

сучасних технологічних принципах, та з інтерфейсним модулем з конверторами до існуючих корпоративних баз даних при частковій модернізації останніх.

Вибір конкретного варіанту реалізації залежить від трудомісткості його реалізації та фінансових витрат. При цьому слід мати на увазі, що розробка відповідного конвертора, його налаштування та подальший супровід може коштувати порівняно з витратами на розробку самої БД (як, наприклад, для системи І2).

УДК 004.94

ЮРІЙ ВАЛЕРІЙОВИЧ ГНУСОВ

кандидат технічних наук, доцент, завідувач кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

СЕРГІЙ ВОЛОДИМИРОВИЧ КАЛЯКІН

викладач кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

ПЕРСПЕКТИВИ РОЗВИТКУ КВАНТОВИХ ТЕХНОЛОГІЙ

У сучасному суспільстві основним технічним засобом технології переробки інформації служить персональний комп'ютер, який істотно вплинув як на концепцію побудови і використання технологічних процесів, так і на якість отриманої інформації.

Деякі задачі сучасної науки потребують для вирішення великої кількості комп'ютерного часу, тому Візнер і Фейнман висловили ідею побудови квантового комп'ютера.

Квантовий комп'ютер використовує для обчислення не звичайні (класичні) алгоритми, а процеси квантової природи, так звані квантові алгоритми. В основі квантового комп'ютеру лежить кубіт, який може перебувати одночасно в стані 0 і 1. При класичному вимірі 0 або 1 випадуть з певною ймовірністю, а наприклад, система з п'яти кубітів буває одночасно в 32 станах. Квантові обчислення маніпулюють усіма ними відразу, що призводить до значного підвищення швидкодії.

У 2017 році корпорація ІВМ відкрила власні хмарні сервери для всіх бажаючих попрацювати з квантовими алгоритмами. Спочатку це були пятикубітні системи, потім - шістнадцятикубітні. На цих системах вчені вирішують ресурсоємні завдання, потім перевіряють результати на звичайному комп'ютері. Звичайні комп'ютери поки ще дають точніші результати, хоча і витрачають на розрахунки значно більше часу.

У жовтні 2019 року наукова група Джона Мартінеса з Google заявила про досягнення квантової переваги на 53-кубітним прототипі квантового комп'ютера. Ця подія демонструє колосальний прогрес в технології квантових процесорів.

Квантова комп'ютерна система заснована на принципах суперпозиції і заплутаності. Теоретично вона здатна вирішувати за секунди завдання, на які звичайний цифровий комп'ютер витратить десятки тисяч років.

Підвищити швидкість обчислень допомагає також квантова заплутаність - коли неможливо точно дізнатися, який з пари або ланцюжка кубітів знаходиться в даному стані, вони всі знаходяться в ньому одночасно.

Основна проблема квантових обчислень полягає в тому, що потім результат цих обчислень потрібно перевести в класичний формат, на це і витрачається основний час.

Друга фундаментальна проблема - корекція помилок, які неминуче виникають при обчисленнях, зчитуванні й запису інформації в кубіти через руйнування їх квантового стану. Щоб мінімізувати або виключити їх вплив на обчислення, потрібно розробляти квантові коди, на що може піти не один десяток років. Тому поки на практиці намагаються створювати гібридні квантово-класичні процесори класу NISQ - noisy intermediate scale quantum computer, тобто зашумлений квантовий комп'ютер проміжного масштабу.

Квантові обчислювальні системи бувають двох типів. Ті, що вміють вирішувати одне-єдине завдання, називають квантовими симуляторами. Одна з перших таких систем з двох кубітів представляла собою модель молекули водню. На ній можна було тільки розрахувати її властивості. Квантові симулятори можуть працювати в звичайних комп'ютерах як співпроцесори, що вирішують конкретні і дуже затратні за часом задачі.

Універсальний квантовий комп'ютер здатний виконувати безліч різних завдань. Залежно від складності обчислень число кубітів в ньому нарощують. Недавнє досягнення Google - це демонстрація прототипу універсального квантового комп'ютера, але поки що без повної корекції помилок.

