УДК 681.3

В. В. Войтко
В. Д. Шиндирук

РОЗРОБКА ВЕБПЛАТФОРМИ З ПОСТКВАНТОВИМ ШИФРУВАННЯМ ТА СИСТЕМОЮ ВИЯВЛЕННЯ АНОМАЛІЙ У ПОВЕДІНЦІ

Вінницький національний технічний університет

Анотація

У статті описується розробка вебплатформи «Quantum information science» для шифрування корпоративних документів за допомогою постквантових алгоритмів та квантового розподілу ключів. Показано роботу безпечної клієнт-серверної архітектури та подано квантову модель машинного навчання, стійку до квантових атак.

Ключові слова: *постквантове шифрування, вебплатформа, квантове машинне навчання, розподіл ключів, виявлення аномалій.*

Abstract

The article presents the development of the "Quantum Information Science" web platform for encrypting corporate documents using post-quantum algorithms and quantum key distribution. It demonstrates the operation of a secure client-server architecture and introduces a quantum machine learning model resistant to quantum attacks.

Keywords: *post-quantum encryption, web platform, quantum machine learning, key distribution, anomaly detection*

Вступ

Швидка інтеграція квантової теорії у наше життя стала однією з вагомих причин, щоб звернути увагу на безпеку корпоративних даних у документах. Державні та медичні установи, малий, середній та великий бізнес, військові структури можуть бути під загрозою у зв'язку з посиленням інтересу науковців до створення квантового комп'ютера, який, у свою чергу, може допомогти отримати конфіденційні дані з корпоративних сховищ за допомогою розшифрування захисних ключів передбачуваними способами.

На сьогоднішній день компанія IBM розробила квантовий комп'ютер [1], який здатний виконувати складніші розрахунки, проте ця система може використовуватися лише для існуючої кількості операцій, у зв'язку з існуванням ефекту спостерігача, опираючись на Копенгагенську інтерпретацію квантової механіки [2].

Головний напрямок розвитку квантових технологій полягає у можливості значного прискорення обчислювальних операцій над складними математичними завданнями, що потребують обробки надмасштабних для людської свідомості кількості обчислювальних даних.

Метою роботи є підвищення можливостей захисту даних і забезпечення непроникності у доступ до корпоративних систем великих бізнес установ в умовах стрімкого розвитку квантової механіки, що допоможе унеможливити зловмисницькі дії щодо отримання доступу до секретних даних.

Розроблена вебплатформа дозволить користувачам завантажувати файли, захищені постквантовим алгоритмом, також розміщувати їх у групі та сховищі вебпродукту. Додатково вона надасть можливість розпізнавати рукописний текст на фото та конвертувати його як друкований текст у файл, захищений ключом шифруванням.

Розроблена система наділена можливістю розпізнавати аномалії поведінки користувачів платформи за допомогою квантової моделі машинного навчання.

Об'єктом дослідження є процес розробки продукту для захисту документів бізнесу постквантовими алгоритмами шифрування, повністю захищених від атак зловмисників.

Предметом дослідження є методи та засоби реалізації вебплатформи для комфортної роботи з захищеними документами.

Головною задачею є створення вебресурсу, який дозволить користувачам захищати та зберігати важливі файли зі стійкими ключами до квантових атак.

Розробка клієнт-серверної вебсистеми для шифруванням ключа

Питання постквантової захищеності поступово набуває актуальності при розробці вебплатформ для користувачів усіх типів корпоративних бізнесів, що містять засекречені дані, дослідження, річні стратегічні плани, обрахунки та витрати на закупівлю чи продаж, які не повинні ніяким чином потрапити до рук зловмисників. Найбільш актуальним сьогодні є квантове розподілення ключів між користувачами системи. Це допомагає колегам обмінюватися ключами без будь-яких можливих способів втручання в процес комунікації. Якщо відбудеться спроба перехоплення квантового сигналу, відповідні зміни будуть у двох користувачів, що дасть їм змогу зрозуміти, що відбулася спроба несанкціонованого доступу до файлу.

На рисунку 1 наведено діаграму, що ілюструє взаємодію клієнта і сервера у передачі ключа з метою шифрування файлу.

