

УДК 04.056.5

Козіна Г. Л.¹, Ребриков М. М.²

¹ канд. фіз.-мат. наук, доц. НУ «Запорізька політехніка»

² студ. гр. РТ-812м НУ «Запорізька політехніка»

РОЗРОБКА ЗАХИЩЕНОГО СЕРВІСУ ОБМІНУ ФАЙЛАМИ З ВИКОРИСТАННЯМ УКРАЇНСЬКИХ НАЦІОНАЛЬНИХ СТАНДАРТІВ

Захист інформації є однією з найбільш актуальних проблем у сучасному світі, де вірогідність кібератак і порушень безпеки інформації щодня зростає. Найчастіше метою таких несанкціонованих дій є незаконне заволодіння конфіденційною інформацією. Один з ефективних способів захисту конфіденційної інформації – це використання захищених сервісів обміну файлами.

Важливою частиною будь-якого захищеного сервісу є використання криптографічних перетворень. Україна має власні національні стандарти забезпечення конфіденційності та цілісності інформації, які необхідно враховувати при розробці захищеного сервісу обміну файлами. У цьому контексті, розробка захищеного сервісу обміну файлами з використанням українських національних стандартів є важливою темою, яка заслуговує на увагу.

Для розробки захищеного сервісу обміну файлами з використанням українських національних стандартів необхідно враховувати наступні вимоги: захист від несанкціонованого доступу до файлів; конфіденційність обміну файлами між користувачами; захист від шкідливих програм; захист від несанкціонованого копіювання та передачі файлів.

Проектування захищеного сервісу обміну файлами з використанням українських національних стандартів потребує ретельного аналізу вимог до захисту інформації, а також розробки відповідної архітектури та інфраструктури. Однією з ключових складових проектування буде розробка алгоритмів шифрування та дешифрування файлів, які використовують українські національні стандарти забезпечення безпеки інформації. Запропоновано використання наступних національних стандартів:

ДСТУ 7564:2014 «Інформаційні технології. Криптографічний захист інформації. Функція гешування» (Стандарт набрав чинності з 1 квітня 2015 року наказом Мінекономрозвитку від 2 грудня 2014 року №1431)

ДСТУ 7624:2014 «Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення» (Стандарт набрав чинності з 1 липня 2015 року наказом Мінекономрозвитку від 2 грудня 2014 року №1484)

ДСТУ 4145-2002 «Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка» (Стандарт набрав чинності з 1 липня 2003 року наказом Держспоживстандарту від 28 грудня 2002 року №31)

Використання даних державних стандартів України запропоновано згідно наказу Мінцифри від 30 жовтня 2020 року №140/614. У цьому наказі зазначено, що після 1 січня 2021 року ДСТУ 4145-2002 повинен використовуватися для створення кваліфікованого електронного підпису та для перевірки кваліфікованого електронного підпису разом з функцією гешування Купина (ДСТУ 7564:2014).

Однією з можливих архітектур для розробки захищеного сервісу обміну файлами є клієнт-серверна архітектура. У цій архітектурі система розділяється на дві основні складові - клієнтську і серверну.

Реалізація клієнтської складової запропонована у вигляді web-додатку. При розробці запропоновано використання мови програмування TypeScript та наступних бібліотек: React, Zustand, ReactQuery, MaterialUI.

Серверна складова включає програму, яка забезпечує основні функції сервісу, такі як обробка запитів користувачів, збереження файлів, аутентифікація користувачів та інше. Дана серверна програма може бути розміщена на фізичних серверах, що належать компанії, яка розробляє/використовує сервіс, або на віддалених серверах з використанням послуг хмарних провайдерів.

У клієнт-серверній архітектурі, комунікація між клієнтською і серверною складовими здійснюється за допомогою мережевих протоколів, таких як TCP/IP або HTTP/HTTPS. Клієнтська складова здійснює запити до серверної складової, яка обробляє запити і повертає результати до клієнтської складової.

Як подальший розвиток даного сервісу передбачено використання розподіленої децентралізованої архітектури, а саме peer-to-peer (p2p). В мережі p2p не існує поняття клієнтів або серверів, лише рівні вузли, які одночасно функціонують як клієнти та сервери по відношенню до інших вузлів мережі. Дана архітектура має багато переваг, серед яких: зменшення вартості системи; вдосконалена масштабованість/надійність; більш висока приватність (анонімність/конфіденційність) та безпека.

У висновку можна сказати, що розробка захищеного сервісу обміну файлами з використанням українських національних стандартів є важливою задачею з точки зору безпеки та конфіденційності інформації. Клієнт-серверна архітектура дозволяє забезпечити більш високу безпеку даних, оскільки сервер контролює доступ до файлів і може захистити їх від несанкціонованого доступу. Однак, технологія peer-to-peer також має свої переваги, зокрема відсутність одного центрального серверу, що робить її менш залежною від атак на централізовані системи.

Розробка захищеного сервісу обміну файлами з використанням українських національних стандартів може стати важливим кроком для забезпечення безпеки та конфіденційності даних в Україні. Важливо розробляти системи з урахуванням національних стандартів, оскільки це забезпечує сумісність з існуючими системами та допомагає зменшити ризик некоректної роботи через відмінності в стандартах. Захист даних є важливим аспектом сучасного життя, тому розробка захищених сервісів є важливим завданням для інформаційної безпеки.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Kuryna Hash Function. DSTU 7564:2014 [Електронний ресурс]. Режим доступу до ресурсу: <https://shorturl.at/myGY7> – Назва з екрана.
2. Kalyna Block Cipher Function. DSTU 7624:2014 [Електронний ресурс]. Режим доступу до ресурсу: <https://shorturl.at/dsNPR> – Назва з екрана.
3. Digital Signature. DSTU 7564:2014 [Електронний ресурс]. <https://shorturl.at/QWY18> – Назва з екрана.