Експеримент по демонстрації квантового переваги є концептуальним доказом ефективності квантових комп'ютерів. І справа не в тому, наскільки швидше були проведені обчислення в порівнянні з класичним і навіть суперкомп'ютером, а в тому, що була продемонстрована принципова можливість проведення керованих обчислень на квантовому процесорі такого великого масштабу. До теперішнього моменту ряд теоретичних команд висловлювали і продовжують висловлювати припущення про неможливість функціонування великих штучних квантових систем в силу принципових фізичних обмежень. Результати, які отримала команда Google, експериментально спростовують ці твердження.

Перспективи розвитку квантової обчислювальної техніки сьогодні складно спрогнозувати навіть фахівцям, але вже зараз зрозуміло, що з появою квантового процесора впевненості в повному захисті даних, включаючи секрети державних органів, big data бізнес-структур, цивільного населення, може прийти кінець, хоча в той же час квантові технології можуть стати як найпотужнішою зброєю, так і найпотужнішим захистом.

Квантовий алгоритм Шора дає можливість обчислити прості множники великих чисел за практично прийнятний час і зламати шифри RSA криптосистем, тобто асиметрична криптографія опиниться під великим

ударом, як тільки буде запущений ефективний квантовий комп'ютер. Таким чином потрібна розробка нових квантово-криптографічних методів захисту інформації.

Інша загроза, якої можна уникнути, впроваджуючи квантово-криптографічні методи захисту інформації, це можливість переорієнтації великих обчислювальних потужностей, які вже обслуговують майнінг криптовалют, на переборні методи злому асиметричних (класичних) систем шифрування.

Квантові комп'ютери, коли їх можна буде використовувати масово, цілком змінять наш світ і стануть символом прогресу сучасних інформаційних систем.

УДК 343.9:159.9.075

ВОЛОДИМИР МИХАЛОВИЧ СТРУКОВ

кандидат технічних наук, доцент, професор кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

ДМИТРО ЮРІЙОВИЧ УЗЛОВ

кандидат технічних наук, начальник Управління інформаційно-аналітичної підтримки ГУ НП в Харківській області, полковник поліції

ОЛЕКСІЙ ВЯЧЕСЛАВОВИЧ ВЛАСОВ

заступник начальника Управління інформаційного-аналітичної підтримки ГУНП в Харківській області, підполковник поліції

ПРОБЛЕМИ І ПЕРСПЕКТИВИ РОЗВИТКУ ТЕХНОЛОГІЙ ОБРОБКИ ДАНИХ В ПРАВООХОРОННІЙ СФЕРІ УКРАЇНИ

Дослідження, які щорічно проводяться в сфері обробки інформації, свідчать про те, що з моменту появи глобальних комп'ютерних мереж і, зокрема, Інтернету, лавиноподібне наростання кількості згенерованих і загальнодоступних даних є стійкою характерною тенденцією.

До 2020 р. прогнозується збільшення обсягу згенерованих доступних даних до 40 зеттабайт. (Якщо записати 40 зеттабайт даних на диски Blu-ray, загальна вага дисків (без паперової та пластикової упаковки) буде дорівнювати вазі 424 авіаносців.) Одним з основних чинників цього зростання є збільшення частки автоматично генеруюємих даних: з 11% від загального обсягу у 2005 р. до понад 40% у 2020 р.

З усього океану інформації за оцінками фахівців менш 1% піддається аналізу. Разом з тим, реєстрація та зберігання інформації має сенс (тобто вона корисна) лише в тому випадку, якщо вона затребувана, тобто якимось чином обробляється. А на сьогоднішній день навіть сама елементарна обробка, така як простий перегляд, при величезному обсязі інформації людиною просто фізично неможлива.

Такий стан можна спостерігати і в правоохоронній сфері в Україні. Якщо ще зовсім недавно практичні всі накопичувані і обробляемі дані