3. Багатофункціональний пошуковий прилад ANDRE [Електронний ресурс] – Режим доступу до ресурсу: https://www.das-ua.com/ru/katalog/obladnannya-dlya-viyavlennya-kanaliv-vitoku-informacii/mnogofunkcionalnyj-poiskovyj-pribor-andre/.

4. Виявлення прихованих камер електромагнітним шукачем відеокамер. [Електронний ресурс] – Режим доступу до ресурсу: https://studfile.net/preview/5725661/page:14/.

УДК 004.056.55

Кузнецова А. М., здобувачка вищої освіти гр.КБ-181
Науковий керівник: **Семендяй С. М.**, викладач
Національний університет «Чернігівська політехніка»

КВАНТОВА КРИПТОГРАФІЯ

Інформація в сучасному світі є найціннішим товаром, тому завдання, що стоять перед шифрувальником - забезпечення її конфіденційності, цілісності і невідстежуванності, актуальні як ніколи. Можна сказати, що зараз завдяки розвитку класичної криптографії (зокрема, поширення стійких схем шифрування і цифрового підпису з використанням відкритого ключа) ці завдання виконуються цілком успішно.

Однак будь-який шифр коли-небудь зламується. У наш час найбільш суттєвою загрозою класичної криптографії є використання принципів квантової механіки в обчисленнях.

Квантова механіка, з одного боку, погрожує розкриттям ключових класичних шифрів, проте з іншого - дає можливість створювати принципово нові і потенційно абсолютно надійні криптографічні системи.

Квантова криптографія вивчає можливість генерації криптографічних ключів, секретність яких гарантується фундаментальними законами квантової механіки. Становлення квантової криптографії як науки почалося в 1984 року з розробки першого квантового протоколу розподілу ключів BB84. За ним інформація передається за допомогою кодування станів фотонів на передавальному кінці і подальшому їх вимірі на приймальному. У разі якщо порушник спробує вклинитися в канал між легітимними абонентами і перехопити передані фотони, то відповідно до принципу невизначеності Гейзенберга легітимні абоненти зможуть визначити факт такого вторгнення через різке збільшення числа помилок при реєстрації фотонів. Важливим є находження точної величини критичної помилки для протоколу BB84, яка є рівною приблизно 11%.

Отже, головною перевагою криптографічних протоколів є те, що зловмисник може володіти необмеженими можливостями для перехоплення ключової інформації, проте факт прослуховування каналу завжди залишиться поміченим. Це робить використання квантової криптографії привабливим для боротьби зі шпигунством і шахрайством.

Актуальністю використання та розвитку квантової криптографії є можливість протистояти квантовому комп’ютеру в захисті цифрової інформації від злому.

Через надзвичайно широку поширеність алгоритму RSA одним з найважливіших припущень криптографії є складність завдання факторизації великих чисел. І дійсно, до сьогодення не було знайдено алгоритму, досить швидко вирішує цю задачу. Однак у 1994 році був запропоновано алгоритм з поліноміальною складністю, вирішуючий це завдання на квантовому комп'ютері. Головна причина подібного феноменального прискорення - можливість використання так званого "квантового паралелізму" для проведення швидкого перетворення Фур'є, на якому засновані найбільш ефективні з відомих алгоритмів факторизації. Знаходження цього алгоритму дозволяє звести задачу факторизації до технологічної задачі побудови квантового комп'ютера: якщо його вдасться побудувати, схема шифрування RSA виявиться ненадійною. Це ставить можливості шифрування з відкритим ключем під велику загрозу.

Над створенням повноцінного квантового комп'ютера працюють десятки вчених і технологічних компаній - від Google в США до Alibaba в Китаї. Такий пристрій, що використовує явища квантової механіки для передачі і обробки даних, буде набагато більш ефективним, ніж найпотужніші існуючі комп'ютери. Причому настільки, що зможе зламувати найнадійнішу на даному етапі захист цифрової інформації. Єдиний варіант порятунку комерційних і державних таємниць від квантового комп'ютера - це захист їх за допомогою квантового шифрування.

Китай вже вклав десятки мільйонів доларів у будівництво мереж, які здатні передавати дані за допомогою квантового шифрування. У 2017 році китайський космічний супутник «Мо-цзи» дозволив здійснити відеодзвінок між Пекіном і Віднем за допомогою квантового шифрування. Крім того, була запущена квантова комунікаційна мережа між Пекіном і Шанхаєм. Правда, на даному етапі квантове шифрування може використовуватися лише на обмежені відстані. У випадку з відеозв'язком між Пекіном і Віднем був поставлений рекорд - 7450 км. На землі при використанні оптоволоконних мереж максимальна відстань становить 240 км.

В США каліфорнійський стартап Qubitekk розробляє квантовий захист для енергомереж в Теннессі. Інший стартап - Quantum Xchange - створює мережу квантового шифрування на північному сході США. Ще один аналогічний стартап створюється на базі університету штату Нью-Йорк в Стоуні-Брук.

Нещодавно QRate оновила світовий рекорд в ефективності алгоритмів класичної постобработки в системах квантової криптографії та повідомила, що 17 лютого 2021 р. російські вчені скоротили частку ключа, що витрачається на аутентифікацію класичних даних до 1%, а також запропонували алгоритм корекції помилок на основі полярних кодів. Поліпшення алгоритмів класичної постобработки призведе до збільшення швидкості генерації ключів і зниження вартості інтеграції обладнання в майбутньому.

Отже, інформаційна безпека - одна з ключових потреб суспільства. При розробці технологій для захисту даних ми повинні брати до уваги не тільки існуючі, але і майбутні загрози. Квантова криптографія перспективна, в першу чергу, для захисту каналів зв'язку, по яких передається цінна стратегічна інформація. Особливо якщо мова йде про дані з тривалим терміном зберігання або переговорах топ-менеджменту. У міру розвитку цифровізації суспільства будуть з'являтися додаткові сценарії застосування обладнання для квантового розподілу ключів, наприклад захист безпілотного транспорту від масового злому. При цьому відбувається постійне вдосконалення - наукові розробки дозволяють поліпшувати продукти та технології.

Список використаних джерел

1. http://lib.itsec.ru/articles2/crypto/kvantovaya-kriptografiya-chto-novogo
2. https://www.connect-wit.ru/novosti-kriptografii-novye-zadachi-i-novye-metody-peredovyh-napravlenij.html
3. https://www.tbforum.ru/blog/kvantovaya-kriptografiya-uzhe-segodnya-ili-poka-tolko-zavtra
4. http://sqi.cs.msu.ru/store/storage/ss8dw5n_quantum_cryptography.pdf
5. https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9A%D0%B2%D0%B0%D0%BD%D1%82%D0%BE%D0%B2%D0%B0%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F_(%D1%88%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5)