенціал постквантових алгоритмів, їх впровадження в реальні веб-застосунки зіштовхується з низкою технічних та практичних труднощів. Це включає питання сумісності з існуючими інфраструктурами, такими як сервери та клієнтські браузеры, необхідність оптимізації обчислювальних витрат для великих даних і забезпечення зворотної сумісності з уже використовуваними алгоритмами. Інтеграція нових алгоритмів у протоколи безпеки, такі як TLS 1.3, вимагає значних змін у протоколах обміну ключами та їх обробці [3].

Незважаючи на те, що квантові комп'ютери поки що не здатні здійснювати реальні атаки на криптографічні системи, підготовка до цієї ери вже є необхідною. Впровадження постквантових алгоритмів на етапі еволюції технологій дозволить забезпечити безпеку веб-застосунків у майбутньому. Перехід до таких систем має бути плавним і стратегічно продуманим, щоб уникнути перерв у функціонуванні критично важливих веб-систем та інфраструктур.

Для плавного переходу до постквантової криптографії рекомендується використовувати гібридні підходи, які поєднують традиційні та постквантові

алгоритми. Це дозволяє забезпечити сумісність з існуючими системами та захистити дані від потенційних атак як з боку класичних, так і квантових комп'ютерів. Наприклад, гібридні схеми TLS можуть включати як RSA, так і постквантові алгоритми обміну ключами.

Висновок. Деякі компанії вже почали експериментувати з постквантовими алгоритмами. Наприклад, Google тестувала постквантові алгоритми в Chrome, а Cloudflare інтегрувала їх у свої сервіси. Ці приклади демонструють, що перехід до постквантової криптографії є реальним і досяжним [4].

У майбутньому очікується широке впровадження постквантових алгоритмів у веб-застосунки, особливо в галузях, де конфіденційність і цілісність даних є критично важливими. Це включає фінансові транзакції, електронний уряд, IoT та інші сфери. Розвиток квантових технологій також стимулюватиме подальші дослідження в галузі постквантової криптографії.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. An overview of post-quantum threats to proof-of-work cryptocurrencies. [Electronic resource]. – Access mode: <https://cointelegraph.com/learn/articles/post-quantum-threats-to-proof-of-work-cryptocurrencies>
2. Post-Quantum Cryptography [Electronic resource]. – Access mode: <https://csrc.nist.gov/projects/post-quantum-cryptography>.
3. Why use TLS 1.3? [Electronic resource]. – Access mode: <https://www.cloudflare.com/learning/ssl/why-use-tls-1.3/>.
4. How to Configure Post-Quantum Cryptography in Your Web Server [Electronic resource]. – Access mode: <https://medium.com/be-tech-with-santander/how-to-configure-post-quantum-cryptography-in-your-web-server-fcf79e05e526>.