СУЧАСНІ ПРОБЛЕМИ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

Лук’янов М.Ю.
Харківський національний університет радіоелектроніки, м. Харків

Великі обсяги інформації в Інтернеті збільшують відповідальність за роботу усіх систем, які мають контакт з мережею. Багато людей намагаються викрасти інформацію та використати її задля своїх цілей. Саме цьому потрібно більше приділяти уваги захисту даних.

Є багато алгоритмів які дозволяють шифрувати дані. Серед них виділяють симетричні та асиметричні, от деякі приклади з них: DES, RSA, BIP 0032 та інші. Але немає системи яка мала б змогу надавати ієрархічний доступ до даних згідно ієрархічного ключа. Тому можна запропонувати систему, яка матиме можливість збереження закодованих даних у базі та надавати ієрархічний доступ до них. Також система надаватиме захист від найбільш відомих атак, такі як OWASP, Injections, XSS, CSRF, Broken Authentication and Session Management, Security Misconfigurations, Missing Function Level Access Control. Сама система буде складатися з таких компонентів: база даних, серверна та веб частина.

Зважаючи на те, що люди не мають довіри до системи було вирішено покласти завдання шифрування та дешифрування на веб-частину. Це дає декілька переваг. Перш за все, система не зберігає ключі. Як було зазначено вище, будь-який програмний засіб захисту в деякий час буде скомпроментовано і зловмисник може отримати доступ до системи. Якщо зберігати ключі в системі, то зловмисник зможе отримати доступ до усіх ключів. Тоді уся система перестане бути захищеною і всі дані будуть відомі. Насамперед, ключі зберігають самі користувачі. Таким чином, якщо систему буде скомпроментовано, то зловмисник не зможе розшифрувати дані. Також усі дані шифруються та дешифруються у веб-частині. Це дозволяє системі обмінюватися тільки зашифрованими даними з серверною частиною. Алгоритм ієрархічних ключів є основною частиною системи. Його слід реалізовати на JavaScript, зважаючи на те, що алгоритм повинен працювати у веб-частині всередині браузера користувача. Для реалізації алгоритму була використана низка відкритих бібліотек як то bitcoin.js, crypto.js, sha256.js, sha512.js, тощо.

Таким чином був спроєктований програмний продукт для отримання та збереження даних з ієрархічним доступом з інтуїтивно-зрозумілим інтерфейсом. Практична значимість системи обумовлена підвищенням ефективності захисту збереженої інформації у світі, де найбільшою цінністю є саме інформація.