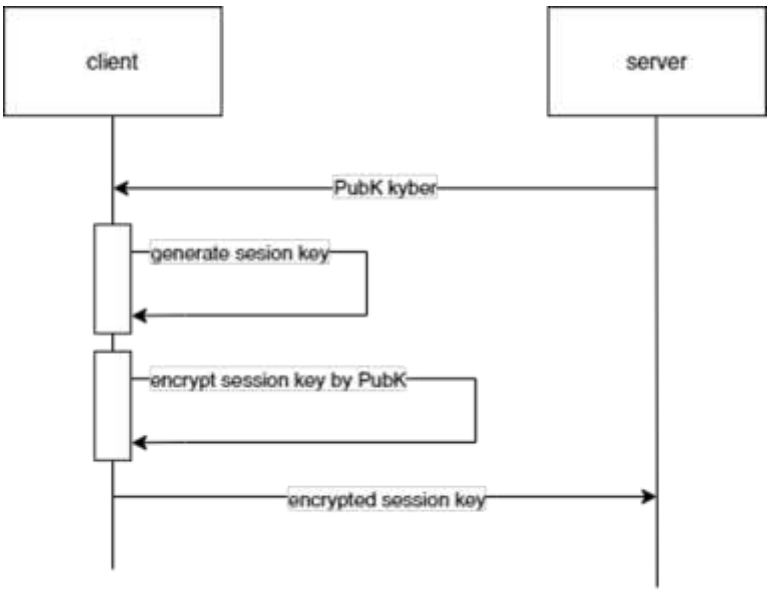

Рис.1. UML діаграма застосування взаємодії клієнта і сервера для передачі ключа, захищеного постквантовим алгоритмом шифрування

Ця архітектура гарантує безпечний обмін криптографічними ключами між клієнтом і сервером за допомогою постквантового алгоритму. Як ілюструє UML-діаграма, користувач розпочинає запит на шифрування документа. Сервер створює унікальний ключ, стійкий до квантових атак, і пересилає його клієнту через безпечний канал. Після цього клієнт проводить локальне шифрування файлу і відправляє його на сервер для зберігання. Якщо відбувається спроба втручання або перехоплення сигналу на будь-якому етапі, система реєструє зміну квантового стану, що попереджає обидві сторони про потенційну загрозу. Цей механізм втілює основні принципи квантового розподілу ключів, до прикладу, перевірку цілісності каналу через аналіз змін поляризації фотонів або станів кубітів у змодельованому середовищі.

Розробка квантової моделі машинного навчання для виявлення аномальної поведінки користувачів на вебплатформі

На сьогоднішній день існує генеративна змагальна мережа [3], яка була взята за основу для розробки квантової моделі виявлення спроби пошкодження сигналів передачі ключа між користувачами системи. Основна логіка її роботи полягає у взаємодії між генератором та дискримінатором, головна задача якого спрямована на можливість розрізняти подані сигнали як звичайні чи аномальні. При навчанні дискримінатор стає кращим у розпізнаванні атак, а генератор покращує свою роботу при спробі обманути його.

Щоб виявити аномальну поведінку, потрібні тести, результати яких вводяться в розроблену і навчену квантову машинну модель. Потім ступінь загрози виявленої поведінки оцінюється мережею виявлення та оцінки поведінки для того, щоб оцінити безпеку поведінки користувача. Розроблена програма має за основу квантово-генеративну змагальну мережу. На її основі було створено архітектуру квантової

моделі машинного навчання, яка має здатність визначати рівень аномальних сигналів на вебплатформі за допомогою навченого дешифратора у квантовій суперпозиції, що проілюстровано на рисунку 2.

Розроблена архітектура моделі базується на заданих квантових вентилях. Їх головна ціль – бути квантовою операцією, яка створить квантову заплутаність між кубітами. Кожен шар складається з вентилів типу Pauli-Y, які виконують обертання за допомогою операції $RY(\theta_{ij})$, де θ_{ij} — це кут обертання для і-го кубіта в j-му шарі, а Z – це контролюючі вентилі.

