```
# Створення даних
df <- data.frame(x = rnorm(100), y = rnorm(100))
# Створення графіка розсіювання з ggplot2
ggplot(df, aes(x = x, y = y)) + geom_point() + ggtitle("Графік розсіювання") + xlab("X") + ylab("Y")
```

3. *За допомогою бібліотеки Plotly.* Plotly є пакетом для створення інтерактивних графіків у R. Цей пакет дозволяє створювати графіки, які можна змінювати, переглядати та зберігати в різних форматах. Нижче наведено код для створення інтерактивного графіка розсіювання з використанням Plotly:

```
# Завантаження пакету Plotly
library(plotly)
# Створення даних
df <- data.frame(x = rnorm(100), y = rnorm(100))
# Створення інтерактивного графіка розсіювання з Plotly
plot_ly(df, x = ~x, y = ~y, type = "scatter", mode = "markers") %>%
  layout(title = "Інтерактивний графік розсіювання", xaxis = list(title = "X"), yaxis = list(title = "Y"))
```

Візуалізація даних є важливою частиною аналізу даних та дозволяє легше зрозуміти взаємозв'язки між даними. Мова R забезпечує розширені можливості для візуалізації даних, зокрема наявність різноманітних графіків та пакетів для візуалізації. Це дозволяє дослідникам та аналітикам створювати якісні та ефективні графіки для представлення результатів аналізу даних.

Список літератури:

1. *" R (мова програмування)", URL: http://surl.li/ecqdz*
2. *Д.О. Павленко, «Аналіз даних за допомогою мови R», Житомирський державний технологічний університет, 2017 р.*

УДК 004.056

Радзіховська А.О., студентка 3 курсу спеціальності 122 «Комп'ютерні науки»
Січко Т. В., к.т.н., доцент кафедри інформаційних технологій

КВАНТОВІ ОБЧИСЛЕННЯ ТА ЇХ РОЛЬ У ГАЛУЗІ КІБЕРБЕЗПЕКИ

Донецький національний університет імені Василя Стуса, м. Вінниця

Вимоги до кібербезпеки для організацій критичної інфраструктури або інших підприємств з конкретними доменами є доволі високими. Промислово розвинені країни забезпечують жорсткий контроль кібербезпеки для установ з фінансових, медичних та оборонних галузей. Більш поширеними стають

теоретичні або практичні моделі, які підтримують процес оцінки позиції щодо кібербезпеки, а також дотримання національних або організаційних елементів контролю. Використання моделей може бути обумовлене рядом факторів, починаючи від національних правил, економічних переваг, аж до аспектів ефективності та стандартизації. З практичної точки зору набагато ефективніше використовувати публічно перевірену модель, розроблену, а не розробляти індивідуально нову модель. Більш того існує багато останніх розробок в галузі кібербезпеки за допомогою нових алгоритмів, процедур і фреймворків [1].

Світ рухається до нового етапу безпеки за допомогою асиметричних схем, які обіцяють забезпечити захищеність та конфедеційність даних у цифровому просторі. Розвиток квантових обчислень все більш набирає обертів. Результати цього розвитку мають наслідки і для для кібербезпеки, адже ця технологія має потенціал для експоненціального підвищення обчислювальної потужності комп'ютерів. Квантові обчислення можуть швидше обробляти інформацію за допомогою кубітів, які можуть представити кілька значень одночасно, і тому вони здатні вирішувати складні проблеми більш ефективно, ніж традиційні комп'ютери. Однак підвищення обчислювальної потужності квантових комп'ютерів також передбачає більший ризик порушення безпеки, зокрема, можливості зламування існуючих протоколів шифрування. Це може призвести до серйозних наслідків для безпеки персональних даних та національної безпеки [2].

Квантовий розподіл ключа - метод передачі ключа, який використовує квантові явища для гарантії безпечної зв'язку. Цей метод дозволяє двом сторонам, з'єднаним з відкритого каналу зв'язку, створити загальний випадковий ключ, який відомий тільки їм, і використовувати його для шифрування і розшифрування повідомлень. Важливою і унікальною властивістю квантового розподілу ключа є можливість виявити присутність третьої сторони, яка намагається отримати інформацію про ключ. Тут використовується фундаментальний аспект квантової механіки: процес виміру квантової системи порушує її. Третя сторона, яка намагається отримати ключ, повинна виміряти надіслані через з'єднання квантові стани, що веде до їх зміни і появи аномалії. За допомогою квантової суперпозиції, квантової заплутаності і передачі даних в квантових станах можна здійснити канал зв'язку, який виявляє аномалії. Якщо кількість аномалій нижче певного порогу, то буде створено, ключ що гарантує безпеку (третя сторона не має інформації про це), інакше секретний ключ не буде створено і зв'язок припиняється [3].

Квантовий розподіл ключів (QKD), замість того, щоб покладатися на поняття математики, базується на законах квантової фізики для створення симетричного ключа. Перший практичний протокол QKD, в якому дві сторони спілкуються за допомогою класичних і квантових каналів зв'язку. Класичний канал дозволяє окремим бітам інформації проходити через канал.

Протокол розповсюдження квантового ключа безпечний, якщо він правильний і секретний. Правильність - це твердження, якщо одна сторона та інша мають один і той самий рядок бітів, а самий секретний ключ у кінці

протоколу. Секретність - це твердження про те, що людина, яка хоче “підслухати” інформацію не знає остаточного ключа [4].

У сучасному світі квантові технології можуть змінити все, починаючи від способу розрахунку складних математичних завдань і завершуючи зміни у сфері безпеки та захисту інформації. Однак, можливість зламування квантовими комп'ютерами існуючих протоколів шифрування може мати серйозні наслідки для безпеки персональних даних та національної безпеки в цілому. Тому, разом із розвитком квантових технологій, важливо продовжувати розробляти нові методи захисту інформації від квантових атак.

Список літератури:

1. *Рогожук Н.В., Січко Т.В. Передача даних небезпечним каналом зв’язку, з використанням шифрування відкритим ключем. Прикладні інформаційні технології: матеріали всеукр. наук.-практ. конф., м. Вінниця, 2020. С. 88-90.*
2. *Квантові обчислення та кібербезпека: загрози та рішення: веб-сайт. URL: http://surl.li/gvqgx (дата: 04.04.2023).*
3. *Хорунжий О. Є. Аналіз видів та способів генерації квантових та таємних ключів. Магістрерська робота, Київський національний політехнічний університет ім. Ігоря Сікорського, Київ, 2018р, ст.14.*
4. *Квантовий розподіл ключів: веб-сайт. URL: https://wiki.veriqloud.fr/index.php?title=Quantum_Key_Distribution (дата: 21.12.2020)*

УДК 004.01

Рудкевич Б. М., студент 3 курсу спеціальності 122 «Комп’ютерні науки»
Хмелівський Ю.С., асистент кафедри інформаційних технологій

ВІЗУАЛІЗАЦІЯ ТА АНАЛІЗ ДАНИХ МІГРАЦІЇ РОБОЧОЇ СИЛИ В УКРАЇНІ

Донецький національний університет імені Василя Стуса, м. Вінниця

Сьогодні, в період повномасштабної війни в Україні, багато людей попри основну проблему вторгнення, переймаються також проблемою безробіття, з часом ця проблема тільки загострюється, адже люди витрачають власні заощадження аби мати змогу жити в цей непростий час. На основі цієї проблеми спробуємо провести невелике дослідження мігрантів які виїжджають за кордон задля достойного заробітку, і хорошого фінансового старту в майбутньому.

Розглянемо дані виїзду за кордон робочої сили впродовж 2010-2021 років.