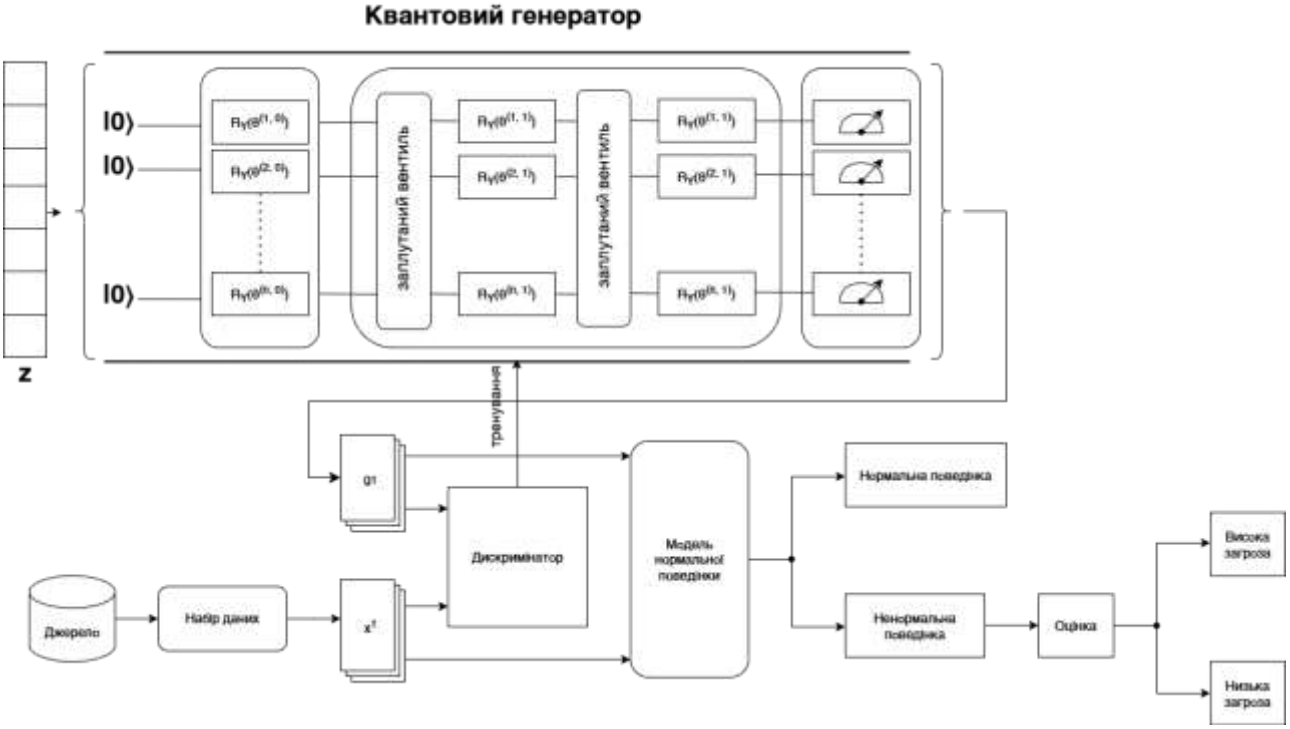

Рис.2. Архітектура роботи квантової моделі машинного навчання для виявлення аномальних сигналів

У результаті виявлення незвичайного сигналу програма за поданою схемою ідентифікуватиме рівень втручання як високий чи низький. Відслідковувати сигнали можна буде цілодобово. Графіки наочно ілюструватимуть ідентифіковані стани й вказуватимуть, чи входить визначений рівень втручання у допустимі межі.

Висновок

Розроблено вебплатформу на основі постквантової криптографії. Створено архітектуру, яка враховує можливі збої у передачі сигналів, оцінює їх рівень та забезпечує безпечний обмін ключами шифрування на основі клієнт-серверної архітектури. Розроблена квантова модель машинного навчання для аналізу поведінкових аномалій користувачів дає змогу виявляти потенційні квантові загрози і розуміти, як з ними боротися, враховуючи можливість отримання більшої кількості даних про зловмисника.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Компанія IBM розробила найпотужніший квантовий комп'ютер [Електронний ресурс] – Режим доступу до ресурсу: https://nachasi.com/news/2017/11/13/ibm-rozrobyla-najpotuzhnishyj-v-sviti-kvantovyj-kompyuter/
2. Копенгагенська інтерпретація квантової механіки: ключ до розуміння суперпозиції [Електронний ресурс] – Режим доступу до ресурсу: https://www.fizykaua.com/post/kopengag-enska-interpretatsiya-kvantovoyi-mehaniky
3. Типи генеративних нейронних мереж [Електронний ресурс] – Режим доступу до ресурсу: https://www.tech.vernadskyjournals.in.ua/journals/2021/1_2021/part_1/19.pdf

Войтко Вікторія Володимирівна – кандидат технічних наук, доцент кафедри програмного забезпечення, Вінницький національний технічний університет, м. Вінниця, e-mail: dekanfki@i.ua

Шиндирук Вікторія Дмитрівна – студентка групи 1ПІ-21б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: svikaa1998@gmail.com

Viktoriia Voitko – Ph.D., Associate Professor of Software Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: dekanfki@i.ua.

Viktoriia Shyndyruk – student of group 1PI-21b, Faculty for Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: svikaa1998@gmail.com